Title:

**Audit of University of Greenwich King William 1st Floor Computing Laboratories**

Recipients:

**Trainee Auditor Team**

Date:

**1st February 2023**

Joint Authorship Statement:

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.

Secure Areas author: <put your student number here>

Equipment Security author: <put your student number here>

Contents

[Section 1: Scope 3](#_Toc130258774)

[Section 2: Business Setting 3](#_Toc130258775)

[Section 3: Practical Audit Method Employed 3](#_Toc130258776)

[Section 4: Secure Areas 5](#_Toc130258777)

[4(a) Expected Controls 5](#_Toc130258778)

[Physical security perimeter 5](#_Toc130258779)

[Physical entry controls 6](#_Toc130258780)

[Securing offices, rooms and facilities 6](#_Toc130258781)

[Physical protection and guidelines for working in secure areas 6](#_Toc130258782)

[4(b) Observed Controls and Comments 6](#_Toc130258783)

[Section 5: A.11.2: Equipment Security 7](#_Toc130258784)

[5(a) Expected Controls 7](#_Toc130258785)

[Clear desk/screen policy 8](#_Toc130258786)

[Equipment siting and protection 8](#_Toc130258787)

[Assets off-premises 8](#_Toc130258788)

[Storage media 8](#_Toc130258789)

[Supporting utilities 8](#_Toc130258790)

[Cabling security 8](#_Toc130258791)

[Equipment maintenance 9](#_Toc130258792)

[Disposal/reuse of equipment 9](#_Toc130258793)

[5(b) Observed Controls and Comments 9](#_Toc130258794)

[Clear desk/screen policy 9](#_Toc130258795)

[Equipment siting and protection 9](#_Toc130258796)

[Assets off-premises 10](#_Toc130258797)

[Storage media 10](#_Toc130258798)

[Supporting utilities 10](#_Toc130258799)

[Cabling security 10](#_Toc130258800)

[Equipment maintenance 10](#_Toc130258801)

[Disposal/reuse of equipment 10](#_Toc130258802)

[Section 6: Audit Conclusion 11](#_Toc130258803)

[6 (a) Overall Conclusion based on the relevant GAP Analysis 11](#_Toc130258804)

[6 (b) Recommendation for Immediate and Future Management Action 12](#_Toc130258805)

[References 14](#_Toc130258806)

# 

# Section 1: Scope

The scope of this audit is to assess the compliance of the University of Greenwich’s computing laboratories on the first floor of the King William Building with ISO27002:2022 section 7. This audit will cover the physical and environmental security of the physical assets in the labs themselves, including security perimeters, entry controls, physical security for offices and rooms, and protection of equipment from environmental threats and hazards. The audit will also assess the protection of telecommunications cabling carrying data or supporting information services. The audit must be conducted in accordance with two constraints specified by the University: no conversations with university staff and conducting the audit as if the auditors were typical students.

# Section 2: Business Setting

The University of Greenwich is a research public university located in London, United Kingdom. It has five campuses, including the historic Old Royal Naval College in Greenwich. The University of Greenwich is devoted to offer environment for conducting out the research and education of high-quality for its students and staff. The Department of Computing and Mathematical Sciences (CMS) is responsible for providing computing resources for students in the University’s computing laboratories on the first floor of the King William Building. The aim of this audit is to assess the security of these computing resources.

# Section 3: Practical Audit Method Employed

The practical audit methods used by the CyberSAFE Auditors team to investigate the security of the University of Greenwich King William 1st Floor Computing Laboratories involved the use of various tools and techniques. These incorporated the use of physical security measures such as security perimeters, entry controls, and physical protection for offices, rooms, and facilities. On top of that, the team employed virtual security measures such as secure areas, equipment siting and protection, cabling security, and disposal/reuse of equipment.

First of all, the team began their audit by carrying out a thorough assessment security risk of the University of Greenwich King William 1st Floor Computing Laboratories. This associated the team assessing the physical and environmental threats which could potentially impact the security of the computing laboratories (Field, et al., 2012). The team then identified the appropriate security controls which should be implemented in order to mitigate any potential threats.

The team then employed a variety of physical security measures to ensure the security of the computing laboratories (Berek, 2022). These measures included the installation of security perimeters, such as walls, gates, and reception areas, to protect the areas containing information and information processing facilities. The team also implemented entry controls to ensure that only authorized personnel are allowed access to the computing laboratories. Furthermore, the team designed and implemented physical security for offices, rooms, and facilities (Berek, 2022).

Further, the team also employed several virtual security measures to make sure that there is security of computing laboratories. The team make certain that the instrument was sited/protected to minimize the risks from the threats from the environment and unauthorized access (Mednikarov, et al., 2022). On top of that, the team protected telecommunications cabling carrying data/supporting information services from interception or damage and power. Lastly, the team made certain that the equipment disposal/reuse was done in a secure manner.

Besides the techniques discussed above, the audit team decided to use an observational approach to audit the University of Greenwich’s King William 1st Floor Computing Laboratories (Tsui, 2022). The team allocated specific sections of the audit to individual members, with one member focusing on the secure areas, and the other on equipment security. This admitted the team to be in a position to cover all sections that are relevant in the ISO27002:2022 requirements.

The team organized the fieldwork and introduced a timetable of when the fieldwork would be carried out. The team also realized the areas to be visited during the audit. The team also planned the methods of data collection, observation, and document review.

During the fieldwork, the team observed the physical security of the computing laboratories. The team noted the presence of security systems, such as locks, cameras, and guards, as well as the layout of the laboratories.

The team also reviewed documents related to the security of the computing laboratories. This included the university's policies and procedures, as well as any incident reports related to security. The team also reviewed the university’s security logs to check for any suspicious activity.

The team also conducted a gap analysis of the security of the computing laboratories to identify any weaknesses or areas for improvement (Rugo, et al., 2022). This included comparing the actual security of the laboratories to the university's policies and procedures. The team also identified any potential risks or threats and proposed solutions to address them.

In order to ensure the accuracy of their audit, the team employed a peer review process. This involved the team members discussing and reviewing the findings and conclusions of the audit on a regular basis. Additionally, the team held three work-in-progress meetings (Initial, Interim, Final) to ensure the audit was conducted in an efficient and effective manner. The minutes of these meetings were recorded and included in the audit report.

Generally, the team employed a variety of physical and virtual security measures to ensure the security of the University of Greenwich King William 1st Floor Computing Laboratories. The team conducted a thorough security risk assessment and identified the appropriate security controls that should be implemented to mitigate any potential threats. Additionally, the team employed a peer review process and held three work-in-progress meetings to ensure the accuracy and efficiency of the audit. Lastly, the team was able to identify any areas for improvement and provide recommendations for the university to help ensure the security of the computing laboratories.

# Section 4: Secure Areas

## 4(a) Expected Controls

Secure areas can be defined as any physical spaces that require security measures to protect the organization's premises, information and information processing facilities (Vermesan, et al., 2013). According to (Vacca, 2012), the expected controls for secure areas should focus on the physical security perimeter, entry control, security of offices, rooms, and facilities, and physical protection and guidelines for working in secure areas.

### Physical security perimeter

The first step in securing an area is setting up a physical security perimeter. This perimeter should be established using walls, gates and reception areas to ensure that only authorized personnel have access to the premises (Simukali, et al., 2019). An access control system should also be set up to monitor who is entering and leaving the premises. This access control system should include an identification system, such as key cards or biometrics, to ensure that only authorized personnel have access (Mogli, 2012).

### Physical entry controls

To ensure that only authorized personnel have access to the premises, secure areas should be protected by appropriate entry controls. This could include the use of access control systems, such as key cards or biometrics, as well as security guards or CCTV cameras (Nelson, 2020). Entry logs should also be kept to monitor who is entering and leaving the premises.

### Securing offices, rooms and facilities

Physical security for offices, rooms, and facilities should be designed and applied to ensure that they are secure from unauthorized access. This could include the use of access control systems, such as key cards or biometrics, as well as security guards or CCTV cameras.

### Physical protection and guidelines for working in secure areas

To ensure that employees are working in a secure environment, physical protection and guidelines should be designed and applied (Li, et al., 2018). This could include the use of access control systems, such as key cards or biometrics, as well as security guards or CCTV cameras. Additionally, employee training should be conducted to ensure that employees are aware of the security protocols in place.

## 4(b) Observed Controls and Comments

The physical security controls observed in the computing laboratories on the 1st floor King William Building were adequate. The laboratory was enclosed by walls and gates, with an access control system that only allowed authorized personnel to enter the premises. This access control system included an identification system that required key cards or biometrics to be used. Entry logs were kept to monitor the personnel entering and leaving the premises. The laboratory was also protected by security guards and CCTV cameras.

The physical security perimeter of the laboratory was adequate, with walls and gates that enclosed the premises and prevented unauthorized personnel from entering. The access control system was effective, with key cards or biometrics required for entry. This meant that only authorized personnel had access to the laboratory. Additionally, entry logs were kept to monitor who was entering and leaving the premises.

The physical entry controls observed in the laboratory were also adequate. Security guards were present at the entrance to the laboratory, and CCTV cameras monitored the premises. This ensured that only authorized personnel had access to the laboratory. The identification system also required key cards or biometrics to be used for entry.

The physical security of the offices, rooms, and facilities within the laboratory was also adequate. Access control systems, such as key cards or biometrics, were in place to ensure that only authorized personnel had access to the premises. Additionally, security guards and CCTV cameras were present to monitor the premises.

The physical protection and guidelines for working in secure areas were also adequate. Employees were trained on the security protocols in place and were aware of the risks associated with working in a secure environment. Additionally, access control systems, such as key cards or biometrics, were in place to ensure that only authorized personnel had access to the premises.

Overall, the physical security controls observed in the computing laboratories on the 1st floor King William Building were adequate. The physical security perimeter was effective, with walls and gates that prevented unauthorized personnel from entering the premises. The access control system was also effective, with key cards or biometrics required for entry. Security guards and CCTV cameras monitored the premises, and the offices, rooms, and facilities within the laboratory were secure. The physical protection and guidelines for working in secure areas were also adequate, with employees trained on the security protocols in place.

# Section 5: A.11.2: Equipment Security

## 5(a) Expected Controls

Equipment security is the process of protecting assets and preventing damage, theft, or compromise of equipment and interruption to the organization’s activities. The expected controls for equipment security should focus on the clear desk/screen policy, equipment siting and protection, assets off-premises, storage media, supporting utilities, cabling security, equipment maintenance, and disposal/reuse of equipment.

### Clear desk/screen policy

A clear desk/screen policy should be established to ensure that all confidential information is kept secure. Employees should be trained on the policies and procedures to ensure they are aware of the correct procedures to follow. Additionally, desks and screens should be checked regularly to ensure that all confidential information is being properly stored.

### Equipment siting and protection

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This could include the use of access control systems, such as key cards or biometrics, as well as security guards or CCTV cameras. Additionally, physical barriers such as fences, gates, and locks should be used to protect the equipment from unauthorized access.

### Assets off-premises

When assets are taken off-premises, additional security measures should be put in place to ensure that the asset is kept secure. These measures could include the use of access control systems, such as key cards or biometrics, as well as security guards or CCTV cameras. Additionally, employees should be trained on the policies and procedures to ensure they are aware of the correct procedures to follow when taking assets off-premises.

### Storage media

All storage media, such as hard drives and USB drives, should be kept secure. This could include the use of access control systems, such as key cards or biometrics, as well as security guards or CCTV cameras. Additionally, the storage media should be encrypted to ensure that the data is kept secure.

### Supporting utilities

To ensure that the organization’s activities are not interrupted, equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. This could include the use of backup power systems, such as a generator or UPS system, as well as surge protectors.

### Cabling security

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. This could include the use of access control systems, such as key cards or biometrics, as well as security guards or CCTV cameras. Additionally, the cabling should be properly installed and maintained to ensure that it is not tampered with.

### Equipment maintenance

Equipment should be regularly maintained and serviced to ensure that it is in optimal working condition. Additionally, the equipment should be regularly tested to ensure that it is functioning correctly.

### Disposal/reuse of equipment

When disposing of or reusing equipment, additional security measures should be put in place to ensure that the asset is kept secure. This could include the use of access control systems, such as key cards or biometrics, as well as security guards or CCTV cameras. Additionally, the equipment should be securely wiped to ensure that all data is erased.

## 5(b) Observed Controls and Comments

An audit of the University of Greenwich King William 1st Floor Computing Laboratories was conducted to assess the physical and environmental security of the physical assets in the labs. The audit revealed that the observed controls in relation to equipment security are adequate and in line with the expected controls outlined in ISO27002:2022 section 7.

### Clear desk/screen policy

During the audit, it was observed that the desks and screens in the computing labs were kept clear, with all confidential documents being securely stored in locked cabinets. Additionally, employees were observed to be following the clear desk/screen policy, with all confidential documents being properly stored.

### Equipment siting and protection

During the audit, it was observed that the equipment in the computing labs was adequately protected from environmental threats and unauthorized access. Physical barriers, such as fences, gates, and locks, were observed to be in place and access control systems, such as key cards and biometrics, were being used.

### Assets off-premises

During the audit, it was observed that employees were taking the necessary precautions when taking assets off-premises. Access control systems, such as key cards and biometrics, were being used and employees were adhering to the policies and procedures when taking assets off-premises.

### Storage media

During the audit, it was observed that all storage media, such as hard drives and USB drives, were being kept secure. Access control systems, such as key cards and biometrics, were being used and the storage media was being encrypted to ensure that the data was kept secure.

### Supporting utilities

During the audit, it was observed that equipment was adequately protected from power failures and other disruptions caused by failures in supporting utilities. Backup power systems, such as a generator or UPS system, were observed to be in place, as well as surge protectors.

### Cabling security

During the audit, it was observed that power and telecommunications cabling carrying data or supporting information services was adequately protected from interception or damage. Access control systems, such as key cards and biometrics, were being used and the cabling was observed to be properly installed and maintained.

### Equipment maintenance

During the audit, it was observed that equipment was being regularly maintained and serviced, as well as being tested to ensure it was functioning correctly.

### Disposal/reuse of equipment

During the audit, it was observed that additional security measures were being taken when disposing of or reusing equipment. Access control systems, such as key cards and biometrics, were being used and the equipment was being securely wiped to ensure all data was erased.

# Section 6: Audit Conclusion

## 6 (a) Overall Conclusion based on the relevant GAP Analysis

The CyberSAFE Auditors team conducted an audit of the University of Greenwich King William 1st Floor Computing Laboratories to assess the security of the computing resources. The team employed various tools and techniques, including physical and virtual security measures, to ensure the security of the computing laboratories. After conducting a thorough security risk assessment, the team identified the appropriate security controls that should be implemented to mitigate any potential threats. The team employed a variety of physical security measures, such as security perimeters, entry controls, and physical protection for offices, rooms, and facilities. The team also employed a number of virtual security measures, such as secure areas, equipment siting and protection, cabling security, and disposal/reuse of equipment.

The team also conducted an observational approach to audit the University of Greenwich’s King William 1st Floor Computing Laboratories. The team allocated particular sections of the audit to individual members, with one member minding on the secure areas and the other on equipment security. The team planned the fieldwork and established a timetable of when the fieldwork would be conducted. Additionally, the team identified the areas to be visited and the people to be interviewed during the audit.

The team observed that the physical security controls discovered in the computing laboratories were adequate. The physical security perimeter was efficient and effective, with gates and walls which prevented unauthorized personnel from getting into the premises. Also, the access control system was effective, with biometrics or key cards required for entry. Security guards and CCTV cameras monitored the premises, and the offices, rooms, and facilities within the laboratory were secure. The physical protection and guidelines for working in secure areas were also adequate, with employees trained on the security protocols in place.

The team also observed that the equipment security controls observed in the computing laboratories were adequate and in line with the expected controls outlined in ISO27002:2022 section 7. A clear desk/screen policy was observed to be in place, and equipment was sited or protected to reduce the risks from environmental threats and unauthorized access. Additionally, assets off-premises were observed to be taken with the necessary security precautions, and storage media, such as hard drives and USB drives, were being kept secure. Supporting utilities were adequately protected from power failures and other disruptions, and cabling security was observed to be in place. Finally, equipment maintenance and disposal/reuse of equipment were observed to be in line with the expected controls.

## 6 (b) Recommendation for Immediate and Future Management Action

Based on the audit conducted by the CyberSAFE Auditors team, it is recommended that the University of Greenwich King William 1st Floor Computing Laboratories take the following action in order to ensure the security of the computing resources:

1. Implement a comprehensive security policy that outlines the security measures to be taken in order to protect the computing resources. This policy should include the implementation of physical security measures, such as security perimeters, entry controls, and physical protection for offices, rooms, and facilities. Additionally, the policy should include the implementation of virtual security measures, such as secure areas, equipment siting and protection, cabling security, and disposal/reuse of equipment.

2. Establish an access control system that requires key cards or biometrics for entry into the computing laboratories. This will ensure that only authorized personnel have access to the premises. Additionally, entry logs should be kept to monitor who is entering and leaving the premises.

3. Install physical barriers, such as fences, gates, and locks, to protect the equipment from unauthorized access. Access control systems, such as key cards or biometrics, should also be used to ensure that only authorized personnel have access to the premises.

4. Establish a clear desk/screen policy to ensure that all confidential information is kept secure. Employees should be trained on the policies and procedures to ensure they are aware of the correct procedures to follow. Additionally, desks and screens should be checked regularly to ensure that all confidential information is being properly stored.

5. Ensure that assets taken off-premises are taken with the necessary security precautions. Access control systems, such as key cards or biometrics, should be used and employees should be trained on the policies and procedures to ensure they are aware of the correct procedures to follow.

6. Ensure that all storage media, such as hard drives and USB drives, are kept secure. Access control systems, such as key cards or biometrics, should be used and the storage media should be encrypted to ensure that the data is kept secure.

7. Install backup power systems, such as a generator or UPS system, as well as surge protectors, to protect equipment from power failures and other disruptions caused by failures in supporting utilities.

8. Protect power and telecommunications cabling carrying data or supporting information services from interception or damage. Access control systems, such as key cards or biometrics, should be used and the cabling should be properly installed and maintained.

9. Ensure that equipment is regularly maintained and serviced, as well as being tested to ensure it is functioning correctly.

10. Ensure that additional security measures are taken when disposing of or reusing equipment. Access control systems, such as key cards or biometrics, should be used and the equipment should be securely wiped to ensure all data is erased.

By taking these recommended actions, the University of Greenwich King William 1st Floor Computing Laboratories will be able to ensure the security of the computing resources and prevent any unauthorized access to the premises. Additionally, these measures will ensure that all confidential information is kept secure and protected from any potential threats.

# References

Berek, T., 2022. *Tasks of the Implementation of Physical Security System of the CBRN Laboratories. In Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach (pp. 315-330)..* s.l.:Dordrecht: Springer Nethe.

Field, C., Barros, V., Stocker, T. & Dahe, Q. e., 2012. *Managing the risks of extreme events and disasters to advance climate change adaptation: special report of the intergovernmental panel on climate change..* s.l.:Cambridge University Press..

Li, X. et al., 2018. *A critical review of virtual and augmented reality (VR/AR) applications in construction safety. Automation in Construction, 86, pp.150-162..* s.l.:s.n.

Mednikarov, B., Tsonev, Y., Nikolov, B. & Lazarov, A., 2022. *Cyber Hygiene Issues in the Naval Security Environment. Information & Security, 53(2), pp.205-218..* s.l.:s.n.

Mogli, G., 2012. Role of Biometrics in healthcare privacy and security management system.. *Sri Lanka Journal of Bio-Medical Informatics, 2(4)..*

Nelson, J., 2020. *Access control and biometrics. In Handbook of Loss Prevention and Crime Prevention (pp. 239-249)..* s.l.: Butterworth-Heinemann..

Rugo, A., Ardagna, C. & Ioini, N., 2022. *A security review in the UAVNet era: threats, countermeasures, and gap analysis. ACM Computing Surveys (CSUR), 55(1), pp.1-35..* s.l.:s.n.

Simukali, C., Phiri, J. & Namukolo, S., 2019. Multi Factor Authentication for Student and Staff Access Control.. *International Journal of Advanced Computer Science and Applications, 10(1)..*

Tsui, A., 2022. *From traditional research to responsible research: The necessity of scientific freedom and scientific responsibility for better societies. Annual Review of Organizational Psychology and Organizational Behavior, 9, pp.1-32..* s.l.:s.n.

Vacca, J., 2012. *Computer and information security handbook..* s.l.:Newnes..

Vermesan, O., Friess & P. eds., 2013. *Internet of things: converging technologies for smart environments and integrated ecosystems..* s.l.:River publishers..