A REPORT ON

ISMS - ISO 27001:2013 Audit Project

Control & Audit in Information Systems

INFO 4330

Lecturer's Name:
Asst. Prof. Dr Noor Hayani

Student's Name:

Muhammad Azhad bin Muhammad Nasim

INTRODUCTION

This report has been completed by our group and relates to the auditing activity detailed below:

Type/Date/Duration	Certification/Standard	Site Address
Internal Audit 23/05/2023 1 hour	ISO 27001:2013	IIUM International Culture Center (ICC), International Islamic University Malaysia 53100 Gombak, Selangor

OBJECTIVE OF THE AUDIT

The objective of the internal audit was to conform to the organisation's own requirements for its information security management system, and the requirement of this International Standard has been effectively implemented and maintained.

AUDIT SUMMARY

Audit Information

Audited Entity: Kulliyyah of Information & Communication Technology, IIUM

Auditee (s):

1. Prof Dr Asadullah Shah, Head of the Department Information System
2. Asst. Prof Dr Nurul Nuha, Security Officer
3. Zuyati binti Mohamad, Secretary of Department Information System
4. Wan Nasruddin, Administrative Officer

Auditor (s):

1. Muhammad Azhad bin Muhammad Nasim
2. Muhammad Syazwan Bin Hosen
3. Muhammad Amiruddin Bin Khairuddin
4. Adibah Binti Rokasah

Overall Conclusion

The audit conducted at the IIUM International Culture Center (ICC) focused on assessing the centre's physical and environmental security measures as well as the condition and functionality of its equipment.

We would like to express our sincere appreciation and gratitude to all the auditors who were involved in this process. Your expertise, attention to detail, and thoroughness were instrumental in successfully carrying out the audit.

A special thank you goes to Prof. Noor Hayani for opening the meeting and for her support and cooperation throughout the audit. Your involvement and guidance have greatly contributed to the effectiveness and efficiency of the audit process.

During the audit, the auditors diligently examined the ICC's physical security measures, including access controls, surveillance systems, and emergency preparedness. They also assessed the centre's environmental security practices, such as fire prevention and detection systems, security lock system, and maintenance of a safe working environment. Additionally, the audit team thoroughly inspected and tested the functionality and maintenance of the ICC's equipment to ensure optimal performance and longevity.

Based on the audit findings, the report will provide detailed recommendations to address any identified weaknesses or areas for improvement in the ICC's physical and environmental security measures and equipment management. These recommendations aim to enhance the centre's ability to safeguard its premises, protect its assets, and maintain a secure and efficient operational environment.

By conducting this audit, we have contributed to strengthening the overall security and operational resilience of the IIUM International Culture Center. The findings and recommendations will serve as a guide for the centre to implement necessary measures and best practices to mitigate risks, promote safety, and ensure the longevity and effectiveness of its equipment.

<u>OPENING MEETING</u>

The formal opening meeting included the objective of the audit, methodology and terminology used confidentiality, number of staff in scope and the scope of assessment.

RELATED DOCUMENTS

Documents reviewed included:

1. **IIUM International Culture Center (ICC) (Outside)**

SCOPE OF THE AUDIT

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001:2013 and the defined assessment plan provided in terms of locations and areas of the system and organisation to be assessed.

Physical and Environment Security: A.11

The client occupies IIUM Culture Centre. The following scopes of the audit were observed:

A.11	**Physical and environmental security**	
A.11.1	**Secure areas**	
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.		
A.11.1.1	Physical security perimeter	*Control* Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
A.11.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms and facilities shall be designed and applied.
A.11.1.4	Protecting against external and environmental threats	*Control* Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
A.11.1.5	Working in secure areas	*Control* Procedures for working in secure areas shall be designed and applied.
A.11.1.6	Delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

A.11.2 Equipment		
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
A.11.2.1	Equipment siting and protection	*Control* Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.11.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
A.11.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.11.2.5	Removal of assets	*Control* Equipment, information or software shall not be taken off-site without prior authorization.
A.11.2.6	Security of equipment and assets off-premises	*Control* Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
A.11.2.7	Secure disposal or re-use of equipment	*Control* All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
A.11.2.8	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.
A.11.2.9	Clear desk and clear screen policy	*Control* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

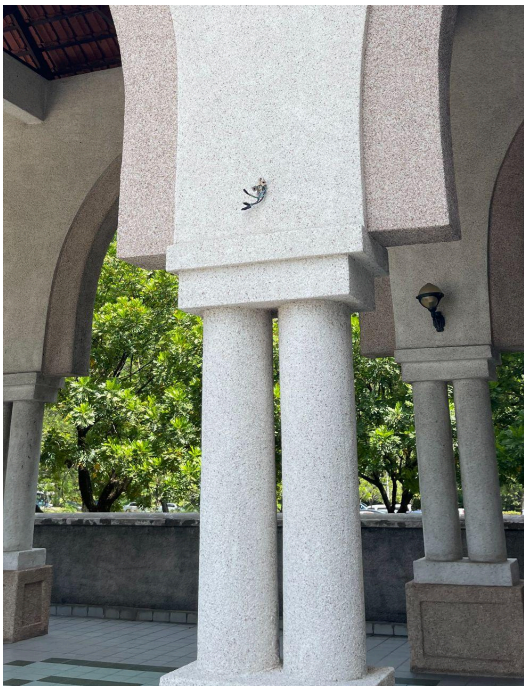
AUDIT SCHEDULE

Time	**Location**	**Remarks**
2.00- 2.15	Opening Meeting KICT Block C Level 1	Attendance: Head of Dept. (HOD) Security Officer Secretary
2.20-3.00	ICC IIUM Physical and Environment	Attendance: Security Officer Technical & Administrative Officer

CLOSING MEETING

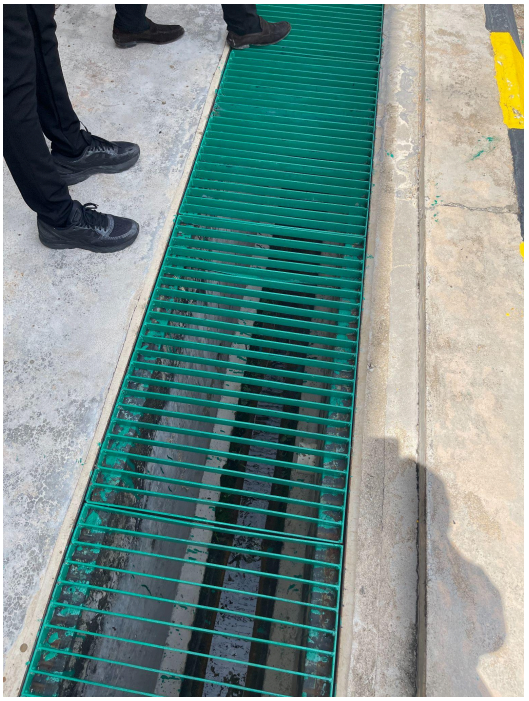
OBSERVATION:

Clause	A.11.2.3
Date	23/5/2023
Time	2:34 pm
Location	Left-wing outside of ICC



Report
The lamp cabling is being left out without proper cover after the lamp has been thrown away.

Clause	A.11.2.1
Date	23/5/2023
Time	2:19 pm
Location	Beside Main Entrance of ICC

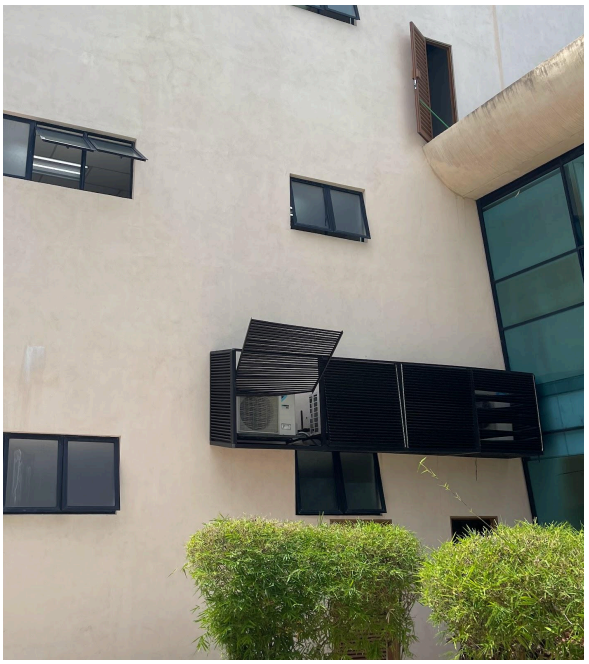


Report
The drain cover is properly maintained to avoid incidents.

The cage to secure the air conditioner was not appropriately closed which can cause danger. This is contradicted by **policy requirement A.11.2.1. Equipment siting and protection "Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access"**.

Clause	A.11.2.1
Date	23/5/2023
Time	2:41 pm
Location	Foyer 2 ICC near Azman Hashim Complex

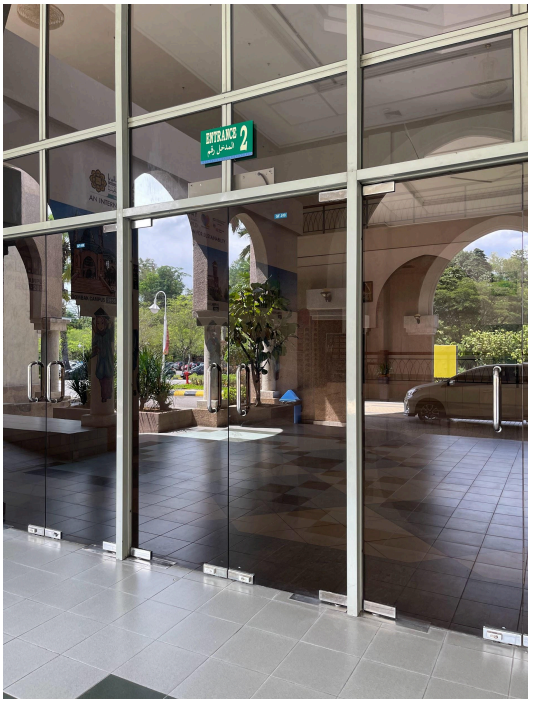
Report
Non-compliance.The cage used to protect the air-conditioner is open and can trigger an accident.



The main entrance door is locked when there are no occasions. This aligns with the **policy requirement A.11.1.3 Securing offices, rooms and facilities "Physical security for offices, rooms, and facilities shall be designed and applied"**.

Clause	A.11.1.3
Date	23/5/2023
Time	2:27 pm
Location	Main Entrance ICC

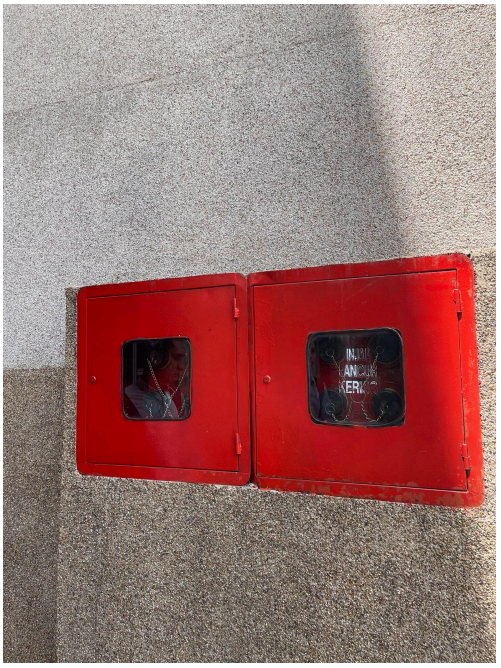
Report
Compliance. The door is locked to protect rooms and facilities inside the building.



There is a dry riser system available at the building which will be used by firefighters when a fire happens. This is parallel with the **policy requirement A.11.1.4 Protecting against external and environmental threats "Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.**

Clause	A.11.1.4
Date	23/5/2023
Time	2:29 pm
Location	Near ICC car park

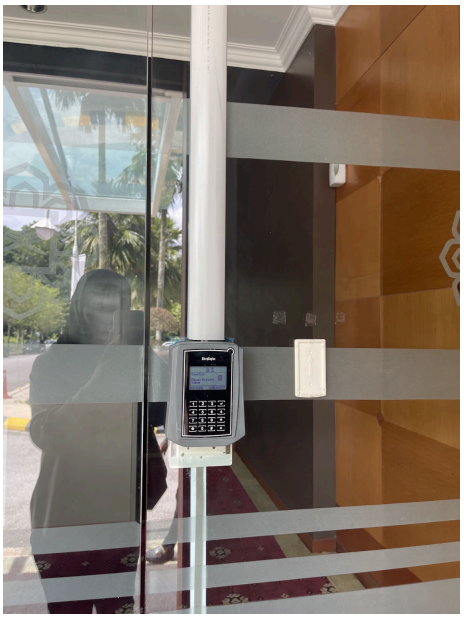
Report
Compliance. There are two dry riser systems found at the building.



The management room is locked appropriately with a security lock door system which is aligned with the **policy requirement A.11.1.2 Physical entry controls "Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access".**

Clause	A.11.1.2
Date	23/5/2023
Time	2:20 pm
Location	Management room

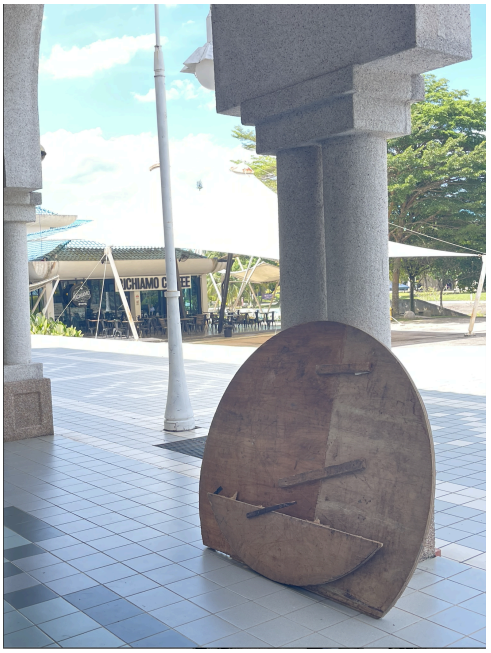
Report
Compliance. The door is protected by a security lock door.



An unused round table is stored in an improper place which denies the **policy requirement A.11.2.8 Unattended user equipment "Users shall ensure that unattended equipment has appropriate protection".**

Clause	A.11.2.8
Date	23/5/2023
Time	2:42 pm
Location	Left wing outside the ICC

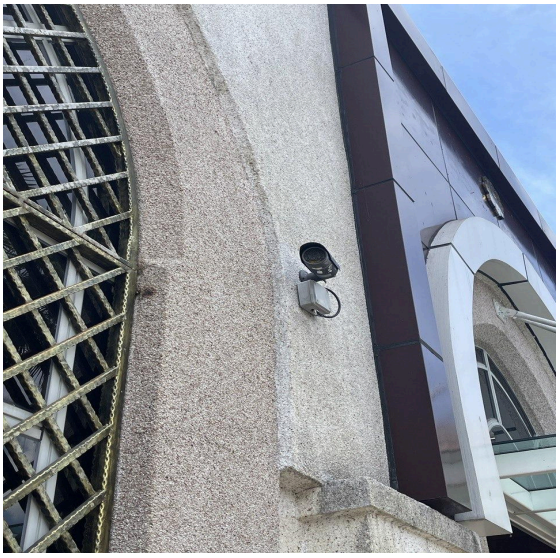
Report
Non-compliance. An unused round table should be placed in the store room.



CCTV is installed in front of ICC to increase security. It can be used to identify potential threats and to investigate incidents that do occur. This aligns with the **policy requirement A.11.1.4 Protecting against external and environmental threats "Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.**

Clause	A.11.1.4
Date	23/5/2023
Time	2:32 pm
Location	In front of ICC

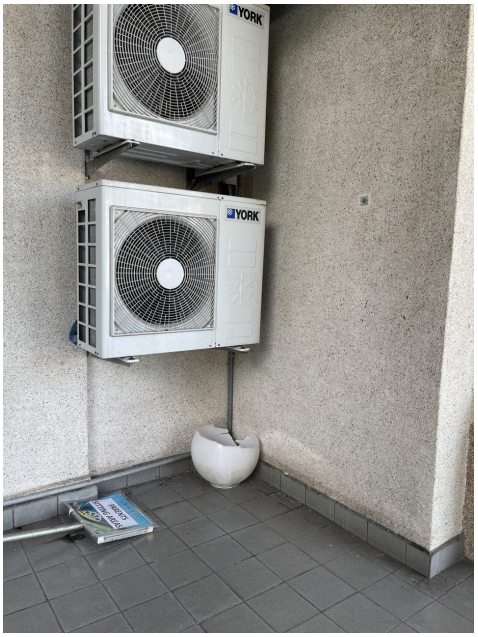
Report
Compliance. The CCTV is installed properly



A broken lamp was found not properly disposed of besides the ICC building. It may harm the passerby of the building. This is contradicted by **policy requirement A.11.2.4. Equipment maintenance. "Equipment shall be correctly maintained to ensure its continued availability and integrity.**

Clause	A.11.2.4
Date	23/5/2023
Time	2:40 pm
Location	Left wing outside the ICC

Report
Non-Compliance. Improper disposal of broken equipment



APPENDIX :Closing Meeting Report

Function: Physical & Environmental Security **Location: IIUM International Culture Center (ICC)**				**Prepared by: M. Azhad** **Date: 14/6/2023**	
Clause	**Nature of Weakness and Impact**	**Non-Conformity(NC)**		**Notification to Management**	
		Yes/No	**Justification**	**Report Date**	**Proposed Recommendation**
A.11.1.1	Physical Security Perimeter -Reception Area -Physical Barriers -Fire Doors -Intruder Detection System	No	Every single area and system secured	23/5	**OFI**: Enforcement of 24/7 hour physical barrier implementation *(ICC Management)
A.11.1.2	Physical Entry Control -Visitors -Access Control -Audit Trail -Visible Identification	No	Existing security devices functioning well Eg. Password and ID door access system -implementation and week enforcement of ID Card display	23/5	**OFI:** Provide safety mechanism to limit potential intruder *(OSeM rounding)
A.11.1.3	Securing Offices, Rooms and Facilities -Additional Security -Recording Equipment -Vacant Areas -Directories	No	Security measures under control Eg. Security officer, CCTV	23/5	**OFI:** Need regular/ schedule maintenance *(ICC Management)
A.11.1.4	Protecting Against External and Environmental Threats -Fire Drill -Drainage system -Recording Equipment	No	Good drainage system surrounding the premises. CCTVs are installed around premises	23/5	No Comment
A.11.1.5	Working in Secure Areas -Air conditioning system	No	OCSH – good practice of working in secure area -Air conditioning	23/5	**OFI:** Regularly maintenance must be carried out *(Daya Bersih)

			system sometime caught failure		
A.11.1.6	Delivery and Loading Area	No	Well maintained and secured but no proper signage	23/5	**OFI:** Provide proper signage and restricted area to avoid illegal parking vehicle *(ICC Management)
A.11.2.1	Equipment Siting and Protection -Siting -Protection -Environmental Lightning Protection	Yes	Some equipments are not properly installed and may cause harm	23/5	**OFI:** The cage used to protect the air-conditioner is open and should be fixed to avoid any accident. *(Daya Bersih)
A.11.2.2	Supporting Utilities -Capacity -Inspection and Testing -Alarms	No	Every single device under scheduled inspection but alarm system got function improperly	23/5	**OFI:** Maintenance check should be implemented to make sure alarm system working properly *(Daya Bersih)
A.11.2.3	Cabling Security -Cable Routing -Shielding -Access Control	Yes	Some cables are being left out without a cover	23/5	**OFI:** Lamp cabling is being left out without proper cover.
A.11.2.4	Equipment Maintenance	No	Every equipment in the premises undergone scheduled maintenance but reported equipment failures not immediately taken care	23/5	**OFI:** Proper and immediate action needed for failure equipment report *(Daya Bersih)
A.11.2.5	Removal of Assets	No	Every single asset protected from easily removed	23/5	No comment
A.11.2.6	Security of Equipment and	No	All are well protected	23/5	No comment

	Assets off-premises				
A.11.2.7	Secure Disposal or reuse of equipment	No	All item of equipment containing storage media are verified for disposal	23/5	**OFI:** Properly dispose confidential document with paper shredder etc
A.11.2.8	Unattended User Equipment	No	Secured by password and identification security but sometime left unattended	23/5	**OFI:** Prepare backup staff to avoid unattended equipment being access illegally and enforce clear desk policy
A.11.2.9	Clear Desk and Clear Screen Policy	No	Well prepared and observed carefully	23/5	**OFI:** Clear desk and clear screen policy should be well alert and acknowledge the employees regularly

APPENDIX: Assessment Participants

On behalf of the KICT Management:

Name	Position
Prof Dr Asadullah Shah	Head of Department Information System
Asst Prof Dr Nurul Nuha	Security Officer
Zuyati binti Mohamad	Secretary
Wan Nasruddin bin Ahmad	Administrative Officer

On behalf of Auditing Committee:

Name	Position
Muhammad Azhad bin Muhammad Nasim	Lead Auditor
Muhammad Syazwan Bin Hosen	Auditor 1
Muhammad Amiruddin Bin Khairuddin	Auditor 2
Adibah Binti Rokasah	Auditor 3

APPENDIX: Attendance Sheet

<table>
<tr><th colspan="4">Physical security audit schedule and attendance record</th></tr>
<tr><td colspan="2">Date of Audit: 23/5/2023
Start time: 2.00 PM</td><td colspan="2">Audit file no: 12345678
Finish time: 3.00 PM</td></tr>
<tr><td colspan="4">Company being audited: IIUM Cultural Centre
Address: International Islamic University Malaysia,53100 Jalan Gombak, Kuala Lumpur.

Company contact persons: Dr Noor Hayani

Email:noorhayani@iium.edu.my

Auditor’s details:
Muhammad Azhad bin Muhammad Nasim
Muhammad Syazwan Bin Hosen
Muhammad Amiruddin Bin Khairuddin
Adibah Binti Rokasah</td></tr>
<tr><td rowspan="2">Company staff</td><td rowspan="2">Position</td><td colspan="2">Signature</td></tr>
<tr><td>Entry meeting</td><td>Exit meeting</td></tr>
<tr><td>Dr Noor Hayani</td><td>Security Officer</td><td>2.00 PM</td><td>3.00 PM</td></tr>
<tr><td colspan="4">Proposed schedule</td></tr>
<tr><td colspan="2">Time</td><td colspan="2">Location</td></tr>
<tr><td colspan="2">2.00</td><td colspan="2">Arrival and Open Meeting</td></tr>
<tr><td colspan="2">2.15</td><td colspan="2">Site audit</td></tr>
<tr><td colspan="2">2.50</td><td colspan="2">Completion, Auditee sign-off</td></tr>
</table>