

22CSCI34H

Computer Systems Security

Phase 2

Done by: Mayar192785.

Major: Software Engineering.

Table of Contents

[Introduction to the ISO 27001 Framework: 3](#_Toc132714216)

[Iso 27001 phases: 4](#_Toc132714217)

[Iso 27001 controls: 4](#_Toc132714218)

[Annex A.5 Information Security Policies (2 controls): 4](#_Toc132714219)

[I. A.5.1.1 Policies for information security: 4](#_Toc132714220)

[II. A.5.1.2 Review of the policies for information security: 5](#_Toc132714221)

[Annex A.6 Organization of information Security (7 controls): 5](#_Toc132714222)

[I. A.6.1.1 Information Security Roles and Responsibilities: 5](#_Toc132714223)

[II. A.6.1.2 Segregation of duties: 5](#_Toc132714224)

[III. A.6.1.4 Contact with special interest groups: 5](#_Toc132714225)

[IV. A.6.1.5 Information Security in Project Management: 5](#_Toc132714226)

[V. A.6.2.1 Mobile Device Policy: 5](#_Toc132714227)

[VI. A.6.2.2 Teleworking: 6](#_Toc132714228)

[Annex A.7 Human Resource Security (6 controls): 6](#_Toc132714229)

[I. A.7.2.1 Management Responsibilities: 6](#_Toc132714230)

[II. A.7.3.1 Termination or change of employment responsibilities: 6](#_Toc132714231)

[Annex A.8 Asset Management (10 controls): 6](#_Toc132714232)

[I. A.8.1.1 Inventory of Assets: 7](#_Toc132714233)

[II. A.8.1.2 Ownership of Assets: 7](#_Toc132714234)

[III. A.8.1.3 Acceptable Use of Assets: 7](#_Toc132714235)

[IV. A.8.1.4 Return of Assets: 7](#_Toc132714236)

[V. A.8.2.1 Classification of Information: 7](#_Toc132714237)

[VI. A.8.2.2 Labelling of Information: 7](#_Toc132714238)

[VII. A.8.2.3 Handling of Assets: 7](#_Toc132714239)

[Annex A.9 Access Control (14 controls): 7](#_Toc132714240)

[I. A.9.1.1 Access Control Policy: 7](#_Toc132714241)

[II. A.9.1.2 Access to Networks and Network Services: 8](#_Toc132714242)

[III. A.9.2.1 User Registration and Deregistration: 8](#_Toc132714243)

[IV. A.9.2.2 User Access Provisioning: 8](#_Toc132714244)

[V. A.9.2.5 Review of User Access Rights: 8](#_Toc132714245)

[VI. A.9.2.6 Removal or Adjustment of Access Rights: 8](#_Toc132714246)

[VII. A.9.4.1 Information Access Restriction: 8](#_Toc132714247)

[Annex A.11 Physical and Environmental Security (15 controls): 8](#_Toc132714248)

[I. A.11.1.4 Protecting against External and Environmental Threats: 8](#_Toc132714249)

[Annex A.13 Communications Security (7 controls): 9](#_Toc132714250)

[I. A.13.1.1 Network Controls: 9](#_Toc132714251)

[Cybersecurity Attack Scenarios: 10](#_Toc132714252)

[Scenario 1: Administrative Branch: 10](#_Toc132714253)

[Scenario 2: Students: 10](#_Toc132714254)

[Scenario 3: Academic Staff: 10](#_Toc132714255)

[References: 11](#_Toc132714256)

# Introduction to the ISO 27001 Framework:

ISO/IEC 27001 is an information security management system adaptation that provides cost-effective protection for the organization’s information. Organizations using ISO 27001 are certified and acknowledged for having good privacy protection. Moreover, ISO 27001 has three important aspects: confidentiality, integrity, and availability (the CIA triad), where each aspect represents an important role in this framework. Confidentiality in allowing authorized persons to access the information. While integrity is where authorized people have the permission to change information, and finally availability is having the information available to the authorized people whenever they need it. To reach those three aspects, ISO 27001 must be one step ahead by trying to figure out what risks can threat the existing information, risk assessment, and then define a suitable plan on how to prevent the threat, which is called a risk treatment, and eventually implementing a safeguard that prevents any security risk. ISO 27001 can manage any organization, whether private or public, profit or non-profit, of any size. In contrast, BUE will need this framework to achieve high-level security, and it will help manage each group and their requirements independently. Furthermore, ISO 27001 will help the organization, BUE, address the security weakness and solutions to solve it without any concerns from any of the staff in understanding the risk or how to enable it; everything is taken care of by ISO 27001. Any change of legal requirement, ISO can implement it easily, and it can prevent any cost, but for future concerns, it will save a lot of money since ISO has high protection. This framework provides technical and theoretical approaches to protect and train the user on the use of the information security framework. And it can protect information whether it is physical or not, which the university would need since it includes both physical and applicational information, including student records, research, and more. Moreover, the framework has legal procedures for systematic approaches, which gives it extra credit, and follows GDPR (General Data Protection Regulations) and FERAP (The Family Educational Rights and Privacy Act). This legal regulation helps in avoiding any penalties. ISO 27001 always updates and improves their framework in consideration of any change in either technical or legal regulation, which also proves that it provides the organization with the most up-to-date version. In addition, the university can gain more stakeholders and funds if it uses ISO 27001 as its information security standard because it has a good reputation among many big international organizations, which can raise its profile among other universities and gain a lot of trust for securing the privacy of the user.

# Iso 27001 phases:

There are six phases that any organization should follow to implement ISMS; ISO is the standard for information security management systems (ISMS), which are:

Phase 1: Identifying the risks, stakeholders, and assets that the ISMS must cover, which includes defining the scope.

Phase 2: Identify the risks that are associated with the assets that were evaluated in the first phase. This phase is called risk assessment.

Phase 3: Create a plan called a risk treatment plan to figure out how to eliminate the risks found in Phase 2.

Phase 4: Implement the risk treatment plan by adjusting the necessary controls in place to eliminate the risks.

Phase 5: Monitor and review the effectiveness and efficiency of the ISMS work.

Phase 6: The final phase is to keep monitoring, reviewing, and updating to keep improving the ISMS and to ensure that everything is effective and stable.

Those six phases help organizations enable the ISMS and protect sensitive information and assets from any security threats or risks.

# Iso 27001 controls:

Annex A of ISO 27001 contains 114 controls that are divided into 14 sections. Each organization chooses the controls that they need to protect the information. The controls that the BUE needs are as follows:

## Annex A.5 Information Security Policies (2 controls):

These policies will be required to be written and known by the BUE. [1] It is important for the policies to be achieved to have the ISO 27001 certification.

### A.5.1.1 Policies for information security:

A set of guidelines must be developed, authorized by the BUE, and distributed to the staff members. Those policies must be guided by the requirements that the BUE needs with the rules and legislation that may have an impact on the organization. The guidelines outline the values that members must uphold. [2]

### A.5.1.2 Review of the policies for information security:

The policies must be reviewed regularly on an annual basis, whenever any changes occur whether risks, legislation, regulation, or even security weakness so the policies will be required to be changed according to the changes. The ISMS has a feature that can automatically review which helps in reducing a huge amount of time.[2]

## Annex A.6 Organization of information Security (7 controls):

It covers the responsibilities and tasks assigned to each group which is divided into 2 sections:

Section 1: Annex A.6.1: it ensures that BUE is implementing and maintaining information security. [1]

Section 2: Annex A.6.2: it addresses the remote practice and guarantees that any remote work is working probably. [1]

They are 7 controls on total but all 6 will be used in the BUE security which are:

### A.6.1.1 Information Security Roles and Responsibilities:

Roles and responsibilities of every member of staff must be defined and make it clear for the auditor the responsibility that each staff to ensure security. [3]

### A.6.1.2 Segregation of duties:

The roles and tasks must be set apart from each other, so no confusion or unauthorized modification happens. The university has a lot of different staff with different tasks so it must be isolated to have a higher control on higher risks. [3]

### A.6.1.4 Contact with special interest groups:

Discussions with specialists or any group must be held to organize each group and their purpose. [3]

### A.6.1.5 Information Security in Project Management:

The organization must be accountable for information security and all staff must consider information security, as well, in all stages. [3]

### A.6.2.1 Mobile Device Policy:

It takes into consideration the use of any mobile devices such as phones, laptops etc. which makes the organization more flexible but raises a security vulnerability. There must be policies and awareness to control the free use of mobile devices such as having no free access to Wi-Fi to prevent any unauthorized observer navigating without permission to access. Trusted networks, backup, registration, malware, antivirus, remote disabling all those must be considered in the policies. [3]

### A.6.2.2 Teleworking:

Off-site working, known as teleworking, must also have regulations added to the policies to secure the information. In the risk assessment phase, teleworking must be considered to help flexibility but with an appropriate plan of any potential threats. [3]

## Annex A.7 Human Resource Security (6 controls):

This section is to help the staff understand their required tasks. It includes 3 sections which are:

Section 1: A.7.1: it states the contracts of each member of staff before working.

Section 2: A.7.2: During employment, it states the responsibilities that are upon the staff.

Section 3: A.7.3: It addresses the restrictions that are taken in case of unemployment or change of roles.

Two controls will be used in this section which are:

### A.7.2.1 Management Responsibilities:

Staff that are responsible for information security must have good training and understanding of their important role and how they are going to manage and secure information. The staff who are given this role must be trusted and managed correctly to have a well-secured system with no downfalls.[4]

### A.7.3.1 Termination or change of employment responsibilities:

The contract that is upon each member of staff must clearly state that if they leave, no information is stated outside to prevent any risk. The auditor must be provided with any changes to check if all assets are returned, and if a member of the staff changed roles, the auditor must take into consideration that no assets from the previous job are accessible to that staff anymore.[4]

## Annex A.8 Asset Management (10 controls):

It illustrates the list of information assets and the controls needed to protect them and it’s divided into three sections:

Section 1: Annex A.8.1: identifying the assets within the scope of ISMS. [1]

Section 2: Annex A.8.2: makes sure that the assets are subjected to an appropriate defense. [1]

Section 3: Annex A.8.3: it handles any unauthorized disclosure, modification, removal, or destruction that could affect the sensitive data, this practice is called media handling. [1]

We will be using 7 controls which are:

### A.8.1.1 Inventory of Assets:

A list of assets must be managed and controlled together to show the lifecycle of information which includes creation, processing, storage, transmission, deletion, and destruction stages.[5]

### A.8.1.2 Ownership of Assets:

Assets must have owners to manage them effectively; additionally, ownership can change through the lifecycle.[5]

### A.8.1.3 Acceptable Use of Assets:

Every person in the organization must know the acceptable use of assets and the rules associated with it and the acceptable use of assets must be documented.[5]

### A.8.1.4 Return of Assets:

Assets must be returned and managed appropriately it is an obligation of all the staff.[5]

### A.8.2.1 Classification of Information:

To protect the information, all assets must be classified as any unauthorized threats. Moderating classifications helps in adjusting the options to not be complicated which could be confusing or simple which could be under controlled.[5]

### A.8.2.2 Labelling of Information:

Information must be labeled to be easily followed and implemented effectively.[5]

### A.8.2.3 Handling of Assets:

Access restrictions must be considered in each classification which is a part of handling assets.[5]

## Annex A.9 Access Control (14 controls):

It ensures that each staff views only the information that is related to them, and divides it to 4 sections:

Section 1: Annex A.9.1: this is where the business requirements are being controlled. [1]

Section 2: Annex A.9.2:user access management. [1]

Section 3: Annex A.9.3: user responsibilities. [1]

Section 4: Annex A.9.4: system and application access controls. [1]

Only 7 controls will be used from Access Control which are:

### A.9.1.1 Access Control Policy:

It is the rules of who can access what and who needs to use it. Access control must be documented and reviewed on a regular basis based on the role change. Must be considered in the document, the responsibilities, and roles, and managing the rights of access. [6]

### A.9.1.2 Access to Networks and Network Services:

The users should know the network services and know who, when and what to access. [6]

### A.9.2.1 User Registration and Deregistration:

Each member of staff must have an individual ID to control the people who access the system. So, each group will access their own task without any complication. [6]

### A.9.2.2 User Access Provisioning:

Access and authorization to the information must be implemented and documented to verify the grant of access is relevant to the role. The users that have access to create, modify, or delete any information must have more protection since they access sensitive data and manage any risk. [6]

### A.9.2.5 Review of User Access Rights:

Owners must regularly review all access rights, so if any user has exited or moved, that must be changed in the system. The access rights must be up to date to reduce risks because any unchanged right will raise the attacker. [6]

### A.9.2.6 Removal or Adjustment of Access Rights:

In A.7 control, it makes a procedural change in the event of any change in the access rights. This control is where it tracks the procedural process with the recent access rights to avoid any confusion or risk that may come upon it. [6]

### A.9.4.1 Information Access Restriction:

Access control policy must provide control over role-based permissions, level of access, and authorization for modification. The auditor must review it to manage and limit any unauthorized access or reject any request without permission. [6]

## Annex A.11 Physical and Environmental Security (15 controls):

This section represents the physical and environmental security of an organization. It has two subsections which are:

Section 1: A.11.1: works to prevent unauthorized access, damage, and interference to buildings and critical data. [1]

Section 2: A.11.2: explicitly refers to equipment. It is intended to stop the theft, loss, or damage of containers holding information assets for an enterprise. [1]

### A.11.1.4 Protecting against External and Environmental Threats:

This control is where the description of how attacks, natural disasters, and accidents are prevented is found. Threats must be considered in all their forms, whether natural or man-made. Once the threat is identified, the auditor will try to search for evidence of the threat to solve it. [7]

## Annex A.13 Communications Security (7 controls):

This section is to protect the network from any attackers or intrusion. It is divided into two subsections which are:

Section 1: A.13.1: relates to network security management, which looks out for the confidentiality, availability, and integrity of data within those networks.[1]

Section 2: A.13.2: includes security when sending information to clients or other interested parties, whether they are inside or outside the firm.[1]

### A.13.1.1 Network Controls:

This control is to protect the information within the network; some operations must be considered such as designing and implementing how to secure the organization’s network. [8]

# Cybersecurity Attack Scenarios:

## Scenario 1: Administrative Branch:

In the administrative branch, there could be an attack on the servers or the computers. Using Annex A.11 control will help in protecting against the physical and environmental attacks that could lead to destruction, theft, or any failure. A.11.1.4, Protecting against External and Environmental Threats, is the control that will protect the information, and the auditor will have to identify the potential threats and find the corresponding evidence to treat them.

## Scenario 2: Students:

If a student uses his or her university password to register for an untrusted website, leading to an attack, and the password is known to the attacker, ISO 27001 has two controls that can prevent an unprivileged attacker from accessing any information. Firstly, A.9.4.2, Secure Log-on Procedures, manages access by using multi-factor authentication that can prove the identity of the student and prevent any attacker. Moreover, it uses other procedures, such as limiting the number of logs on trials, and any suspicious log on or off will be recorded as evidence to reach the attacker. Secondly, A.9.4.3, Password Management System, helps in creating strong passwords that can be hard to guess and helps in reducing the risk to the system.

## Scenario 3: Academic Staff:

Since the academic staff has the tasks of almost all the networks in the university, there could be an intrusion through the network to access the information, and the staff must have good training on how to manage it. So, ISO 27001 has a control in Section 13, A.13.1.1 Network Controls, where it provides connection control, endpoint verification, firewalls, and intrusion detection, which helps in protecting any transformation through the network.

# References:

[1] L. Irwin, “ISO 27001 annex a controls - A complete guide,” *IT Governance UK Blog*, 30-Mar-2023. [Online]. Available: <https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained>. [Accessed: 16-Apr-2023].

[2] “ISO 27001 – annex A.5: Information security policies,” *ISMS.online*. [Online]. Available: [https://www.isms.online/iso-27001/annex-a-5-information-security-policies/.](https://www.isms.online/iso-27001/annex-a-5-information-security-policies/.%20) [Accessed: 17-Apr-2023].

[3] “ISO 27001 – annex A.6: Organisation of Information Security,” *ISMS.online*. [Online]. Available: [https://www.isms.online/iso-27001/annex-a-6-organisation-information-security/](https://www.isms.online/iso-27001/annex-a-6-organisation-information-security/%20) [Accessed: 17-Apr-2023].

[4] “ISO 27001 – annex A.7: Human resource security,” *ISMS.online*. [Online]. Available: [https://www.isms.online/iso-27001/annex-a-7-human-resource-security/](https://www.isms.online/iso-27001/annex-a-7-human-resource-security/%20) [Accessed: 17-Apr-2023].

[5] “ISO 27001 – annex A.8: Asset management,” *ISMS.online*. [Online]. Available: <https://www.isms.online/iso-27001/annex-a-8-asset-management/> [Accessed: 17-Apr-2023].

[6] “ISO 27001 – annex A.9: Access control,” *ISMS.online*. [Online]. Available: <https://www.isms.online/iso-27001/annex-a-9-access-control/> [Accessed: 18-Apr-2023].

[7] “ISO 27001 – annex A.11: Physical & Environmental Security,” *ISMS.online*. [Online]. Available: <https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/> [Accessed: 17-Apr-2023].

[8] “ISO 27001 – annex A.13: Communications security,” *ISMS.online*. [Online]. Available: [https://www.isms.online/iso-27001/annex-a-13-communications-security/](%20https:/www.isms.online/iso-27001/annex-a-13-communications-security/) [Accessed: 17-Apr-2023].