NOVEMBER 1, 2022

ISO 27001: A BRIEF INTRODUCTION

WHITE PAPER BY AUUDITR

SARA AFTAB
AUUDITR
20-22 Wenlock Road, London, N1 7GU

Introduction

nformation Security these days is the main concern of businesses working globally. Modern methods of marketing include online presence of the companies and winning the trust of the customers. In a time when the global market is more available, it has gotten even harder to treat information and data as critical asset. ISO 27001 is the Information Security Management Systems (ISMS) that works as a framework to handle information and assets. It helps companies to manage the data security and evaluate their infrastructure in an organized manner.

ISO 27001, its contents, and the methodology needed to implement the protocol are further discussed in this paper. Moreover, the Auuditr's way of working and its approach is also discussed.

"In a time when the global market is more available, it has gotten even harder to treat information and data as critical asset. "

Key words: ISMS, ISO 27001, Information Security, Auuditr, Management Systems, Risk Management, Incident Management, Security Breach.

Context

ISO 27001 is developed for the organizations to us as reference for the implementation of Information Security Management System (ISMS), by giving you controls that can be implemented fully or depending upon the size and complexity of the organization, can be modified and selected controls can be implemented. All types of organizations whether public or private, commercial, or non-profit, deal with the creation, development, processing, and storage of information. The information can be either electronic or physical, verbal or written, and need to be dealt with considering Confidentiality, Integrity, and Availability. These attributes are covered in the ISO 27001 reference model.

The standard contains 14 security clauses, with 35 main security categories and 114 controls. Each clause contains one or few main security clauses. These clauses contain information about the controls that are critical to implement and legal requirements to fulfill the control demands.

ISMS mainly deals with the

- identification of assets on the level of criticality in terms of CIA (Confidentiality, Integrity, Availability),
- handling of tangible and intangible assets,
- retention of the information
- storing and backup of data

- access control and management
- risk management
- problem management
- service availability
- supplier management

The requirements of the clauses can be modified according to the scope of the organization. Organizations may not want to implement to the whole rather its parts. Scoping helps to understand the clauses that must be implemented to achieve certification.

Who can achieve ISO 27001?

> "Digital companies, software houses, internet service providers, website hosting services etc. can be the example of companies that need this certification the most."

ISO 27001 framework is for all, whether the company is a service provider or manufacturer, public or private and non-profit. Yet it seems more useful for organizations that are handling the customer data and information or acting a third-party service for other businesses need to achieve this standard the most. Digital companies, software houses, internet service providers, website hosting services etc. can be the example of companies that need this certification the most. ISMS certification not only helps you manage the information assets but also prove that your organization is trustworthy. Among other competitors, this standard gives you the benefit of tested and certified system.

ISO 27001 has become increasingly important for the organization in this age of data breaches and cyber threats.

- Organizations go for this standard because most of the times it is the

requirements of their clients to protect their data.

- By achieving ISMS, it becomes easier to be compliant with legal or regulatory data protection acts that are enforced in various countries.
- ISMS makes your organization one step ahead of other competitors by giving you a management system that ensures data security.

Content of standard requirements

The structure of the requirement as stated previously is divided into 14 Clauses and related 114 Controls. The clauses are related to the following:

1. **Information Security Policies**
   The objective of this clause is to provide direction and support related to information security to the followers of the policy. Policy making helps the management to understand the set of rules to be followed.

2. **Organization of Information Security**
   The purpose is to establish framework to initiate implementation and operations related to information security.

3. **Human Resource Security**
   The objective is to ensure that employees understand their responsibility and their strengths are appropriate for their role.

4. **Asset Management**
   The objective is to identify organizational assets and segregate them into appropriate protection required. Asset management is a major clause that not only identifies the

assets but classifies, handles, labels and gives the appropriate management of disposal as well.

5. **Access Control**
   The objective of this clause is to not only protect information but also limit the access according to the identified roles in the organization. It handles everything related to access from registration of user to the privileges management.

6. **Cryptography**
   The main purpose this clause is to ensure the effective use of cryptography to protect the information from unwanted access and retain authenticity.

7. **Physical and Environmental Security**
   One of the information security protocols is to maintain the physical security using ways to upkeep the information security in the facility.

8. **Operations Security**
   The main purpose is to ensure the secure operations of information processing facilities. This clause also ensures the capacity management, a proper change management and ensure a safe development, testing and operational environment.

9. **Communications Security**
   The main purpose is to ensure that networks and connections are protected within the facility. It further deals with the network security, information transfer, electronic messaging and non-disclosure agreement.

10. **System Acquisition, development, and Maintenance**
    The objective of this clause is to ensure the secure application services, secure development, and regular maintenance activities.

11. **Supplier Relationships**
    The objective of this is to protect the organization's assets that are directly handled by the suppliers.

12. **Incident Management**
    The objective of this clause is to ensure that the management of security incidents related to information and communication related to security breaches.

13. **Information Security Aspects of Business Continuity Management**
    The main purpose of this clause is to ensure information security while maintaining business continuity during downtime.

14. **Compliance**
    The objective is to avoid breaches legal, regulatory, or contractual obligations to maintain information security.

These related controls are categorized as in the following example:

- **A.5 Information Security Policies**
  - A.5.1 Management direction for information security
    - A.5.1.1 Policies for information security
    - A.5.1.2 Review of the policies for information security

Further information of these controls can be found in implementation guides of these standards.

Services Offered by Auuditr

We as a consultancy firm, offer our team that has the expertise to develop processes and management methods to ensure information security in the organizations. We offer the following services:

- Gap assessment sessions to find out the capability of the organization to achieve the ISO 27001
- A statement of applicability
- Policies and procedure guidelines
- Consultancy sessions
- Tools & templates guidelines

In conclusion, ISO 27001 is a comprehensive framework for managing information security in depth. Auuditr is here to help you in detail with the complex development and implementation of the standard. Our team is well equipped to understand the detail your organization chooses to go into the standard and makes the standard into implementable portions of processes that can be followed.

Further information on

www.Auuditr.com