Introduction to ISO 27001

ISO 27001 is a globally recognized standard that provides a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

Perera R.Y IT22552488

What is ISO 27001?

Standard

ISO 27001 is an internationally recognized standard that outlines best practices for information security management.

Framework

It provides a comprehensive framework for organizations to protect their confidential, sensitive, and critical information.

Management System

The standard helps organizations develop and maintain a robust Information Security Management System (ISMS) to manage information security risks.

Benefits of ISO 27001 Certification

1

Enhanced Security

ISO 27001 certification demonstrates a commitment to information security and helps organizations minimize risks.

2

Increased Trust

Certification builds trust with customers, partners, and stakeholders, proving a company's security measures are robust.

3

Competitive Advantage

ISO 27001 certification can give organizations a competitive edge by demonstrating their commitment to information security.

ISO 27001 Requirements

Risk Management

Organizations must identify, assess, and mitigate information security risks.

Control Implementation

Implement controls to address identified risks and ensure the effectiveness of the ISMS.

Documentation and Review

Maintain documentation of the ISMS and regularly review its effectiveness.

The ISMS (Information Security Management System)

1

Policy and Objectives

Establish a clear information security policy and define specific security objectives.

2

Risk Assessment

Identify and evaluate potential information security risks and vulnerabilities.

3

Control Selection

Choose appropriate controls to mitigate identified risks.

4

Implementation and Monitoring

Implement controls and monitor their effectiveness on an ongoing basis.

5

Review and Improvement

Regularly review the ISMS and make improvements to ensure its effectiveness.

Risk Management

1

Identification

Identify potential threats and vulnerabilities that could impact information security.

2

Assessment

Evaluate the likelihood and impact of each identified risk.

3

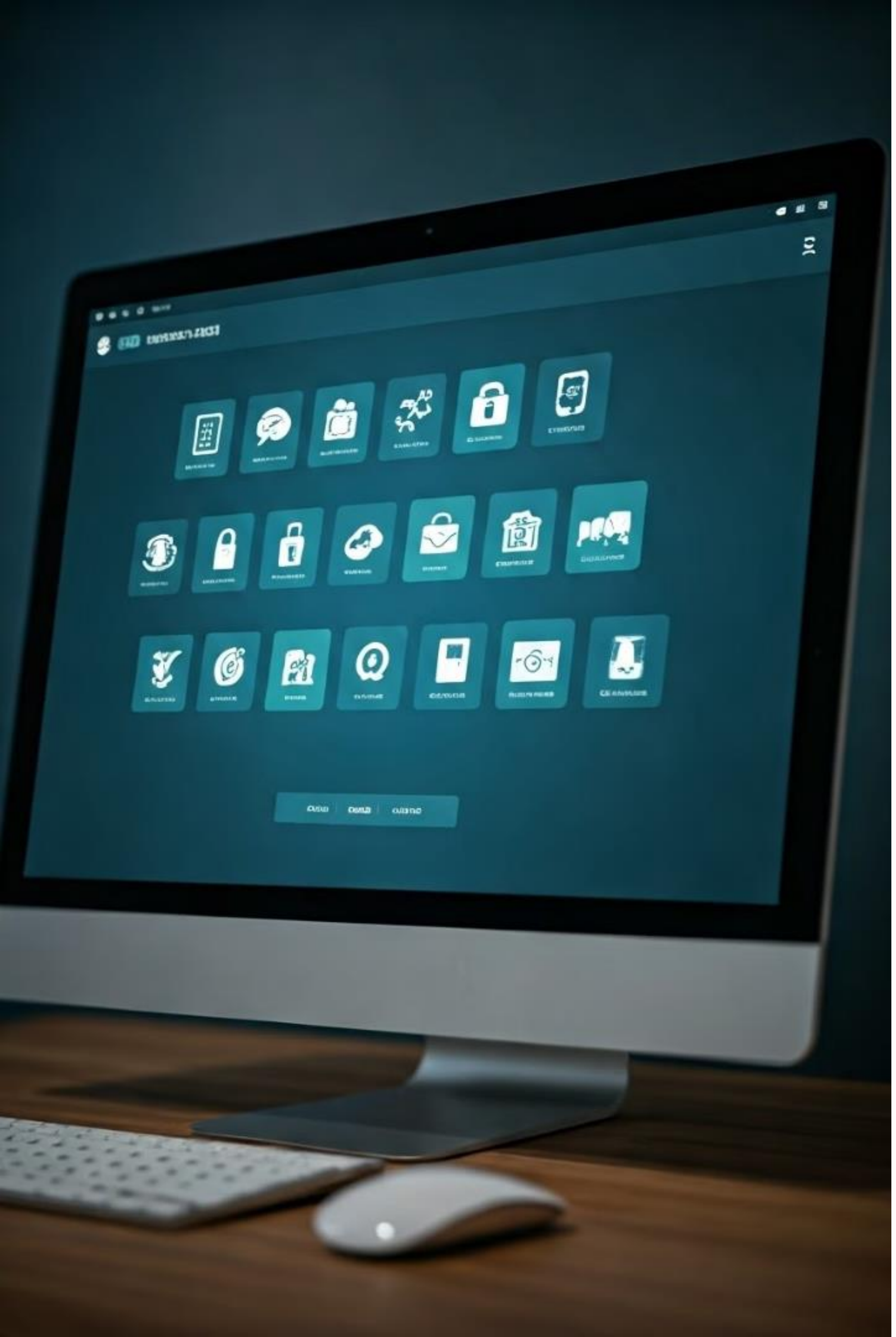
Mitigation

Develop and implement appropriate controls to mitigate risks.

4

Monitoring

Continuously monitor risks and adjust controls as needed.



Controls and Implementation

Technical Controls	Access Control	Encryption	Antivirus Software
Organizational Controls	Security Policies	Employee Training	Incident Response Plan
Physical Controls	Building Security	Access Badges	CCTV

Documentation and Record-Keeping

Policies and Procedures

Document all information security policies, procedures, and guidelines.

Risk Assessments

Maintain records of risk assessments, including identified risks and mitigation plans.

Audits and Reviews

Document the results of internal audits and management reviews.

Incident Reports

Record details of any security incidents, including responses and corrective actions.

Certification Process and Maintenance

1

Gap Analysis

Identify any discrepancies between the organization's existing practices and ISO 27001 requirements.

2

ISMS Implementation

Implement the necessary controls and documentation to meet the standard's requirements.

3

Certification Audit

A third-party auditor assesses the organization's ISMS to ensure compliance with ISO 27001.

4

Certification

Upon successful completion of the audit, the organization receives ISO 27001 certification.

5

Surveillance Audits

Regular surveillance audits ensure continued compliance and maintain the validity of the certification.