INFORMATION SECURITY

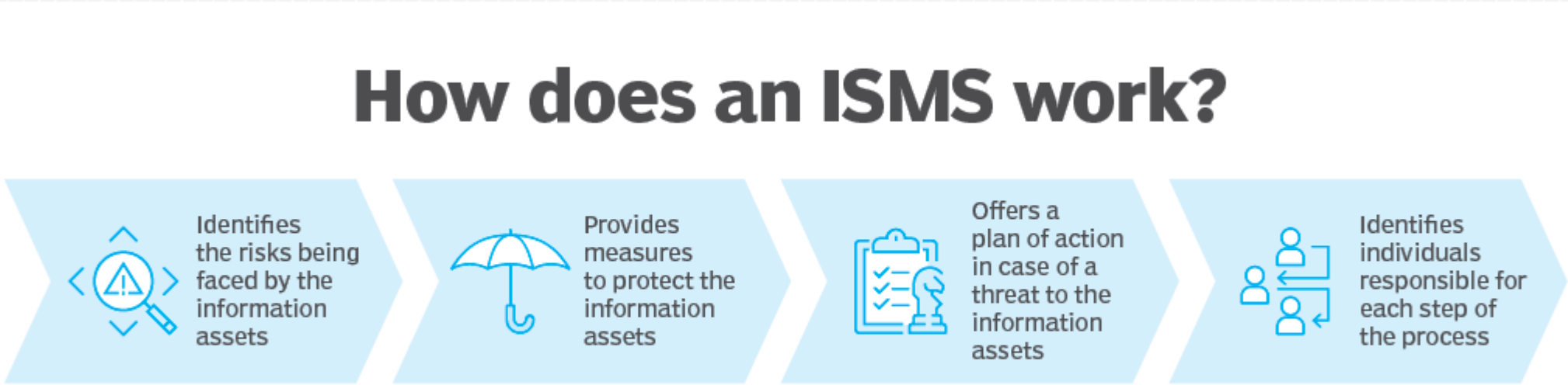
INTRODUCTION TO ISMS, NSIT AND ISO 27001 STANDARD

What is Information Security Management System (ISMS)?

An **Information Security Management System (ISMS)** is a set of objectives and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by proactively limiting the impact of a security breach.

It usually target a particular type of data, such as customer data or it can be implemented in a comprehensive way that becomes part of the company's culture.

How does ISMS work?



Benefits of ISMS?

- Protects sensitive data
- Meet regulatory compliance
- Provides business continuity
- Reduces cost
- Adapt to emerging threats

Introduction to ISO 27001

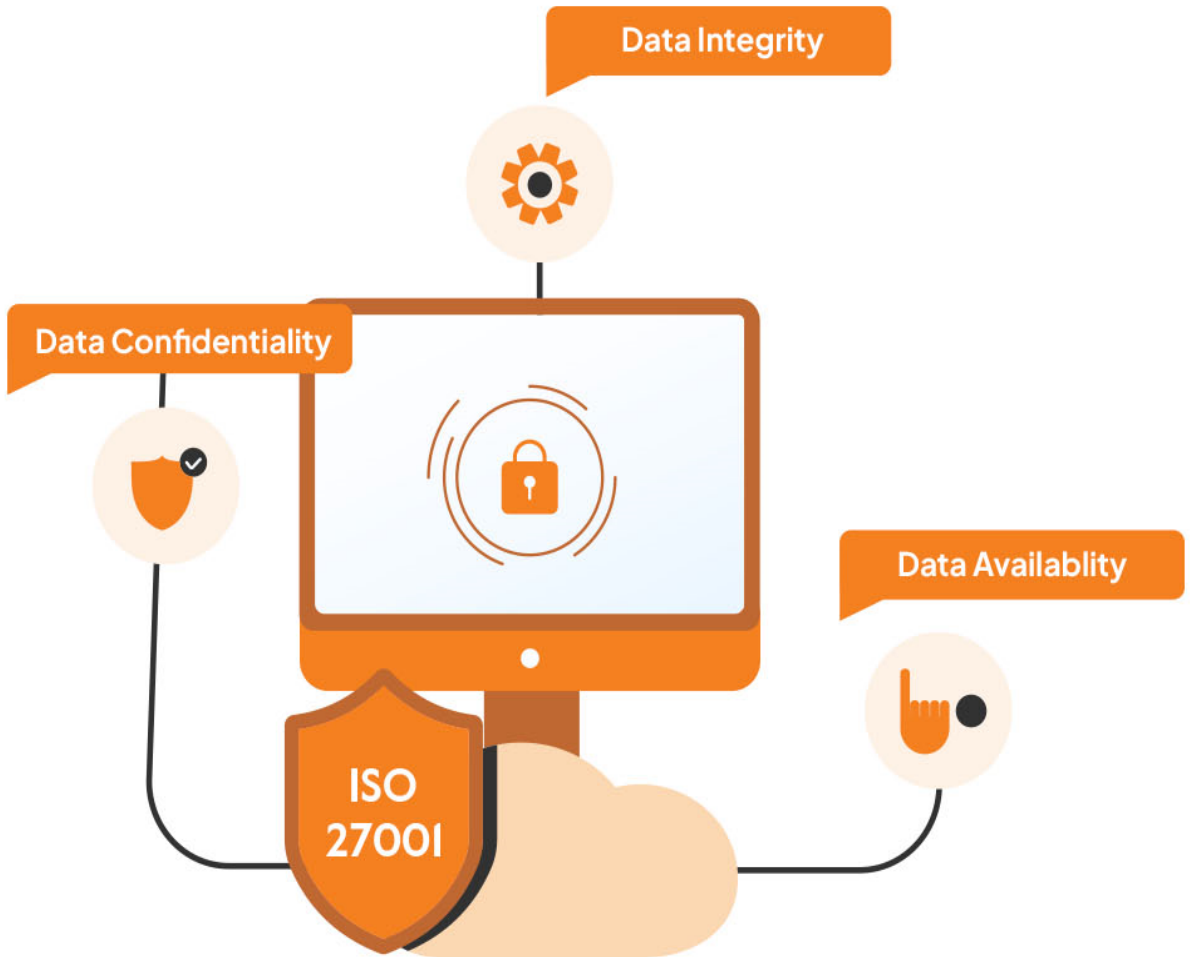
What is ISO 27001?

ISO 27001 is the leading international standard focused on information security. ISO 27001 is published by the International Organization for Standardization (ISO) in partnership with the International Electrotechnical Commission (IEC). Its based on the "**plan - do - check - act (pdca) cycle".**

ISO 27001 standard is a set of requirements for defining, implementing, operating and improving an ISMS. ISO 27001 provides a company with the necessary know-how for protecting their most valuable information, and also a company can get certified against ISO 27001 and in this way prove to its customers and clients that it safeguards their data.

ISO 27001 Principles

- Confidentiality of data
- Integrity of data
- Availability of data

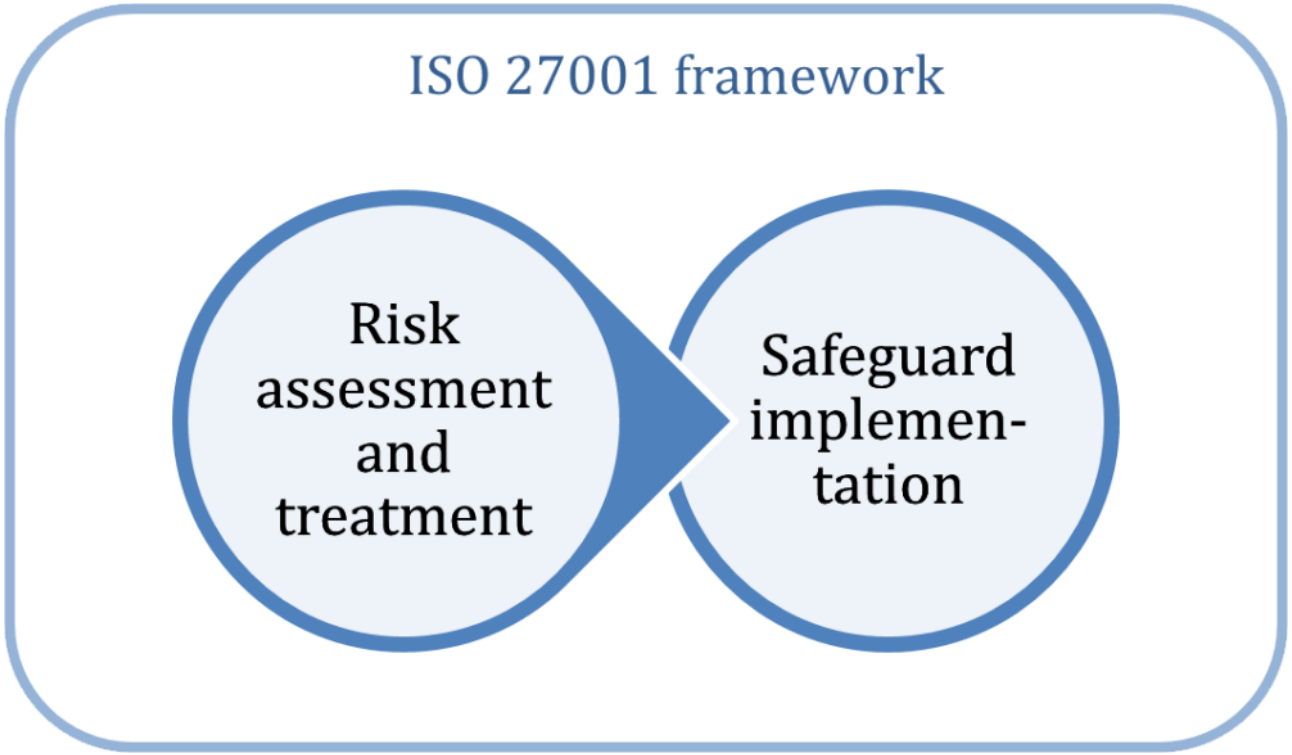


How does ISO 27001 work?

1. **Risk management**: finding out what potential incidents could happen to the information.

2. **Risk treatment/mitigation:** defining what needs to be done to prevent such incidents from happening.

3. **Safeguard implementation**



Controls in ISO 27001

- **Organizational controls:** are implemented by defining the rules to be followed as well as expected behaviour from users, equipment, software, and systems. e.g. Access control policy.
- **People controls:** are implemented by providing knowledge, education, skills or experience to persons to enable them to perform their activities in a a secure way. e.g. ISO 27001 awareness training
- **Physical controls:** are primarily implemented by using equipment or devices that have a physical interactions with people and objects e.g. CCTV cameras, alarm systems etc.
- **Technological controls:** are primarily implemented in information system using software, hardware and firmware components added to the system e.g. backup, antivirus software.

Benefits of ISO 27001

- Resilience of cyber-attacks
- Preparedness for new and existing threats
- Data integrity, confidentiality and availability
- Security across all supports
- Organization-wide protection
- Cost savings

NIST CYBERSECURITY FRAMEWORK

What is the NIST Cybersecurity Framework?

NIST CSF is a set of best practices, standards, and recommendations that help an organization improve its cybersecurity measures. The standards was compiled by National Institute of Standards and Technology (NIST) after former United States President Barack Obama signed an executive order in 2014.

The Framework consolidates industry standards and best practices to guide organizations in managing their cybersecurity risks. It helps companies reduce cybersecurity threats as well as respond to and recover from incidents.

Core Functions of NIST Cybersecurity Framework

- **Identify:** To protect against cyber attacks, the cyber security team needs a thorough understanding of what are the most important assets and resources of the organization. This function includes categories such as risk assessment, assets management etc

- **Protect:** The protect function covers much of the technical and physical security controls for developing and implementing appropriate safeguards and protecting critical infrastructure. This includes awareness and training, data security, maintenance etc

- **Detect:** The detect function implements measures that alert an organization to cyber attacks. Includes anomalies and events, security continuous monitoring and detection processes.

Functions of NIST (cont'd)

- **Respond:** The respond function categories ensure the appropriate response to cyberattacks and other cybersecurity events. Categories include response planning, communications, analysis, mitigation etc

- **Recover:** Recovery activities implement plans for cyber resilience and ensure business continuity in the event of a cyberattack, security breach, or other cybersecurity event.

Uses of NIST Cybersecurity Framework

- to determine current levels of implemented cybersecurity measures by creating a profile;
- to identify new potential cybersecurity standards and policies;
- to communicate new requirements; and
- to create a new cybersecurity program and requirements.

Differences and Similarities of ISO 27001 and NSIT Framework

SIMILARITIES:

At their core, both **NIST and ISO 27001** have the same purpose: to protect an organization's data and cybersecurity. This affects not only your organization but the clients, customers, and partners that you do business with.

By complying with ISO 27001, your company demonstrates that it is capable of responsibly handling data at the international level. The NIST framework us used to measure the maturity of your program against a set of outcomes it defines.

Differences and Similarities of ISO 27001 and NSIT Framework (cont'd)

DIFFERENCES:

NIST is a set of recommendation and standards to help organizations for cybersecurity threats and ways to recover from them. As every organization is different, NSIT is used as a baseline for how to create a cybersecurity program.

ISO 27001 was designed for international use throughout all sectors. To be ISO 27001 complaint you need certified with ISO 27001 compliance certificate.

THANK YOU FOR YOUR TIME AND ENJOY THE REST OF YOUR DAY

Chop life - AgbaCooker

References

- https://advisera.com/27001academy/what-is-iso-27001/
- https://www.iso.org/standard/27001
- https://www.techtarget.com/searchsecurity/definition/NIST-Cybersecurity-Framework
- https://advisera.com/27001academy/what-is-iso-27001/
- https://www.isms.online/iso-27001/
- https://www.globalsuitesolutions.com/what-is-the-iso-27001-standard-and-what-is-its-purpose/