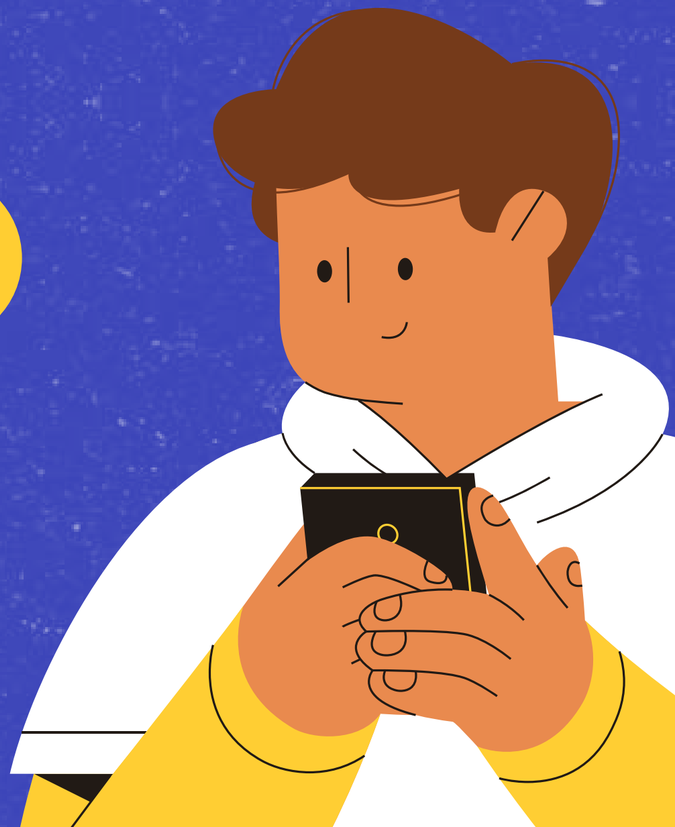
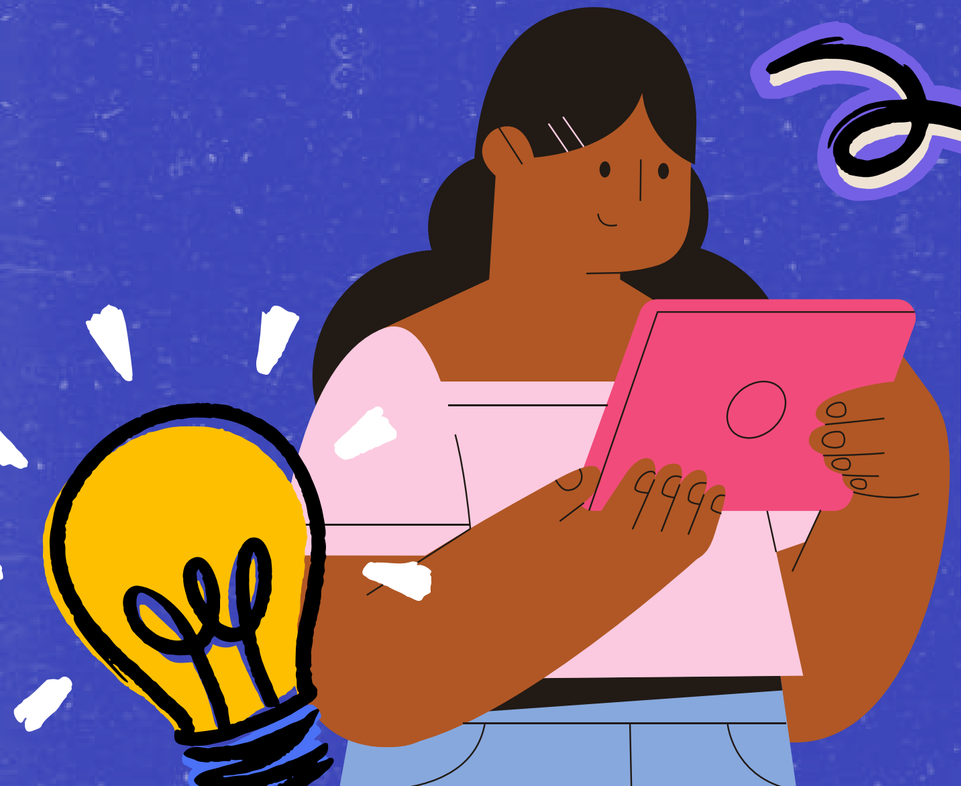
ISO 27001 AND FRIENDS: YOUR ULTIMATE SECURITY SQUAD

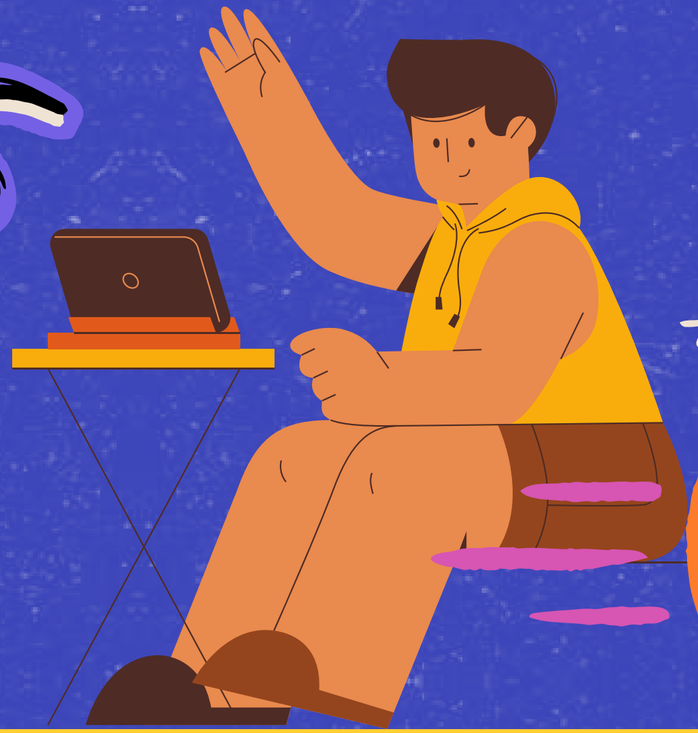
Enter the ISO 27001 Galaxy



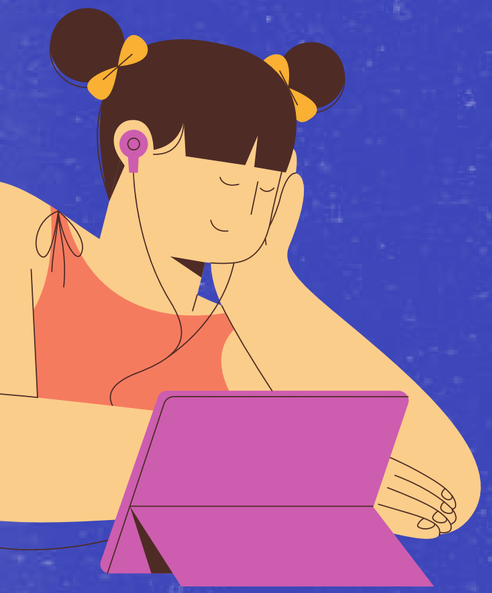
LIST OF CONTENTS

01.





STANDARDS SPECIFYING REQUIREMENTS



ISO/IEC 27001

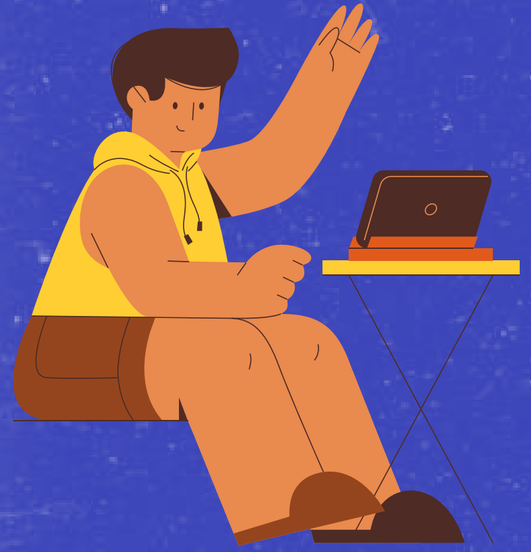
INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS

Overview

ISO/IEC 27001:2022 is an international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

Purpose

The primary purpose of ISO 27001:2022 is to help organizations Establish and implement a robust ISMS to protect their information assets and identify, assess, and treat information security risks effectively.



ISO/IEC 27006

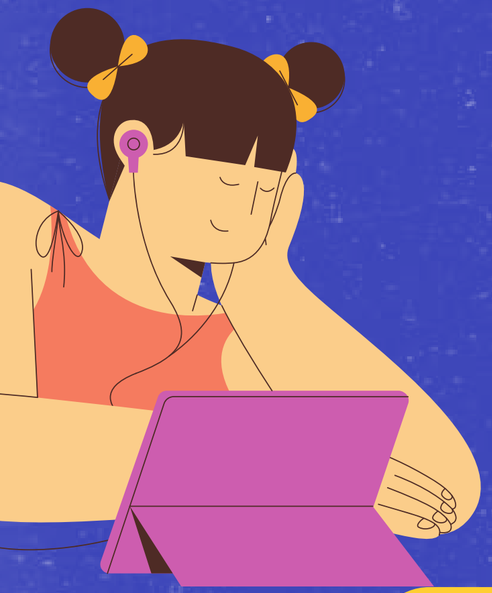
INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS

Overview

ISO/IEC 27006 provides requirements and guidance for bodies that audit and certify Information Security Management Systems (ISMS) against ISO/IEC 27001.

Purpose

The primary purpose of ISO/IEC 27006 is to ensure the consistency and reliability of ISMS certifications & provide a framework for certifying bodies to demonstrate their competence in auditing and certifying ISMS.



ISO/IEC 27009

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — SECTOR-SPECIFIC APPLICATION OF ISO/IEC 27001 — REQUIREMENTS

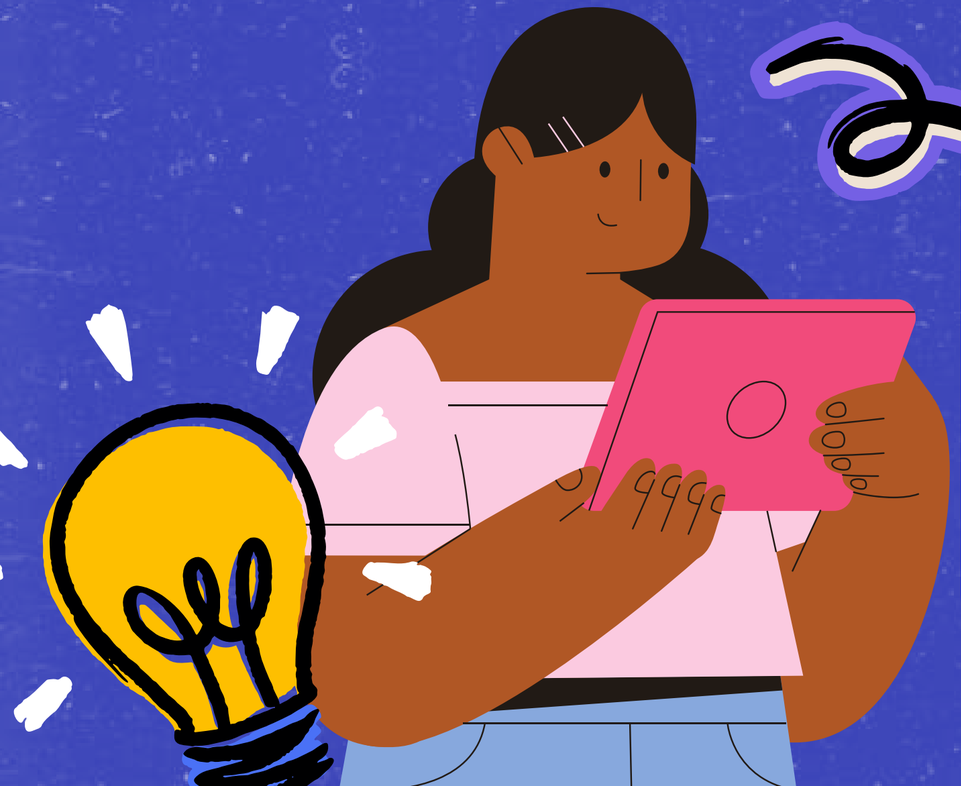
Overview

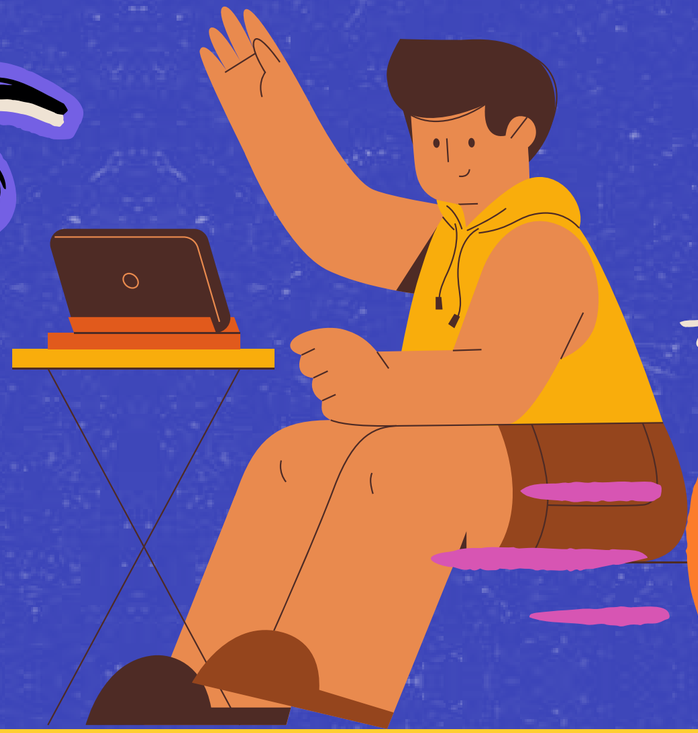
ISO/IEC 27009 provides a framework for developing sector-specific standards that complement or amend ISO/IEC 27002, the code of practice for information security controls.

Purpose

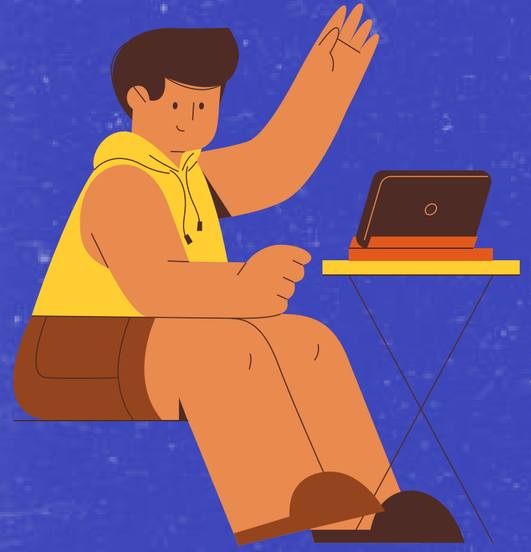
The primary purpose of ISO/IEC 27009 is to enable the development of tailored information security standards for specific sectors and ensure that sector-specific standards align with the broader ISO/IEC 27000 family of standards.

02.





STANDARDS DESCRIBING GENERAL GUIDELINES



ISO/IEC 27002

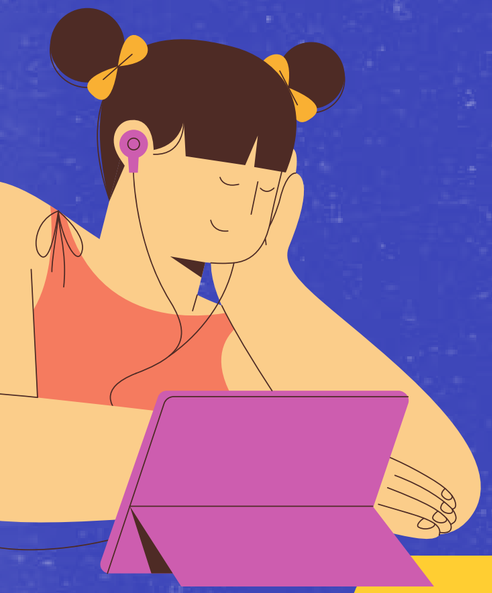
INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

Overview

ISO/IEC 27002 provides a comprehensive set of information security controls, offering guidance on their selection, implementation, and management. It serves as a practical tool for organizations to protect their information assets by addressing a wide range of security risks.

Purpose

The primary purpose of ISO/IEC 27002 is to provide a catalogue of information security controls for organizations to select from and offer guidance on the implementation and management of these controls.



ISO/IEC 27003

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT —GUIDANCE

Overview

ISO/IEC 27003 is a practical roadmap for organizations to implement an Information Security Management System (ISMS). It provides step-by-step guidance, best practices, and recommendations to help businesses effectively apply the requirements outlined in ISO/IEC 27001.

Purpose

The primary purpose of ISO/IEC 27003 is to support organizations in implementing an ISMS and provide practical advice and recommendations for various stages of the ISMS implementation process.

ISO/IEC 27004

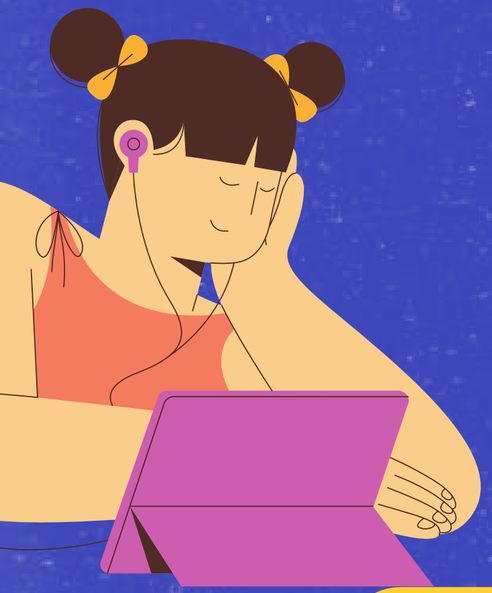
INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT — MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

Overview

ISO/IEC 27004 provides guidance for measuring how well an organization's information security system is performing. It helps businesses understand if their security measures are effective and where improvements can be made.

Purpose

- The primary purpose of ISO/IEC 27004 is to assist organizations in evaluating the performance of their ISMS and provide a structured approach to measuring information security metrics.



ISO/IEC 27005

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY RISK MANAGEMENT

Overview

ISO/IEC 27005 provides a framework for information security risk management. It offers guidance on identifying, assessing, evaluating, treating, and monitoring information security risks.

Purpose

The primary purpose of ISO/IEC 27005 is to assist organizations in establishing and maintaining an effective information security risk management process and to provide a structured approach to identifying and assessing information security risks

ISO/IEC 27007

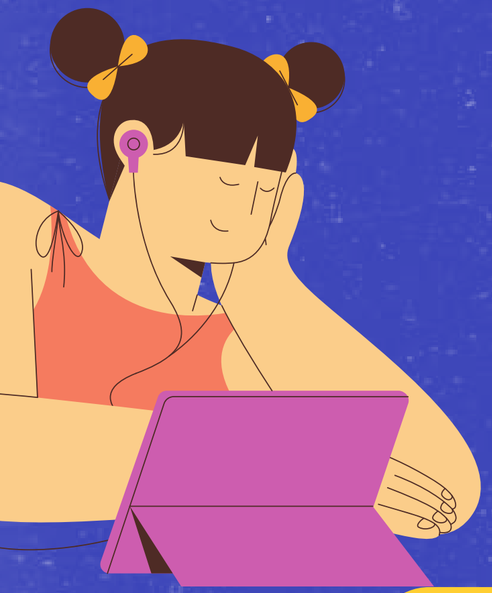
INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — GUIDELINES FOR INFORMATION SECURITY MANAGEMENT SYSTEMS AUDITING

Overview

ISO/IEC 27007 provides guidelines for assessing the health of an organization's information security system. It provides step-by-step instructions on how to conduct thorough audits, identify strengths and weaknesses, and recommend improvements.

Purpose

The primary purpose of ISO/IEC 27007 is to provide a framework for conducting effective ISMS audits and assist organizations in assessing the compliance of their ISMS with ISO/IEC 27001 and other relevant standards.



ISO/IEC 27013

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — GUIDANCE ON THE INTEGRATED IMPLEMENTATION OF ISO/IEC 27001 AND ISO/IEC 20000-1

Overview

ISO/IEC 27013 provides guidance for merging information security (ISO/IEC 27001) and IT service management (ISO/IEC 20000-1) systems. It helps organizations streamline operations, save money, and improve overall performance.

Purpose

The primary purpose of ISO/IEC 27013 is to assist organizations in integrating ISMS and SMS for optimal efficiency and to provide guidance on aligning information security and service management processes.

ISO/IEC 27014

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — GOVERNANCE OF INFORMATION SECURITY

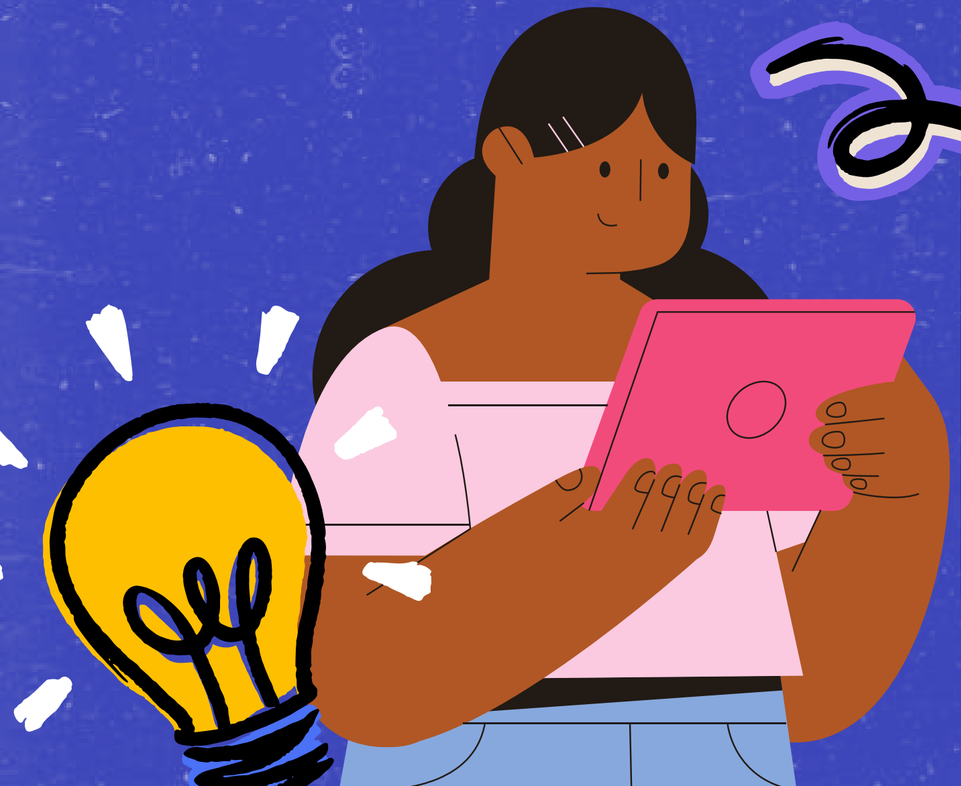
Overview

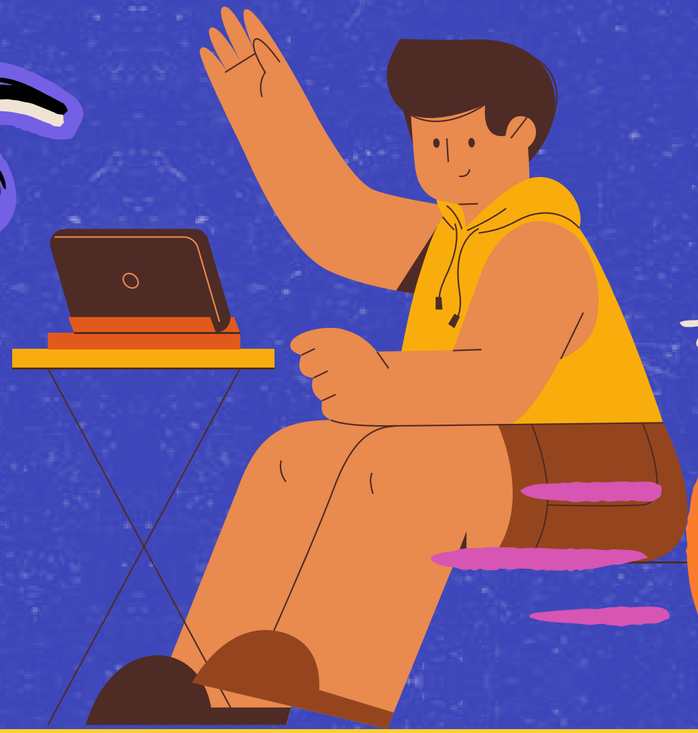
ISO/IEC 27014 provides guidelines for information security governance. It outlines principles, objectives, and procedures for organizations to evaluate, direct, monitor, and communicate information security-related processes

Purpose

The primary purpose of ISO/IEC 27014 is to assist organizations in establishing effective information security governance and provide guidance on aligning information security with organizational strategy.

03.





STANDARDS DESCRIBING SECTOR-SPECIFIC GUIDELINES

ISO/IEC 27021

INFORMATION TECHNOLOGY — INFORMATION SECURITY MANAGEMENT — COMPETENCE REQUIREMENTS FOR INFORMATION SECURITY MANAGEMENT SYSTEMS PROFESSIONALS

Overview

ISO/IEC 27021 outlines the skills and knowledge needed to be an effective information security manager. It sets the standard for professionals responsible for building, maintaining, and improving an organization's information security system.

Purpose

The primary purpose of ISO/IEC 27021 is to define the competence requirements for ISMS professionals and provide a framework for developing training and certification programs for ISMS professionals.

ISO/IEC 27011

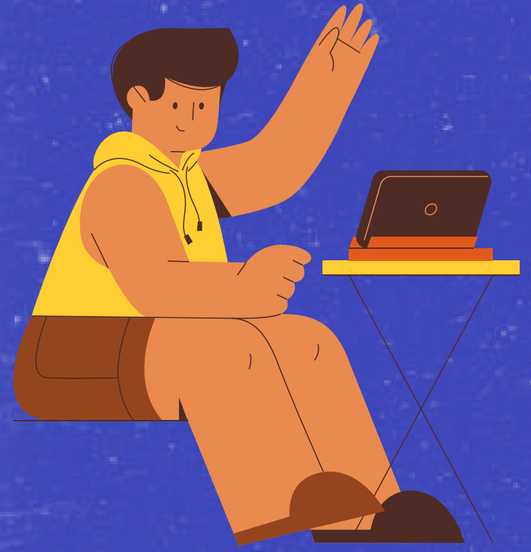
INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS BASED ON ISO/IEC 27002 FOR TELECOMMUNICATIONS ORGANIZATIONS

Overview

ISO/IEC 27011 is a specialized guide for securing telecommunications. It builds on general security principles and offers specific advice for protecting networks, systems, and customer data in the telecom industry.

Purpose

The primary purpose of ISO/IEC 27011 is to assist telecommunications organizations in implementing information security management systems and Provide specific security controls and guidance tailored to the telecommunications sector.



ISO/IEC 27017

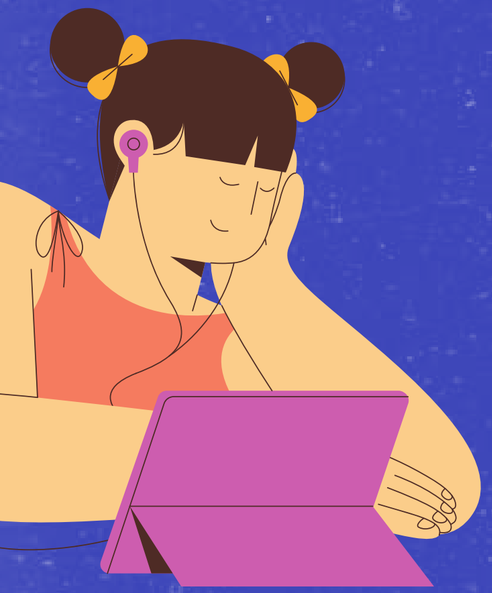
INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS BASED ON ISO/IEC 27002 FOR CLOUD SERVICES

Overview

ISO/IEC 27017 is a specialized guide for securing cloud services. It offers specific security controls and best practices to protect data privacy, ensure uninterrupted service, and clarify responsibilities between cloud providers and customers.

Purpose

The primary purpose of ISO/IEC 27017 is to assist organizations in implementing information security controls within cloud environments and provide specific guidance for both cloud service providers and cloud service consumers.



ISO/IEC 27018

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) IN PUBLIC CLOUDS ACTING AS PII PROCESSORS

Overview

ISO/IEC 27018 enhances ISO/IEC 27002 by providing specific guidelines and controls for protecting Personally Identifiable Information (PII) in public clouds. It aims to guide cloud service providers, improve personal data protection, and build trust among users.

Purpose

The primary purpose of ISO/IEC 27018 is to provide specific guidance for cloud service providers handling PII, Enhance the protection of personal data in public cloud environments and Build trust and confidence among cloud service users.

ISO/IEC 27019

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY CONTROLS FOR THE ENERGY UTILITY INDUSTRY

Overview

ISO/IEC 27019 is a security blueprint specifically designed for the energy industry. It builds on general security practices to address the unique risks faced by power generation, transmission, and distribution companies.

Purpose

The primary purpose of ISO/IEC 27019 is to assist energy utility organizations in implementing information security management systems and provide specific security controls and guidance tailored to the energy industry.

THANK YOU

CLICK HERE TO JOIN OUR MOS UNIVERSITY COMMUNITY FOR EXCLUSIVE TRAINING PROGRAMS TO BECOME A CYBERSEC PRO!