KPMG

Understanding ISO 27001:2022: People, process, and technology

The importance of information security management systems in the life sciences industry

kpmg.com/us

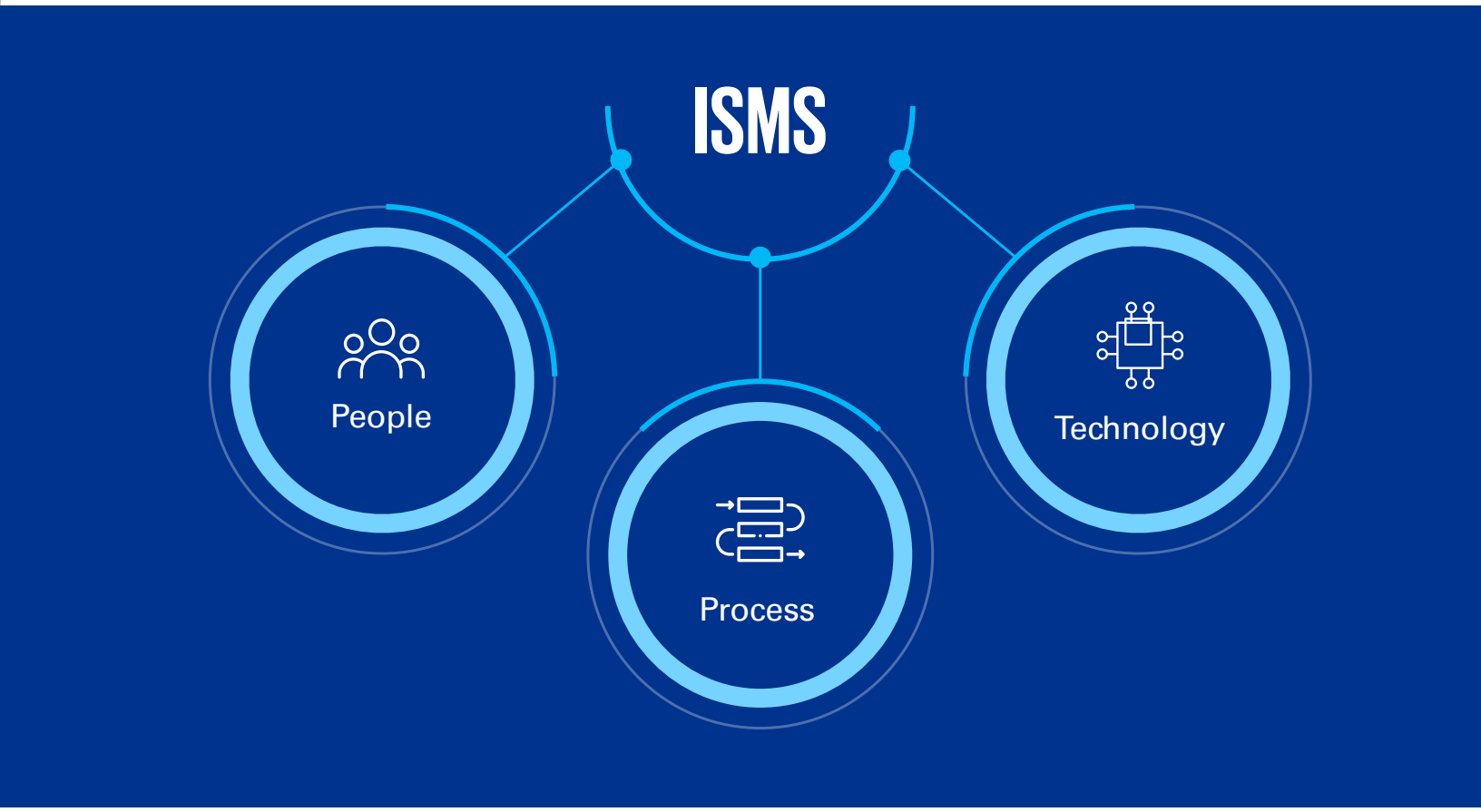
Introduction

As the risks associated with cyberattacks and data breaches continue to increase, information security has become a critical issue for the life sciences industry. An effective approach should help defend against both external attacks and common internal threats. That is why the world of information security management systems (ISMS) has become so important.

What is an ISMS?

An ISMS is a framework of policies and procedures for systematically managing an organization's sensitive data.

An ISMS includes the people, process, and technology that are designed to protect against unauthorized access, use, disclosure, disruption, modification, or destruction of information. It also supports and demonstrates that security is appropriately managed across numerous areas, including operations, financial information, intellectual property, employee details, or information entrusted from third parties.



An overview of ISO 27001

ISO 27001 is the international standard that provides the specification for an ISMS. This is a systematic approach consisting of people, process, and technology that helps you protect and manage all your organization's information through risk management. ISO/IEC 27001 is a primary ISO standard that aims to enhance the security of an organization's information[1, 2]. ISO/IEC 27001 provides a framework to assist organizations in managing information security, while ISO/IEC 27002 provides implementation guidance for information security controls specified in ISO/IEC 27001.

Pharmaceuticals, biotech, and medical devices, as well as many other sectors within the life sciences industry[3], are required to adhere to numerous laws and regulations. It is highly recommended to implement ISO 27001 in these industries as a compliance threshold, and it is easy to present these projects to executives. The data protection legislation is primarily based on ISO 27001 standard[4], which supports these organizations to strengthen their cybersecurity posture.

ISO 27000 Family of Standards					
For Auditees and Auditors				For Auditors	
Requirements	**Guidance**	**Extension(s)**	**Key Processes**	**Requirements**	**Guidance**
ISO/IEC 27001 Information Security Management System (ISMS)	**ISO 27003** Implementation Guide	ISO 27017 Additional Guidance and Controls for CLOUD	ISO 27005 Information Security Risk Management	ISO 17021-1 Requirements for Certification Bodies providing certification of Management System	ISO 19011 Guidelines for auditing Management System
		ISO 27018 Additional Guidance and Controls for CLOUD as PII Processors	ISO 27004 Information Security Measurement (i.e. monitoring of ISMS)		
ISO/IEC 27001 ISMS ANNEX A Reference Control Objectives and Controls	**ISO 27002** Detailed Implementation Guidance	ISO 27701 Privacy Information Management System (PIMS)	ISO 27036 Information Security for Supplier Relationship (Vendor Management)	ISO 27006 Requirement for Certification Bodies for ISMS	ISO 27007 Additional Guidelines for auditing ISMS
			ISO 27035 Security Incident Management		

[1]Source: Forbes, Drolet, Michelle (March 23, 2022)
[2]Source: Yahoo Finance, PR Newswire (July 12, 2023)
[3]Source: Bloomberg, Business section (March 8, 2022)
[4]Source: Microsoft, Microsoft Compliance section (April 19, 2023)

What is new with ISO 27001:2022?

As the life sciences industry is facing new evolving security threats and challenges, the ISO/IEC 27001:2013 has been updated to a new, more relevant, and up-to-date edition. The new version of the standard[5,6] that reflects changes to the ISMS framework design and guidance to enhance organizational security posture was published in October 2022[7].

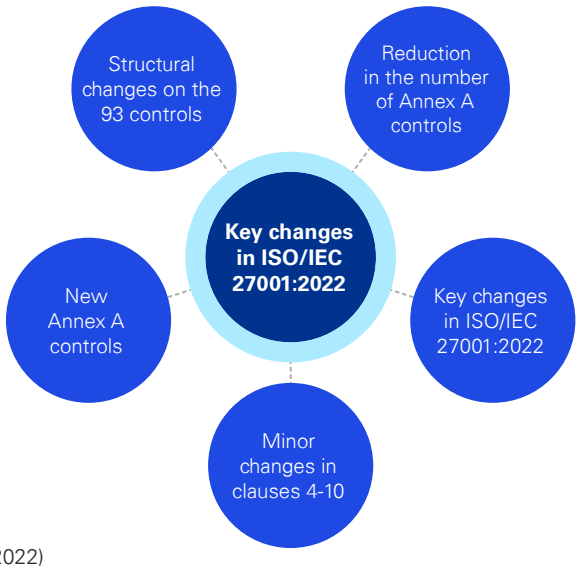
ISO 27001:2022 focuses on protecting three key aspects of information: **confidentiality, integrity,** and **availability.**

Confidentiality means that the information is not available or disclosed to unauthorized people entities or processes.

Integrity means that the information is complete, accurate, and protected from corruption.

Availability means that the information is accessible and usable as and when authorized users require it.

The number of information security controls has been reduced from 114 to 93. However, reduction of controls is primarily because of the merging of requirements and no control has been removed. The controls have been structured into four categories (people, technological, physical, and organizational) to simplify and streamline the process of selecting and implementing security controls.



Current control domains of ISO 27001:2022[8]

People
08
controls

Physical
14
controls

Technology
34
controls

Organizational
37
controls

[5]Source: Forbes, Drolet, Michelle (March 23, 2022)
[6]Source: Bloomberg, Business section (March 8, 2022)
[7]Source: Microsoft, Microsoft Compliance section (April 19, 2023)
[8]Source: ISO Annual Meeting 2023

The value of an ISO 27001:2022 certification

01 Helps address potential regulatory expectations

ISO 27001 can help organizations comply with a host of laws including the high-profile General Data Protection Regulation, commonly referred to as the GDPR[9], and the network and information systems regulations, also known as the NIS regulations.

02 Provides trust to customers during contracting

By obtaining ISO 27001 certification, an organization demonstrates to its customers, partners, and stakeholders that information security is an upmost priority and has implemented rigorous measures to protect sensitive data[10]. This can serve as a competitive advantage and set your organization apart from others in its industry.

Achieving ISO 27001 certification provides companies with compliance with the requirements of the standard itself. This not only instills customer confidence but also meets the compliance frameworks that various industries require. By following the ISO standard, companies are getting a benchmark that results in regular assessment and improvement of their risk management strategy.

03 Reduces complexity of other ISO certifications

ISO 27001 certification reduces complexities associated with other certifications from within ISO family of standards and other related international standards.

04 Provides a company with greater visibility of high-risk cyber areas

The certification process involves a systematic risk assessment of the organization's information assets and associated threats. This identification and assessment of risk areas help prioritize the security controls and focus its resources on protecting the most vulnerable areas. This approach enables organizations to establish clear priorities for mitigation and investment, as the standard requires regular risk assessments and risk treatment plans. This ongoing review of risks helps to ensure that an organization's security strategy aligns with its business objectives. As a result, an organization is enabled to make informed decisions on which security controls to invest in and which risks to accept.

[9]Source: Microsoft, Microsoft Compliance section (April 19, 2023)
[10]Source: Yahoo Finance, PR Newswire (July 12, 2023)

Why KPMG and how we can help?

KPMG LLP has a wide array of knowledge of the life sciences sector and a robust résumé of prior work on ISO 27001:2022. The teams within our Compliance practice understand the technology landscape, target operating model, and ISO 27001 compliance requirements. The KPMG brand performing ISO work is internationally recognized. We have the experience of certifying numerous global organizations, which allows us to bring practical solutions and accelerate efforts. Working with KPMG can help to yield accelerated outputs and minimize implementation times. Our existing accelerators, toolkits, and knowledge allow us to rapidly start engagements and deliver intended results.

KPMG can proactively partner with you in the implementation of ISO 27001:2022 before the September 2025 due date. Through a streamlined and customized process, we will take your organization from a readiness assessment to audit preparedness. Our three-phased preparation approach for ISO 27001 includes scope definition and readiness assessment, remediation support, and audit preparedness.

The first phase is scope definition and readiness assessment, which entails facilitating data-gathering sessions, such as interviews, control demos, and documentation requests to assess your company's readiness for ISO 27001. KPMG will review existing policies, standards, technical architectures, and other relevant evidence necessary for ISO 27001 compliance and certification. This phase clarifies the scope of the certification and identifies any gaps in your company's current processes and procedures, enabling KPMG to develop a customized roadmap that addresses these gaps and aligns with your company's objectives.

In the second phase, remediation support, KPMG identifies items for remediation based on the readiness assessment and provides feedback on the identified gaps. It supports relevant stakeholders in remediation activities and helps ensure documentation aligns with ISO 2700:2022 standards.

During the final phase, audit preparedness, KPMG finalizes an executive summary for ISO certification and supporting reporting materials. It creates an evidence repository to prepare for the certification audit and make necessary revisions.

Through this thorough and dynamic approach, KPMG helps ensure that our clients have a clear path to achieve ISO 27001 certification within the given timeline.

Contact us

Adam Brand
Principal, ISO 27k Services Leader
KPMG LLP
E: adam.brand@kpmg.co.uk

Chetan Gavankar
Cyber Life Sciences Leader, Cyber Security Services
KPMG LLP
E: cgavankar@kpmg.com

Shashanko Roy
Director, Cyber Security Services
KPMG LLP
E: shashankoroy1@kpmg.com

Christoph Henle
Associate, Cyber Security Services
KPMG LLP
E: chenle@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia