ISO/IEC 27001 : 2022

Information Security Management System

Fact Sheet

What You Need to Know

ISO/IEC 27001 is the ISO standard for an Information Security Management System (ISMS). Companies who gain certification for ISO/IEC 27001 are compliant in protecting information and the associated risks of digital protection.

ISO has announced that the ISO/IEC 27001:2013 standard will be upgraded to ISO/IEC 27001:2022. This upgrade is due to the updated changes in ISO/IEC 27002, which is the supporting standard that details how businesses are to comply with the controls in Annex A of ISO/IEC 27001.

ISO published the new ISO/IEC 27002:2022 changes on the 15th of February 2022, and Annex A of ISO/IEC 27001 will be updated to be aligned with the new ISO/IEC 27002 changes. The new ISO/IEC 27001 standard was published on the 25th of October.

Minor changes have been made to the ISO/IEC 27001 standard. However, further changes will be made in the Annex A controls of ISO/IEC 27001 to reflect the updates and modifications detailed in the ISO/IEC 27002:2022 standard.

The new title of ISO/IEC 27002:2022 is Information Security, Cybersecurity and Privacy Protection – Information Security Controls.

What are the new changes to ISO/IEC 27001?

Control Categories

There are now updated control categories, which have been revised down from 114 to 93 controls, distributed across four categories: organisations, people, physical and technological.

- 58 controls remain in place with the update
- 24 controls have been merged
- 11 controls have been added

Cloud security is now a new area covered by the standard, which ISO/IEC 27001:2013 did not cover before.

ISO/IEC 27002:2022 now provides a more transparent structure of controls that can be applied throughout your organisation. The controls now provide more technical aspects of cyber security and the human elements of privacy protection.

Attributes

Attributes have now been introduced to each control. The Attributes in ISO/IEC 27001 allow organisations to create different views, which are different categorisations of controls as seen from a different perspective to the theme; in other words, it will enable the organisation to direct the controls to the right audience.

Organisations can create their own attributes, and each attribute listed below comes with a series of corresponding attribute values.

- Control Types
- Information security properties
- Cybersecurity concepts
- Operational capabilities
- Security domain

Already have ISO/IEC 27001?
Your organisation will have 3 years to transition across to the new version of the standard.

IMSM have been involved with the upgrade, transition and migration of standards for 25+ years and have a professional, fixed fee and value-added transition package – we advise you to contact us at the earliest opportunity to explore suitable options and ensure you have a plan in place.

Contact Us