ISO/IEC 27002:2022 Revision

Learn from the experts

About ISO/IEC 27002

1. What is ISO/IEC 27002?

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—Information security controls provides guidance for organizational information security standards and offers best practices for information security management. It takes into consideration a business' unique information security risk environment, by focusing on the organization's selection, implementation and management of security controls.

2. Is ISO/IEC 27002:2022 a full revision?

Yes, ISO/IEC 27002:2022 is a full revision of the standard and updates the 2013 version. Following its publication, the 2013 version will be withdrawn.

3. What has changed in the revised ISO/IEC 27002:2022?

Within the revised ISO/IEC 27002:2022, users will find that there has been a re-structure of the existing controls and the number of security control listed has decreased from 114 to 93, with some controls being removed as they no longer reflect best practices.

Eleven new controls have been introduced in the latest edition of the ISO/IEC 27002 standard. New controls include aspects such as threat intelligence, information security for use of cloud services and data leakage prevention. This will ensure that businesses are able to maintain continuous control over their information security, despite the nature of cyberattacks changing.

4. What's new in ISO/IEC 27002?

ISO/IEC 27002 has been reviewed to make it easier for businesses to adopt and continues its aim to ensure that no necessary controls have been overlooked. It uses four thematic categories of controls Technological, Organizational, People and Physical. Within this armory, there are other aids such as, use of types of controls labelled as Detective, Preventative or Corrective as well as the use of NIST cybersecurity framework; Identify, Protect, Detect, Respond, Recover and the usual Confidentiality, Integrity and Availability triad. Attributes can also be used to filter, sort, and present controls from different perspectives for different audiences

5. ISO/IEC 27002 is a supplementary guide – What actions my organization needs to take?

BSI recommends that you maintain your best practices for information security, cloud security and data security by reviewing your risk assessment and necessary controls and ensure they align with the new guidance. In this way, your organization will be in a better position to overcome future risks. Additionally, since this change triggers an update to ISO 27001, you will be preparing your organization for an upgrade of your certificate.

The benefits to your organization

6. How will ISO/IEC 27002:2022 help your business?

- Identify suitable and proportionate security controls within the process of setting up an Information Security Management System (ISMS)
- Achieve best practice in information security management
- Meet legal, statutory, regulatory and contractual requirements in relation to information security
- Strengthen risk management and reduce the likelihood of information security breaches
- Increase confidence in the organization's ISMS
- Increase the overall robustness and resilience of ISMS and strengthen risk management
- Contribute to UN Sustainable Development Goal 9 on industry, innovation and infrastructure

The impact on ISO/IEC 27001:2013

7. Will ISO/IEC 27001 be changed in 2022 because of the revised ISO/IEC 27002?

An amendment which is a partial revision will be made to ISO/IEC 27001 to update the Annex A controls to the revised ISO/IEC 27002:2022 and to include the 2 minor corrigenda that were published in 2014 and 2015. ISO/IEC 27001:2022 is anticipated to be published in the second quarter of 2022. We will guide you through the process in due course.

8. What will be the impact of the ISO/IEC 27001 once amended?

A transition assessment is going to be required and a plan will be defined for each client based on their scope, number of sites, systems, and complexity of each organization to ensure your controls and ISMS meet the updated standard.

9. What does the revision to ISO/IEC 27002 mean for an organization that is implementing its ISMS or about to get ISO/IEC 27001 certification?

Whether your organization is just implementing ISO 27001 or ready to get certified, it is important to make sure you maximize the benefits of your ISMS by taking advantage of the guidance provided in the new edition. ISO 27002:2022 will serve as a reference for identifying and implementing the appropriate controls for your organization.