Cyber Security Partners

ISO 27001:2022 changes

Summary of the changes

How to implement ISO 27001:2022

Summary of the changes

ISO 27001:2022

The latest version of ISO/IEC 27001, published in 2022, provides businesses with more robust controls that will help them adapt to today's cloud-based and digitally reliant business practices.

ISO 27001:2022, based upon the new harmonised structure (HS), is designed to strengthen information security posture. This in turn supports digitalization strategies and builds brand trust.

A comparison from the 2013 version to the 2022 version, illustrates that mandatory section changes are:

- grammatical and word changes
- additional clause at 9.3.2 Management review inputs

Updates to the Annex A controls have reduced them from 114 to 93. And of the 93, there are 11 new controls. Zero controls have been removed; all the reductions are due to controls being merged.

The control groups have been reduced from 14 groups to 4 groups into **organisational**, **people**, **physical** and **technological** control groups. New control examples include:

- Threat intelligence
- Information security for cloud services.

.

Image: ISO certification defensive shield

How to implement ISO 27001:2022

Assemble an implementation team

1. Your first task is to instruct the leaders of Departments in scope on actions needed to implement ISO27001. The project leader will require a group of people to help them.

Develop the implementation plan

2. The implementation team will use their project mandate to create a more detailed outline of their information security objectives, plan and risk register.

Initiate the ISMS

3. Create an Information Security Management System (ISMS) policy. This doesn't need to be detailed; simply an outline of what you want to achieve and how to do it.

Define the ISMS scope

4. The fourth step is to gain a broader sense of the ISMS's framework. This process is outlined in clauses 4 and 5 of the ISO 27001 standard.

Identify your security baseline

5. You can identify your security baseline with the information gathered in your ISO 27001 risk assessments and your security objectives.

How to implement ISO 27001:2022

Establish a risk management process

6. Quantify risks by scoring them on a risk matrix; the higher the score, the bigger the threat. Then select a threshold for the point at which a risk must be addressed.

Implement a risk treatment plan

7. Implementing the risk treatment plan is the process of building the security controls that will protect your organisation's information assets.

Measure, monitor and review

8. Review your ISMS to check it is working. We recommend doing this at least annually so that you can keep a close eye on the evolving risk landscape.

Certify your ISMS

9. Once the ISMS is in place, you may choose to seek ISO 27001 certification, in which case you need to prepare for an external audit. Good preparation is key for all audits.

The audit cycle

10. Keep track of internal and external audit findings, as these will be reviewed and tracked at each external audit, as evidence of commitment to following the standard.

Contact us

Anastasiia Nahirna

Sales Manager

anastasiia.nahirna@csp.partners

07842 018 866

Kevin Else

Sales Director

kevin.else@csp.partners

07962 289 255

Cyber Security Partners Limited, Yorkshire House, Greek Street, LS1 5SH

Company registration number: 12364761 | ICO registration number: ZB001933

www.csp.partners

Nov 2023