ISO/IEC 27001:2022 Revision

Learn from the experts

1. What are the key changes in the new version of the standard?

Key changes in this revision come in Annex A, reflecting the changes made in ISO/IEC 27002:2022. These changes are:

- **The structure has been consolidated into 4 key areas:** Organizational, People, Physical and Technological instead of 14 in the previous edition.
- **Controls listed have decreased from 114 to 93.**
- **The concept of attributes has been introduced.**

Also, there are editorial changes, including:

- "International standard" replaced with "document" throughout.
- Re-arranging of some English phrases to allow for easier translation.

There are also changes to align with the ISO harmonized approach:

- Numbering re-structure.
- Requirement to define processes needed for implementing the ISMS and their interactions.
- Explicit requirement to communicate organizational roles relevant to information security within in the organization.
- New clause 6.3 – Planning of Changes.
- New requirement to ensure the organization determines how to communicate as part of clause 7.4.
- New requirements to establish criteria for operational processes and implementing control of the processes.

2. Has the 2022 standard been published?

Yes, ISO 27001:2022 has already been published in late October 2022.

3. Is it essential to work to ISO/IEC 27002:2022 to transition to ISO/IEC 27001:2022?

Whilst it is not essential, the update ISO/IEC 27002:2022 now does a lot of the "heavy lifting" with the new grouping, attributes, and descriptions, making it easier to implement ISO/IEC 27001:2022 controls effectively and enabling easier alignment with cybersecurity frameworks, and other risk management methodologies.

4. **We are implementing ISO/IEC 27001:2013, could we still certify our ISMS to the 2013 version?**

Yes, however you'll have to do it no later than 31st October 2023. Thereafter, you will have to transition to the 2022 version and do so prior to the end of the transition period.

5. **If we have until October 2025 to transition, why should we take any action now?**

The changes reflect the evolution on how we work and the associated threats, plus they enable a clearer and more flexible implementation, so it is important to start on the journey ASAP to:

- Ensure your Information Security posture reflects your current digital business profile and associated risk.
- Get the most from a more flexible controls structure that now easily aligns with global cybersecurity frameworks.
- Improve the efficiency of your management system by bring it into line with the latest harmonized structure for management systems.

6. **Will there be training? If so, what courses and when will they be released?**

Yes, the new "ISO/IEC 27001:2022 Auditor Transition" training course and our "ISO/IEC 27002:2022 Implementing the changes" on-demand and instructor-led training courses are already available. Also, all our ISO/IEC 27001 training courses have been updated to the 2022 version. Look at our ISMS available courses here https://www.bsigroup.com/en-hk/iso-27001-information-security/iso-27001-training-courses/.

7. **What will the transition period be?**

There will be a transition period of 3 years commencing from 1st November 2022 to 31st October 2025.

8. **What impact does the change have on our ISMS - what should we expect?**

The key impact will be the need to revisit your risk assessment and statement of applicability to ensure the revised set of controls are applied appropriately and effectively, bringing your ISMS in line with your digital business risk.

9. **What should we do to transition and update our certificate?**

A transition audit must be carried out to assess that the changes have been implemented effectively. However, a successful transition requires a thorough understanding of the changes and their impact on your organization together with effective implementation. BSI strongly recommends that you read the standard, take the training, and go through a readiness review to ensure that your ISMS is protecting your information assets effectively and your transition is successful.