ISO/IEC 27001:2022 Transition

Get ready for the future with us.

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

Key changes in this revision:

- **A full revision of Annex A**, reflecting the changes made in ISO/IEC 27002:2022. These changes are:
    - **The reference control set has been fully reviewed and revised** with 11 new controls, and total now 93, down from 114.
    - **The structure has been consolidated into four key areas:** Organizational, People, Physical and Technological instead of 14 in the previous edition.
    - **The concept of attributes has been introduced.** This allows management of the control set through several different perspectives.

- **There are also critical changes to align with the ISO harmonized approach:**
    - **Requirement to define processes needed for implementing the ISMS and their interactions.**
    - **New requirements to establish criteria for operational processes and implementing control of the processes.**
    - Numbering re-structure.
    - 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.

    IMPORTANT NOTE: The first two points above need careful attention. Much of the restructuring of the reference controls has been on the basis of implementation of an effective process-driven approach.

- Also, there are editorial changes, including:
  - "International standard" replaced with "document" throughout.
  - Re-arranging of some English phrases to allow for easier translation

2. What is the impact of these changes?

The impact of the changes to the standard is significant, as it contains critical changes needed to ensure your ISMS is aligned with your current business practices and the associated risks. Alongside key structural changes which will make your ISMS clearer and more consistent.

The impact of implementation will differ among organizations, but it cannot be emphasized enough how crucial it is to ensure that your organization's information security posture accurately aligns with its current operations and associated risks. Therefore, it is important to understand the detail of these changes and evaluate the impact on your organization to enable you to assess the risk you hold and the effort required to implement the changes as soon as possible. This will enable you to plan your implementation in a controlled way prioritized by risk and effort. Our four-step transition guide can help you.

3. What will the transition period be?

There will be a transition period of 3 years commencing from 1st November 2022 to 31st October 2025. However, all initial or re-certifications must be conducted against ISO/IEC 27001:2022 from 1st May 2024.

4. I am not ready to transition yet. What should I do?

To ensure you protect your business effectively and have a smooth transition, it is important to understand the scope of the changes and their impact on your organization as soon as possible. You can then plan your implementation of the changes prioritized by risk, scheduling your transition at a time that best suits your organization and giving you plenty of time to prepare effectively. Our four-step transition guide can help you.

5. **We have training requirements and would like to train our staff prior to working on the transition**

Great! training is the first step. We have a range of training solutions – classroom, on-line and on-demand – at various levels, including training specifically covering the changes for those already working to the 2013 version. To ensure you protect your business and have a smooth transition, it is important to understand the scope of the changes and their impact on your organization as soon as possible, see question number one above. Therefore, we recommend to schedule your training and then undertake step two of our four-step guide as soon as possible – to understand the impact of the changes on your organization. You can then plan your next step, prioritized according to risk and effort needed.

6. **We are interested in transitioning. Can we just combine with our next surveillance visits?**

Yes absolutely, but you first need to understand the changes and the impact on your business so you can be sure you are ready in suitable time for a smooth transition and protecting your business effectively in the meantime. See questions number one, two and four above.

7. **Why should I do anything now if I have until October 2025?**

There is potentially a lot of work to do to become compliant. More importantly, by ignoring the fact that global best practice has been updated to reflect current risks, you could be exposing your business to unnecessary risk. All organizations should understand the changes and the impact on their organization as soon as possible. They can then plan the implementation of the changes in a controlled way prioritizing based on risk and effort. See questions number one and two for further info.

8. **The changes to the standard seem minimal, so why would we need to transition in the short term?**

Although the number of changes to the clauses may seem small, they could result in a significant amount of work, starting from the context of the organization, determining all

the necessary processes and their interactions; and then in the operational section, determining criteria for the processes and implementing them in accordance with their criteria. Furthermore, Annex A, the controls to be considered during the risk assessment and in creating the Statement of Applicability (SoA), has gone through extensive change, beyond the 11 new controls. All controls have been reviewed and updated. This update requires a full review of the risk assessment and SoA to ensure effective implementation. The changes to the controls also reflect the changing business environment and evolving threats and so you need to address them promptly to ensure your information security posture reflects your current business practices and the associated risks. See questions number one, two and four above.

9. We need to identify what are the gaps before moving forward to transitioning. Can BSI help with this?

Yes, we can provide a gap assessment. We can help you identify the gaps and provide you with suitable general training to allow you to fill the gaps yourselves and maintain a high level of confidence in the system going forward.

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

Whilst it is not essential, with all the changes to the existing controls, alongside several new controls, working with ISO/IEC 27002 will significantly help ensure you are implementing the required controls effectively. The updated ISO/IEC 27002:2022 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.

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

Yes, however you will have to do it no later than 30th April 2024. Thereafter, you will have to transition to the 2022 version and do so prior to the end of the transition period.

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

Your Certification Body must conduct a transition audit to assess whether your organization have implemented the changes 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 first to ensure that your ISMS is protecting your information assets effectively and your transition is successful.