Main Changes in ISO 27001:2022:

- Main part of ISO 27001, i.e., clauses 4 to 10, are not changing
- Only the security controls listed in ISO 27001 Annex A will be updated
- Number of controls has decreased from 114 to 93
- Controls are placed in 4 sections instead of previous 14
- There are 11 new controls, while none of the controls were deleted, and many controls were merged

1) What exactly is changed in ISO 27001:2022 and ISO 27002:2022?

Main part of ISO 27001, i.e., clauses 4 to 10 are not going to change. These clauses include the scope, interested parties, context, Information security policy, risk management, resources, training & awareness, communication, document control, monitoring and measurement, internal audit, management review, and corrective actions.

Only the security controls listed in ISO 27001 Annex A and in ISO 27002 will be updated.

In general, the changes are only moderate and were made primarily to simplify the implementation: number of controls has decreased from 114 to 93 and are placed in 4 sections instead of previous 14. There are 11 new controls, while none of the controls were deleted, and many controls were merged.

Changes in ISO 27001:2022 Annex A will be fully aligned with changes in ISO 27002:2022, you can read the details about the changes in controls here: **Main changes in the upcoming new version of ISO 27002**.

2) What is the difference between ISO 27001 and ISO 27002?

ISO 27001 is the main standard, and companies can get certified against it; companies cannot certify against ISO 27002:2022 since it is only a supporting standard.

In its Annex A ISO 27001 provides only a list of security controls but does not explain how they can be implemented; ISO 27002 lists those very same controls and provides guidance on how they could be implemented. However, this guidance in ISO 27002 is not mandatory, i.e., companies can decide whether to use those guidelines or not.

3) When are these changes going to take place?

ISO 27002 was updated on February 15, 2022, and Annex A of ISO 27001 will be aligned with those changes.

Updates in ISO 27001 Annex A will happen somewhere during 2022, the date is not announced yet.

4) We want to starting implementing ISO 27001, do we wait until changes are published or should we start now?

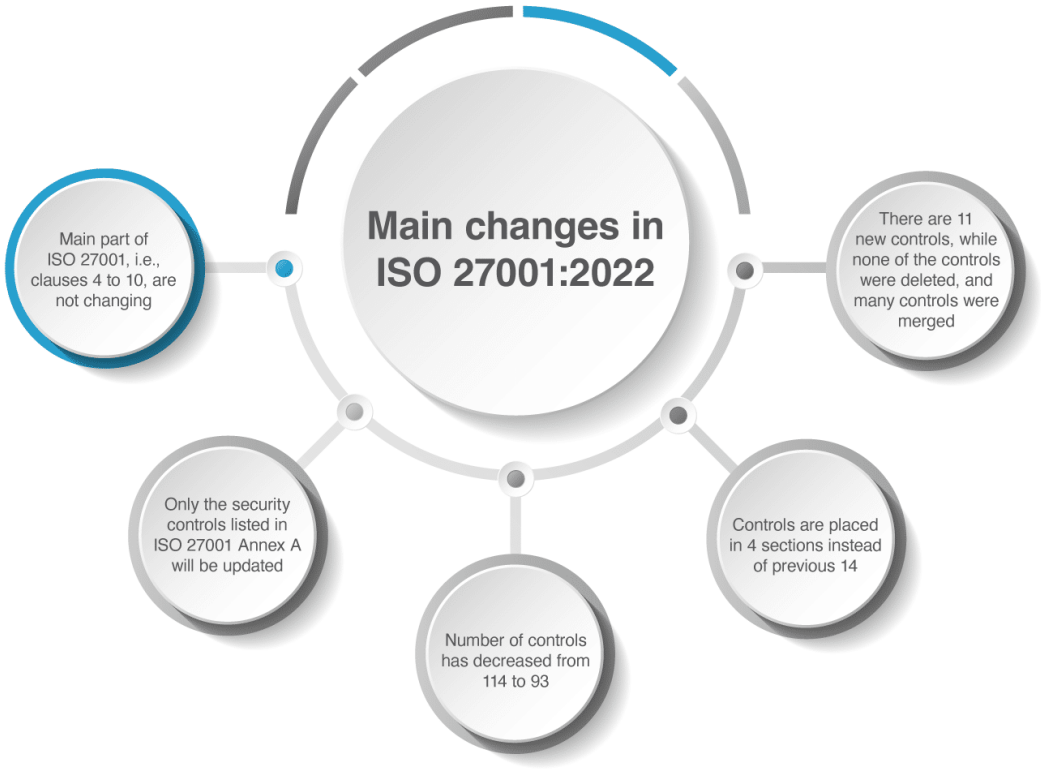
If your existing or potential client expects you to get certified, then you should start as soon as possible; if you can wait with your project until end of 2022 then you can wait for the updated standard.

In other words, this decision has nothing to do with standards – this depends on how quickly you need the ISO 27001 certificate.

5) If we start now with ISO 27001 implementation, do we go with new set of controls or the old ones?

Since the changes in ISO 27001 are not published yet, you should start with the existing (old) controls.

Since the changes in controls are only moderate, and you'll have lots of time to update documentation for the new controls (see explanation in further text), the transition to the new revision of the standard will be a minor effort.



6) We already implemented ISO 27001, what do we need to change in our documentation?

Changes in standards are mostly about reorganizing controls, so no changes in technology will be needed, only the changes in the documentation.

Since the changes are only moderate, our suggestion is that you do not add new documents or delete any of the existing documents.

In our opinion, the best way to comply with these changes is:

a. To update your risk treatment process with new controls

b. To update your Statement of Applicability

c. To adapt certain sections in your existing policies and procedures.

7) When do we need to change our documentation?

Transition period for these changes is not published yet, but it will probably be 2 years starting from the date of official ISO 27001:2022 update.

Therefore, you'll have plenty of time to comply.

8) Does the certification body need to check changes in the documentation?

Yes, if your company is certified, the certification body will check if you have adapted your documentation within the transition period.

There will be no need to schedule any new audits since they will do this during the regular surveillance audits.

9) What does this change mean for my ISO 27001 Lead Auditor / Lead Implementer certificate?

Since the main part of ISO 27001 will not change, your personal ISO 27001 certificates will remain valid and no additional training will be needed.