Key Updates in ISO 27001:2022

ISO 27002:2022 was published on February 15, 2022, and **ISO 27001:2022** on *October 25, 2022.*

ISO 27001:2013	ISO 27001:2022 NEW
Information technology — Security techniques — Information security management systems — Requirements	**Information security, cybersecurity and privacy protection** — Information security management systems — Requirements
11 Clauses in the main part of the standard	**11** Clauses in the main part of the standard
114 security controls in Annex A	**93** security controls in Annex A
14 Domains in Annex A	**4** Domains in Annex A

Summary of Changes:

New Requirements in ISO 27001:2022

The intent of the standard remains the same, with the core fundamental aspects of risk management being unchanged.

Clause 4.2 now includes identifying requirements of interested parties that will be addressed through ISMS.

Clause 6.2 now includes a monitoring capability of information security objectives.

Clause 6.3 (NEW) includes having a plan for any changes to the ISMS

Clause 8.1 now includes establishing criteria for security processes and implementing process.

Clause 9.3 now includes reviewing the changes in needs and expectations of interested parties, and relevant to the ISMS.

Changes in Annex A security controls

Whilst Annex A controls have been revised down from 114 to 93 controls, no controls have been excluded, with some being merged as rationalisation and effectiveness.

4 **domains** instead of previous **14** domains

• **Organisational** • **People** • **Physical** • **Technical**

23 **controls** have been renamed to make them easier to understand

35 **controls** remained the same with change in control number,

24 **controls** merged from **57** controls

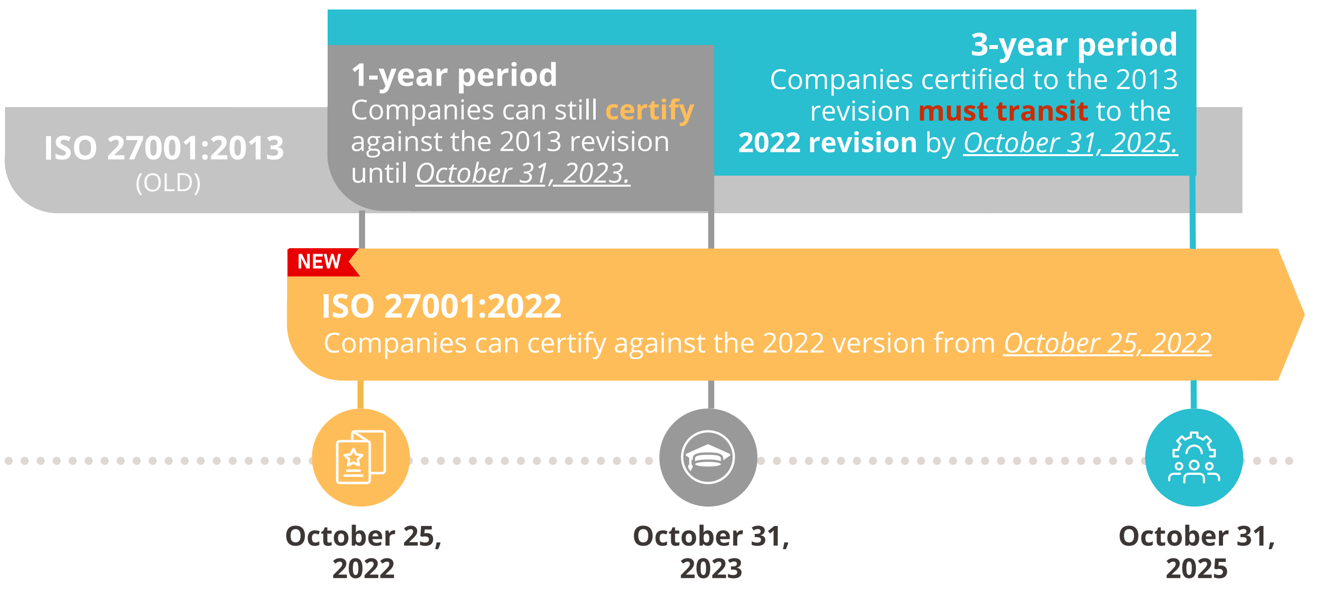
1 **control -** **Control 18.2.3 Technical Compliance Review** was split into;

- **A 5.3.6 – Compliance with policies, rules and standards for information security**
- **A 8.8 – Management of technical vulnerabilities**

11 **new controls** were added:

[1] Physical security monitoring
[2] Threat intelligence
[3] Configuration management
[4] Information deletion
[5] Data masking
[6] Data leakage prevention
[7] Web filtering
[8] Secure coding
[9] ICT readiness for business continuity
[10] Monitoring activities
[11] Information security for use of cloud services

Transition Period:



ISO 27001:2013 (OLD)

1-year period
Companies can still **certify** against the 2013 revision until *October 31, 2023.*

3-year period
Companies certified to the 2013 revision **must transit** to the **2022 revision** by *October 31, 2025.*

NEW
ISO 27001:2022
Companies can certify against the 2022 version from *October 25, 2022*

October 25, 2022

October 31, 2023

October 31, 2025

Privasec
www.privasec.com