io key guides

Stay ahead of the deadline to update • Stay ahead of the deadline to update • Stay ahead of the deadline to update •

31st October 2025

Everything you need to know about the

ISO 27001:2022 standard update

A summary of the fundamental changes to the standard to help organisations identify the key areas they need to review

Public V2.0

The world's best-known standard on information security management helps organisations secure their information assets – which is vital in today's increasingly digital world.

A new and improved version of ISO 27001 was published in 2022 to address global cybersecurity challenges and improve digital trust.

ISO/IEC 27001:2022 took immediate effect in October 2022 but gave organisations already certified to ISO 27001:2013 three years to transition to the new 2022 version. With the October 2025 deadline just months away, organisations that have yet to transition to the 2022 version must ensure their certifications are updated to comply with the new standard.

We've summarised some of the fundamental changes to the standard to help organisations identify the key areas they need to review to either achieve re-certification if they already hold ISO 27001:2013 or acquire brand new certification against the new ISO 27001:2022 version.

What has changed?

The good news is that many changes are editorial, for example, changing 'international standard' to 'document' throughout and rearranging phrases to allow for better international translation.

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

- ✓ Numbering re-structure
- ✓ The requirement to define processes needed for implementing the ISMS and their interactions
- ✓ The explicit requirement to communicate organisational roles relevant to information security within the organisation
- ✓ New clause 6.3 – Planning of Changes
- ✓ A new requirement to ensure the organisation determines how to communicate as part of clause 7.4
- ✓ New requirements to establish criteria for operational processes and implement control of the processes

The core changes, however, apply to updates to the current controls in Annex A to align the standard better with the recent changes to ISO/IEC 27002 – Information security, cybersecurity and privacy protection.

The changes to ISO/IEC 27001: 2022 also consider that risk management increasingly spreads across more organisational functions. Therefore the updates are intended to make it more straightforward for more people to map and implement the proper security controls.

What are the core changes to Annex A Controls?

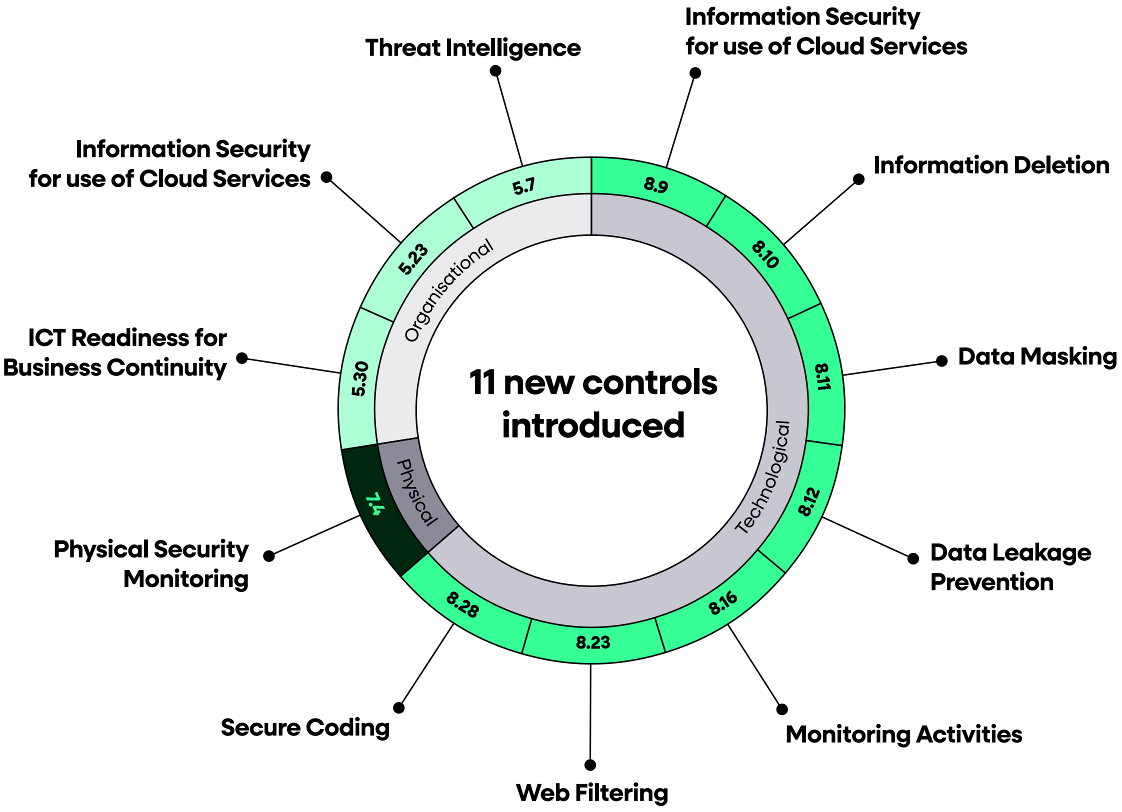
The number of controls has reduced from 114 to 93

Some controls have been deleted, 24 controls have been merged, and 58 have been revised. 11 new security controls have been added, designed to address the evolving information security and cybersecurity landscape.

As a result, you need to update your management system to optimise any existing ISMS and better align with the context of your information security risks and your organisation.

The structure has been consolidated into four key areas: Organisational, People, Physical, Technological.

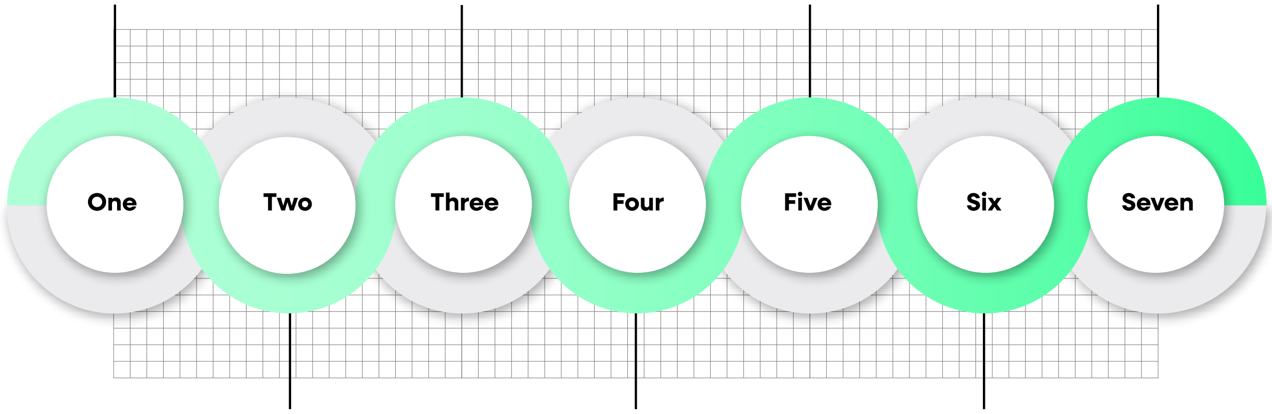
This contrasts with the 14 areas that formed the previous version of the standard.


11 new controls introduced
Organisational
Physical
Technological
5.7 Threat Intelligence
8.9 Information Security for use of Cloud Services
8.10 Information Deletion
8.11 Data Masking
8.12 Data Leakage Prevention
8.16 Monitoring Activities
8.23 Web Filtering
8.28 Secure Coding
7.4 Physical Security Monitoring
5.30 ICT Readiness for Business Continuity
5.23 Information Security for use of Cloud Services

Achieving ISO 27001:2022

We are already helping companies with ISO 27001:2022 and recommend starting your certification now.

We have everything you need to implement an ISO 27001-compliant ISMS and achieve certification to the standard. We’re ready to support you, from helping you understand the changes to checking the impact on your organisation, implementing, and finally transitioning your certification.



One – Update your ‘Risk Treatment Plan’ to align it with the new structure and numbering of controls.

Two – Review and update your Statement of Applicability.

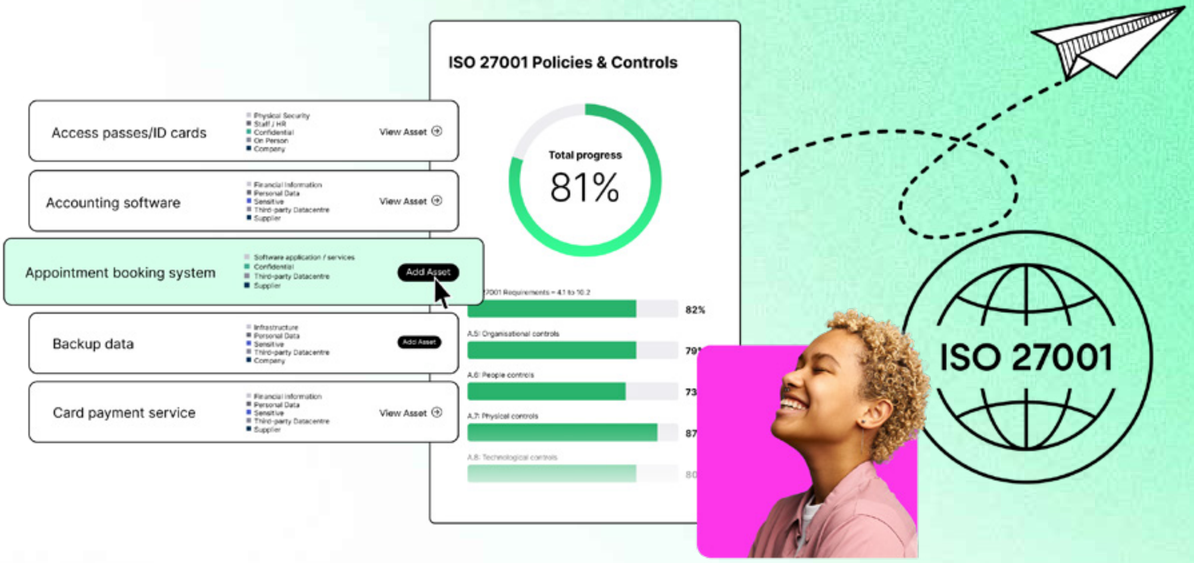
Three – Review and update your ISMS Management review procedure.

Four – Review and update your information security objectives and the monitoring, measurement, analysis and evaluation procedure.

Five – Review and update your ISMS Communication Plan.

Six – Review and update other policies, standards and procedures (where applicable).

Seven – Evaluate your third-party security tools to ensure how you are demonstrating compliance supports the new requirements.



Strengthen your Information Security Posture Today

The ISMS.online platform and tools are ready to support you now, from helping you understand the changes, checking the impact on your organisation's security objectives, implementation guidance, and transitioning your certification. Unlock your compliance advantage today!

Get started →

isms·online