ISO/IEC 27001:2022

Understanding the new ISO 27001 standard, a step-by-step guide for new certification or recertification.

Enhanced information security framework

At the end of October 2022, the International Organization for Standardization (ISO) published a new version of ISO/IEC 27001:2022.

The new version is a moderate update from the previous version of the standard: ISO 27001:2013. The majority of changes relate to the Annex controls and align to ISO/IEC 27002:2022 updates, published earlier in 2022. The Annex controls have been rearranged and new Annex controls added.

At KPMG, we have developed a structured timeline which outlines the transition period, with a deadline of October 2025.

ISO/IEC 27001: 2013

Companies can **certify** against the 2013 revision until April 2024.

Companies certified against the 2013 revision **must transition** to the 2022 revision by October 2025.

ISO/IEC 27001: 2022

Companies can apply for certification against the 2022 revision from October 2023.

October 2022 — **October 2023** — **October 2025**

ISO/IEC 27001: 2013 vs 27001:2022 changes at a glance

Changes to the title of the standard	The title of the ISO 27001 standard has changed to **ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements**. The change reflects the modern compliance landscape, regulations such as GDPR and the evolving cyber threat organisations face.
Minor changes in clauses 4 – 10	• **4** new requirements added to clauses 4 – 10 • No significant requirements from ISO 27001:2013 were removed
Structural changes to Annex A	The 14 Annex A sections have been consolidated into **4** sections (People, Technological, Physical and Organizational) to simplify and streamline the process of selecting and implementing security controls.
Changes in Annex A controls	• **93** Annex A controls, reduced from 114 • **11** new controls • **57** controls merged together • **1** control split • **23** controls renamed • **35** controls with no changes • No controls were removed

New security controls in ISO/IEC 27001:2022

A.5.7	Threat intelligence
A.5.23	Information security for use of cloud services
A.5.30	ICT readiness for business continuity
A.7.4	Physical security monitoring
A.8.9	Configuration management
A.8.10	Information deletion
A.8.11	Data masking
A.8.12	Data leakage prevention
A.8.16	Monitoring activities
A.8.23	Web filtering
A.8.28	Secure coding

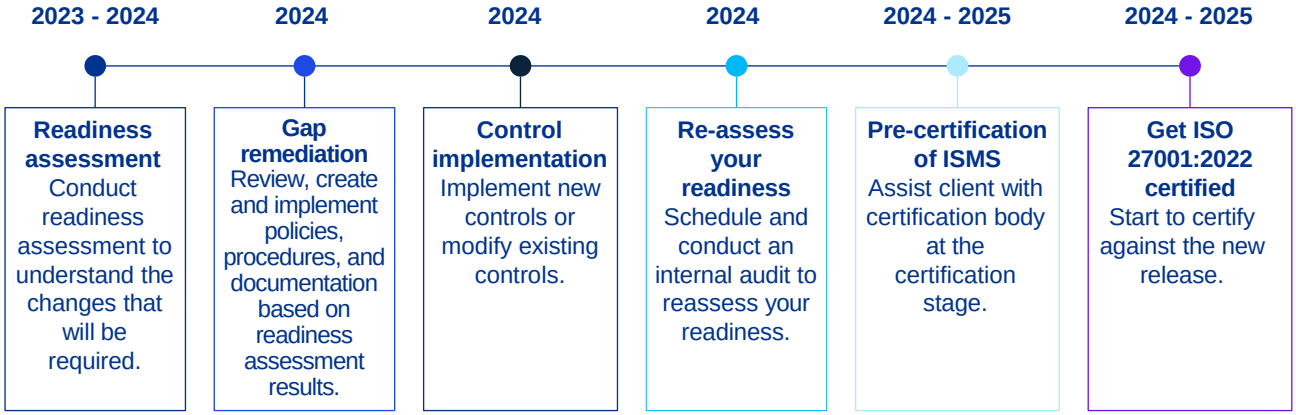
ISO/IEC 27001:2013		ISO/IEC 27001:2022
11	Clauses in the main part of the standard	11
114	Security Controls in Annex A	93
14	Sections In Annex A	4

The ISO 27001:2022 certification process

This information is not intended as professional advice; consult qualified professionals for guidance for your particular circumstances.

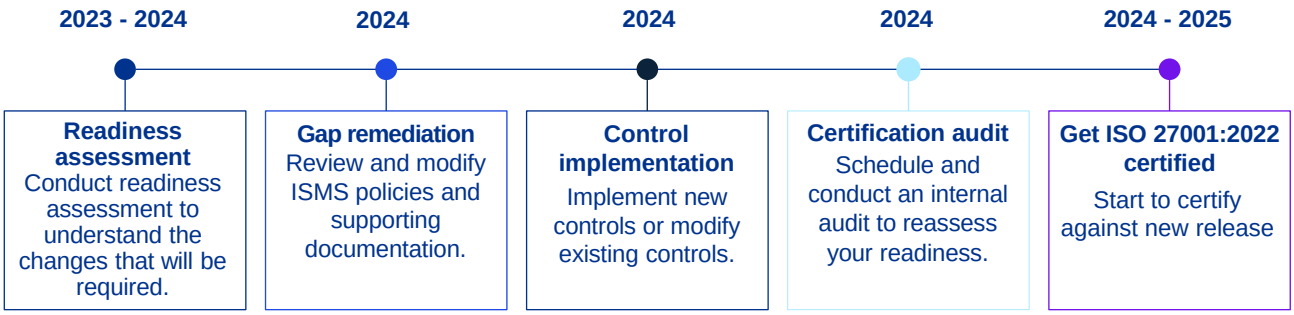
1. Companies seeking certification for the first time

While companies can certify against the 2013 revision of the ISO 27001 standard until April 2024, we highly recommend that all companies seeking certification for the first time pursue certification against the 2022 version of the standard. Companies can apply for certification against the 2022 version **from October 2023**.



2. Currently certified companies

There is a transition period of three years after the publication of ISO/IEC 27001:2022. Currently certified companies will need to recertify against the new standard **by October 2025**.



How KPMG can help

Some or all of the services below may not be permissible for KPMG audited entities.

Gap Analysis

We can complete a gap assessment of your ISMS' conformance to the ISO 27001 standard and review controls which have been identified as applicable to your ISMS, highlighting current design gaps.

Implementation

We can support you in implementing the necessary processes and controls mandated by the ISO 27001:2022 standard, ensuring compliance with its requirements.

Internal Audit

We can support you as your outsourced or co-sourced internal audit function, as having an internal audit function is one of the mandatory requirements stipulated by the ISO 27001:2022 standard.

Neil Coutts
Director
Cyber & Technology Risk | KPMG UK
T: +44 (0) 7810 545 676
E: neil.coutts@kpmg.co.uk

Jack Porter
Senior Manager
Cyber & Technology Risk | KPMG UK
T: +44 (0) 7880 054 417
E: jack.porter@kpmg.co.uk

Darnte Cranston
Manager
Cyber & Technology Risk | KPMG UK
T: +44 (0) 7769 283 582
E: darnte.cranston@kpmg.co.uk

kpmg.com/uk

CREATE: CRT150607A