ISO/IEC 27001: 2022

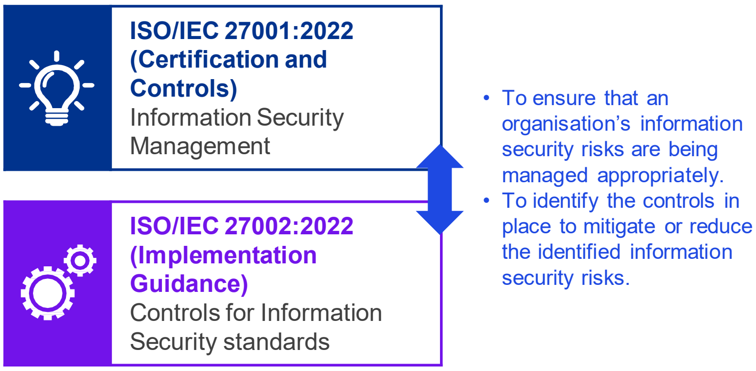
Understanding the “New ISO 27001 standard”, a step-by-step journey for new certification or recertification.

February 2023

Enhanced information security framework

As a result of an ever-changing global digital landscape and evolving cyber threats, cybercrime is growing more severe and sophisticated. To address this evolution and better tackle cybersecurity challenges, the International Organization for Standardization (“ISO”) has updated the ISO/IEC 27001 Information Security Management and ISO/IEC 27002 Controls for Information Security.

An enhanced scheme, ISO/IEC 27001:2022, has now been introduced, with a structured implementation timeline starting in end-2022 and continuing through 2025. We have summarised the changes below:



ISO/IEC 27001:2022 (Certification and Controls)
Information Security Management

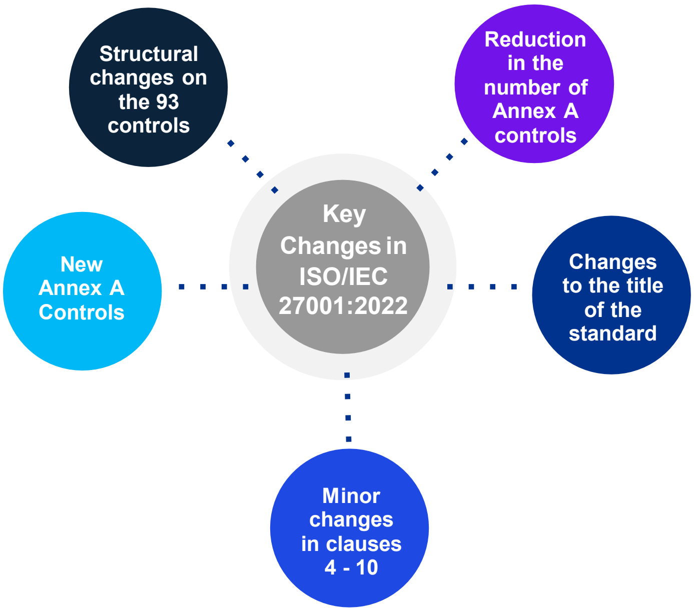
ISO/IEC 27002:2022 (Implementation Guidance)
Controls for Information Security standards

- To ensure that an organisation’s information security risks are being managed appropriately.
- To identify the controls in place to mitigate or reduce the identified information security risks.

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

Dismantling the “New ISO 27001 standard” to help you diagnose information security issues and enhance protection

Changes to the title of the standard	• The ISO/IEC 27001:2022 title has changed from ISO/IEC 27001:2013 Information Technology - Security techniques - Information security management system - requirements to **ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements**. • This change is the result of a need to consider the modern compliance landscape, regulations such as GDPR and the evolving cyber risks organisations face.
Minor changes in clauses 4 - 10	• There have been minor updates in management clauses 4 – 10.
New Annex A Controls	• 11 new controls have been added to Annex A.
Structural changes on the 93 controls	• 93 Annex A controls have been structured to 4 categories (People, Technological, Physical and Organizational) to simplify and streamline the process of selecting and implementing security controls.
Reduction in the number of Annex A controls	• There has been a decrease in the number of Annex A controls from 114 to 93 due to the merging of controls. No controls were removed.

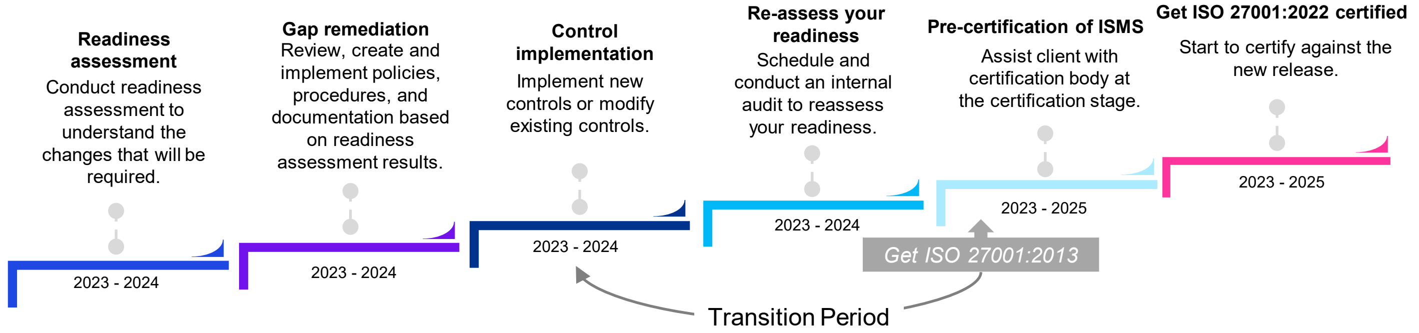


Structural changes on the 93 controls
Reduction in the number of Annex A controls
New Annex A Controls
Key Changes in ISO/IEC 27001:2022
Changes to the title of the standard
Minor changes in clauses 4 - 10

The ISO 27001:2022 certification process

1. Companies seeking certification for the first time

Companies wishing to be ISO 27001 certified are required to comply with 27001:2013 or 27001:2022 requirements for the **first time**. If your company plans to obtain certification before March 2023, your company should use the 2013 release, but if your company plans to obtain certification after March 2023, you can start now with the 2022 version. This is due to the fact that once the 2022 version is published, certification bodies will need time to prepare the certifications according to the updated standard, which will be ready only after March 2023. Your company will need to go through the transition to meet the 2022 version until mid-2024, and this transition will require approximately 5% to 10% of the effort compared to the initial implementation.



Readiness assessment
Conduct readiness assessment to understand the changes that will be required.
2023 - 2024

Gap remediation
Review, create and implement policies, procedures, and documentation based on readiness assessment results.
2023 - 2024

Control implementation
Implement new controls or modify existing controls.
2023 - 2024

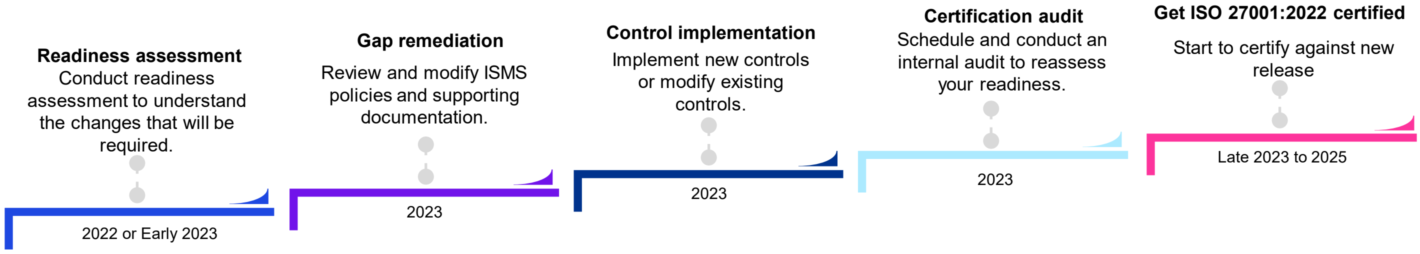
Re-assess your readiness
Schedule and conduct an internal audit to reassess your readiness.
2023 - 2024

Pre-certification of ISMS
Assist client with certification body at the certification stage.
2023 - 2025

Get ISO 27001:2022 certified
Start to certify against the new release.
2023 - 2025

2. Currently-certified companies

There will be a transition period of three years after the publication of ISO 27001:2022. Currently-certified companies will need to certify for the updates **before the end of 2025.**



Readiness assessment
Conduct readiness assessment to understand the changes that will be required.
2022 or Early 2023

Gap remediation
Review and modify ISMS policies and supporting documentation.
2023

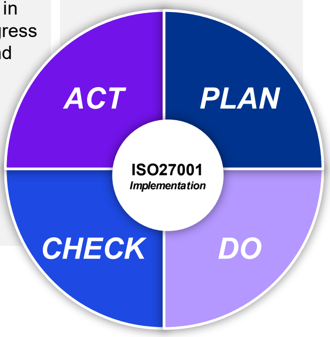
Control implementation
Implement new controls or modify existing controls.
2023

Certification audit
Schedule and conduct an internal audit to reassess your readiness.
2023

Get ISO 27001:2022 certified
Start to certify against new release
Late 2023 to 2025

How KPMG can help

Scoping	Gap assessment	Asset identification, ownership, classification	Risk assessment & risk treatment planning	ISMS implementation	Pre-certification & certification
• Assist in determining external and internal issues. • Assist in determining relevant interested parties and the requirements of these interested parties. • Assist in determining the scope of the system. • Assist in delivering scoping documentation required as per ISO/IEC 27001:2022 standard.	• Assist in reviewing in-scope ISMS elements. • Assist in delivering gap assessment results. • Assist in delivering a roadmap remediation plan.	• Identify, classify and document relevant assets. • Define ownership and responsible departments of assets and perform asset valuation. • Classify assets according to the criticality based on business area and usage. • Deliver asset list with defined ownership and classification.	• Assist in conducting a detailed risk assessment. • Assist in delivering a risk assessment report, prioritised risks, risk treatment plan, information risk inventories, SOA (Statement of Applicability). • Assist in delivering a risk treatment plan. • Liaising with respective party (including internal audit and top management).	• Assist in providing ISO 27001 standard awareness & training programs (as per agreed). • Assist in reviewing the implementation documents in order to fulfil the identified gap. • Provide assistance in monitoring the progress of risk mitigation and remediation processes.	• Perform the pre-certification audit (internal audit). • Assist and work with client to prepare the documentation required.



Contact us

Henry Shek
Partner
Technology Consulting
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Brian Cheung
Partner
Technology Consulting
KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

Lanis Lam
Partner
Technology Consulting
KPMG China
T: +852 2143 8803
E: lanis.lam@kpmg.com

Jack Chan
Associate Director
Technology Consulting
KPMG China
T: +852 2847 5027
E: jack.k.chan@kpmg.com

kpmg.com/cn/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.