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)
ISO/IEC 27002:2022 (Implementation Guidance)

• 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

• 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. |

© 2023 KPMG Advisory (Hong Kong) Limited, a Hong Kong (SAR) limited liability company and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited (“KPMG International”), a private English company limited by guarantee. All rights reserved.
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.

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.

How KPMG can help

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

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