ISO/IEC 27001 and ISO/IEC 27001: 2022 updates

The anticipated long overdue revision to ISO/IEC 27001 is published. This update will be in line with ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls which was published early this year on 16 February 2022.

These important changes reflect the evolution of business practices. The below are some key information including the major changes to get you prepared for transiting to the revised Standard.

The major changes to the 2022 edition of ISO /IEC 27001 are as follows:

- Update of Annex A of the Standard to reflect ISO/IEC 27002:2022, i.e., category restructure and have cut down the total number of controls from the existing of 114 to 93:
- 11 new controls
- 24 merged controls
- 58 updated controls

The restructured (new categories) of controls have been consolidated from 14 to 4 as follows:

- **People** (8 controls): concerning individual people, such as remote working, screening, confidentiality, or non-disclosure agreements.
- **Organisational** (37 controls): concerning the organisation, such as policies for information, return of assets, information security for use of cloud services.
- **Technological** (34 controls): concerning technology, such as secure authentication, information deletion, data leakage prevention, or outsourced development.
- **Physical** (14 controls): concerning physical objects, such as storage media, equipment maintenance, physical security monitoring, or securing offices, rooms and facilities.

The 11 New Controls are:

- Threat intelligence
- Information security for use of cloud services
- ICT readiness for business continuity
- Physical security monitoring
- Monitoring activities
- Web filtering
- Secure coding
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention

ISO/IEC 27001 and ISO/IEC 27001: 2022 updates

What need to be done especially how the revised version of ISO/IEC 27001 would impact your existing information security management system?

Transition requirements:

Same as other management system standards, the transition period should be within 3 years from the publication date of ISO 27001:2022 standard. As the published date is October 2022, you should conform to the requirements of the revised Standard and transit by end of October 2025. All audits normally will be against the revised Standard starting October 2023, a year after the release of the revised Standard and you should anticipate that additional audit time will be required to cover the changed/ new controls to demonstrate your compliance with the revised Standard.

In summary, to ensure smooth transitions and minimise disruption, you should consider the following key activities for the transition:

- Familiarise yourself with the 93 Controls in the revised ISO 27001:2022
- Roll out training program for staff members involved in your ISMS operation
- Conduct gap analysis between your current system and the revised ISO 27001:2022 to help you better understand how your ISMS will be affected, and what will need to be adjusted to be compliant with the revised standard.

For more information regarding the revised Standard especially the new controls and the transition requirements, you are encouraged to attend our ISO 27001:2022 transition training course, please contact us at enquiries.sg@gicgrp.com for a no-obligation discussion.