This letter has been prepared by GCC to provide guidance for the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 which was published on the 25th of October 2022.

After 9 years, ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) finally reviewed and revised the ISO 27001 and published the new standard in October 2022. This third edition of ISO 27001 cancels and replaces the second edition (ISO/IEC 27001:2013)

As expected, the standard text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022.

The key changes

Compared with ISO/IEC 27001:2013, the main changes of ISO/IEC 27001:2022 include, but are not limited to:

i) Annex A references the information security controls in ISO/IEC 27002:2022, which includes the information of control title and control.

ii) The notes of Clause 6.1.3 c) are revised editorially, including deleting the control objectives and using “information security control” to replace “control”.

iii) The wording of Clause 6.1.3 d) is re-organized to remove potential ambiguity.

iv) Adding a new item 4.2 c) to determine the requirements of the interested parties addressed through an information security management system (ISMS).

v) Adding a new subclause 6.3 - Planning for changes, which defines that the changes to the ISMS shall be carried out by the organization in a planned manner.

vi) Keeping the consistency in the verb used in connection with documented information, for example, using “Documented information shall be available as evidence of XXX” in clauses 9.1, 9.2.2, 9.3.3 and 10.2.

vii) Using “externally provided process, products or services” to replace “outsourced processes” in Clause 8.1 and deleting the term “outsource”.

viii) Naming and reordering the subclauses in Clause 9.2 - Internal audit and 9.3 - Management review.

ix) Exchanging the order of the two subclauses in Clause 10 - Improvement.

x) Updating the edition of the related documents listed in Bibliography, such as ISO/IEC 27002 and ISO 31000.

xi) Some deviations in ISO/IEC 27001:2013 to the high-level structure, identical core text, common terms and core definitions of MSS are revised for consistency with the harmonized structure for MSS, for example, Clause 6.2 d).

Note

Compared with the old edition, the number of information security controls in ISO/IEC 27002:2022 decreases from 114 controls in 14 clauses to 93 controls in 4 clauses. For the controls in ISO/IEC

27002:2022, 11 controls are new, 24 controls are merged from the existing controls, and 58 controls are updated. Moreover, the control structure is revised, which introduces "attribute" and "purpose" for each control and no longer uses "objective" for a group of controls.

Changes in the standard structure:

Details	ISO 27001:2013	ISO 27001:2022
Clauses	10	10
Controls	114	93
Domains in Annexure A	14	4

Changes in the control domains

Control Group	Count
A.5 Organizational controls	37 controls
A.6 People controls	8 controls
A.7 Physical controls	14 controls
A.8 Technological controls	34 controls

Changes in controls

Control Group	Count
New Controls	11 controls
Merged Controls	24 controls
Updated Controls	58 controls

Find out more about the changes here.

The Impact

R The impact of the changes in ISO/IEC 27001:2022 includes, but is not limited to the introduction of a new Annex A and Clause 6.3 - Planning for changes because:

i) ISO/IEC 27001:2013/COR 2:2015 has already been published and implemented.

ii) Annex A is normative.

iii) The harmonized structure for MSS is considered as a minor revision for the high-level structure, identical core text, common terms and core definitions of MSS, in which most of the changes are considered editorial.

The requirements in ISO/IEC 27001 that use the reference control set in Annex A are the comparison process between the information security controls determined by the organization and those in Annex A (6.1.3 c)) and the production of a Statement of Applicability (6.1.3 d)). By comparing the necessary information security controls to those in Annex A, the organization may confirm that any necessary information security control from the reference set in Annex A of ISO/IEC 27001:2022 is not inadvertently omitted.

Such comparison might not lead to the discovery of any necessary information security control that has been inadvertently omitted. However, if inadvertently omitted necessary information security controls are discovered, the organization shall update its risk treatment plans to accommodate the additional necessary information security controls and implement them.

As implied above, the impact of ISO/IEC 27001:2022 on the organizations that have implemented ISMS need not be significant.

Key Timeline

Activity	Due Date
ISO Publishes ISO/IEC 27001:2022	**October 2022**
JAS-ANZ publishes its transition policy to certification companies	**November 2022**
GCC trains staff, updates procedures, and submits self-declaration to JAS-ANZ	**November 2022**
GCC Initiates first audits and certification to ISO/IEC 27001:2022	**November 2022**
GCC stops offering new certification according to ISO/IEC 27001:2013	**April 2024 (18 months)**
GCC stops Surveillance/Recertification audit according to ISO/IEC 27001:2013	**October 2024 (24 months)**
GCC withdraws all ISO/IEC 27001:2013 certificates	**October 2025 (36 months)**

What certified clients to do

- Purchase a copy of the new standard and identify organisational gaps which need to be addressed to meet new requirements
- Develop an implementation plan
- Update the statement of applicability (SoA)
- Update the risk treatment plan (if applicable)
- Implement the new or changed controls
- Provide appropriate training and awareness for all parties that have an impact on the effectiveness of the organisation
- Update the existing management system to meet the revised requirements and provide verification of effectiveness
- Liaise with GCC for transition arrangements

Key Notes

- The transition audit can be conducted in conjunction with the surveillance audit, recertification audit or through a separate audit
- The transition audit is not only relied on the document review, especially for reviewing the technological controls
- The transition audit includes a gap analysis of ISO/IEC 27001:2022 key changes and the implementation and effectiveness of the new or changed controls chosen by the clients
- The GCC transition audits include auditor time to confirm the transition of the certified clients

- Surveillance and Recertification audits based on ISO/IEC 27001:2013 will not be offered after **October 2024**
- The transitions of certified clients must be completed by **October 2025**
- If the client fails to transition prior to the end of the transition period (**October 2025**), its current certification will lapse

How GCC can help

- Providing Gap Analysis service if needed Request a Quote
- Providing ISO/IEC 27001 checklist (at no cost) Contact Us

Please feel free to contact our office if you have any question or query.

Thank you,

Global Compliance Certification

HEAD OFFICE
Level 1, 77 Pacific Highway, North Sydney NSW 2060 Australia
T +61 2 8644 0603
W https://gccertification.com/