Recommendations for CQI and IRCA member transition to ISO/IEC 27001:2022

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements

This document has been prepared to describe the position of the CQI regarding the revision to ISO/IEC 27001, resulting in the publication of ISO/IEC 27001:2022. It describes transition training requirements for IRCA Certificated ISMS auditors.

Detailed transition information will be communicated IRCA Certificated auditors directly.

Introduction

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also specifies requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

This standard was created with the intention of protecting an organization's information assets. An information asset can be considered as a definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation. Examples of information assets include:

- Strategies, plans, goals and objectives
- Patents, copyrights, trademarks
- Project records
- Marketing media
- Operational and Financial data
- Legal and compliance information
- Research and development records

ISO/IEC 27001:2022 seeks to maintain the confidentiality, integrity, and availability of such information through the application of a management system coupled with a set of controls. These controls not only appear in ISO/IEC 27001, but also in ISO/IEC 27002.

Summary of changes to ISO/IEC 27001:2022

While there is comparatively little change in the substantive text) of clauses 0 to 10 between the two editions, there have been some amendments to structure, terminology and the ordering of words that are worthy of note.

The most significant impacts however arise from the reworking of the document's normative annex A. The controls appearing in this Annex are drawn directly from ISO/IEC 27002 - Information Security,

Cybersecurity and Privacy Protection - Information Security Controls which was published in March 2022. These controls have undergone extensive revision. There are now different categories of controls (down from 14 to 4 'themes'), control objectives no longer appear in the annex and individual 2013 controls have been updated, merged, renumbered and in some cases deleted. Additionally, 11 brand new controls have been added.

There are further changes too around the classification and ordering of controls based on the new ISO/IEC 27002:2022 which need to be conveyed to learners.

Transition requirements for IRCA certificated ISMS auditors

All IRCA Certificated ISMS auditors, irrespective of grade, are required to ensure their knowledge, skills, and experience pertaining to ISO 27001:2022 are current by the end of the three-year transition period in October 2025.

The recommended method of doing so is to through successfully completing an appropriate CQI and IRCA certified ISO 27001:2022 auditor training course. Alternatively, auditors are required to demonstrate the acquisition of the knowledge, skills and experience through appropriate CPD. This may include, but is not limited to, attending training courses, conferences or seminars; pursuing a course of online study or webinar; private study and reading.

CQI members with responsibility for information security management systems are also strongly encouraged to acquire the necessary knowledge, skill and understanding through appropriate CPD.

Appendix - Changes to ISO /IEC 27002 Annex A

Annex A remains a normative annex but is renamed from 'Reference control objectives and controls' to **'Information Security Controls Reference'** in the 2022 edition

Control objectives are removed from the 2022 list of controls.

There have been extensive changes to the content of this Annex, echoing the significant changes made in ISO/IEC 27002:2021.

The 14 categories of control (Information security policies, Organization of information security, Human Resource Security, Asset Management, Access Control, Cryptography, Physical and Environmental Security, Operations Security, Communications Security, System Acquisition, development and maintenance, Supplier relationships, Information Security Incident Management, Information security aspects of Business Continuity and Compliance) have been replaced by **four new 'themes': Organizational controls, People Controls, Physical Controls, and Technological Controls.**

The control objectives associated with the 2013 edition's 13 categories have all been deleted.

The third edition of ISO/IEC 27002 also

- classifies controls as 'corrective' 'preventive' or 'detective'
- identifies whether the control seeks to support 'confidentiality', 'integrity' or 'availability or a combination of these
- whether the control exists to 'identify', 'protect', 'detect', 'respond' or 'recover'.
- whether the controls relate to Governance, Asset management, Information protection, Human resource security, Physical security, System and network security, Application security, Secure configuration, Identity and access management, threat and vulnerability management, Continuity, Supplier relationships security, Legal and Compliance, Information security event management or Information security assurance.
- whether the control is linked to Governance and Ecosystem, Protection, Defence and Resilience

The total number of controls is reduced from 114 to 93. Some existing 2013 controls have been merged, some deleted, and some taken across 'as is'. Collectively, these changes account for 82 of the 93 controls in the 2022 edition. To this, 11 brand new controls have been added.

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

ISO/IEC 27002:2022 Annex B contains 2 useful tables mapping the 2022 controls to the 2013 controls and vice versa.

Should you require further clarification in respect of the contents of this briefing note, contact policy@quality.org.