Kenya Bureau of Standards

Standards for Quality life

TRANSITION GUIDE TO ISO/IEC 27001:2022

Issue 01

1.0 Direction on the use of this guide

This transition guide is designed to be read in conjunction with the latest available version of the ISO/IEC 27000 family of standards.

2.0 Overview

ISO/IEC 27001 is an internationally recognized standard for Information Security Management Systems (ISMS). It provides a systematic approach for managing, implementing, monitoring, reviewing, and improving information security within an organization. ISO/IEC 27001 is designed to help organizations protect their information assets. Information assets can include sensitive customer data, financial information, intellectual property, and any other data or information critical to the organization's operations.

New Release

New ISO/IEC 27001:2022 standard was published on 25th October 2022 as the 3rd edition standard, this revision came 10 years after the last revision in 2013. This is the greatest milestone for the information security sector considering the shift in the information security landscape across the whole world.

Highlights

updates of ISO/IEC 27001:2022 include a major change of Annex A, minor updates of the clauses, and a change in the title of the standard.

The latest version of ISO/IEC 27002 was published at the beginning of 2022, and its latest changes have also impacted ISO/IEC 27001.

Different from ISO/IEC 27001:2013, the new version's complete title is **ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection.**

The part that has gone under the most significant changes is Annex A of ISO/IEC 27001 which is aligned with the ISO/IEC 27002:2022 updates, published earlier this year.

ISO/IEC 27001 is an internationally recognized standard for Information Security Management Systems (ISMS)

3.0 Reasons for ISO/IEC 27001 Review

It's the norm of ISO to review all ISO and related management system standards under the rules by which they are written.

The objectives for review include:

a) To ensure the standard remains relevant in today's marketplace and in the future.

b) Enhance an organization's ability to ensure business continuity.

c) Adopt the change in the operating environment of the organization(context), technological advancement, and change in the information security landscape.

4.0 Why adopt an information security management system standard?

Adopting an Information Security Management System (ISMS) standard (ISO/IEC 27001) offers several compelling reasons which include the following.

Flexibility in cyber security and privacy

The revision is a game changer to the industry as major subjects in information security, cybersecurity, and privacy protection have been brought on board with clarity on the implementation. This has been necessitated by the evolution of technology and the adoption of new business practices as driven by the environment we operate in, some of these new working techniques include remote working and cloud-based data storage, etc.

In this case, organizations are expected to adapt to the new standard and implement the requirements to remain afloat in Information security, cybersecurity, and privacy protection.

Enhanced Security:

Implementing an ISMS standard helps organizations strengthen their information security posture. It provides a structured framework for identifying, assessing, and mitigating information security risks, which can reduce the likelihood and impact of security incidents.

Risk Management:

ISMS standards are built on a risk-based approach. They enable organizations to systematically identify, assess, and prioritize information security risks. This allows for more effective allocation of resources to address the most critical vulnerabilities and threats.

Legal and Regulatory Compliance:

Many industries and jurisdictions have specific regulations and legal requirements related to information security. Adopting an ISMS standard helps organizations align with these requirements, reducing the risk of non-compliance and associated penalties.

Customer Trust and Confidence:

Demonstrating commitment to information security through ISMS standards can enhance customer trust and confidence. It assures customers that their sensitive information is being handled with care and security.

Competitive Advantage:

In some industries, having ISO/IEC 27001 certification or compliance with other ISMS standards can be a competitive advantage. It may make an organization more attractive to clients, partners, and stakeholders who prioritize security.

Improved Incident Response:

ISMS standards often include guidelines for incident response and management. This helps organizations develop effective strategies for detecting, responding to, and recovering from security incidents.

Cost Savings:

By identifying and addressing security risks proactively, organizations can potentially avoid costly security breaches, downtime, and data loss. Preventing incidents is often more cost-effective than dealing with the aftermath.

Business Continuity:

Effective information security management contributes to business continuity by reducing the impact of disruptions caused by security incidents. Organizations can maintain operations even in the face of security challenges.

Better Supplier and Vendor Relationships:

ISO/IEC 27001 and similar standards are increasingly being requested by customers from their suppliers and vendors. Compliance with these standards can facilitate smoother business relationships and partnerships.

Internal Efficiency:

Implementing an ISMS standard promotes a structured approach to managing security. This can lead to improved internal efficiency, streamlined processes, and better resource allocation.

Employee Awareness and Training:

ISMS standards often include provisions for employee training and awareness programs. This helps educate staff about security risks and best practices, reducing the likelihood of insider threats.

International Recognition:

ISO/IEC 27001 is internationally recognized and respected. Achieving certification can be a valuable credential for organizations operating on a global scale.

In summary, adopting an ISMS standard is a strategic decision that can significantly benefit an organization by improving security, managing risks, ensuring compliance, enhancing customer trust, and providing a competitive edge. While it requires commitment and resources, the long-term benefits often outweigh the initial investment.

5.0 Comparison

Old 2013 Revision Published September 25, 2013		**New 2022 Revision** Published September 25, 2022
11	Number of clauses in the main part of the standard	11
114	Number of clauses in the main part of the standard	93
14	Number of sections in Annex A	4

6.0 Key Changes

Changes on main clauses (4 to 10) of ISO/IEC 27001:2022

The main requirements for an ISO/IEC 27001:2022 have changed slightly.
A brief overview of those changes is provided below:

S/NO	CLAUSES OF THE STANDARD
a	***Clause 4.2 Understanding the needs and expectations of interested parties***
	(c) which of these requirements will be addressed through the information security management system.
b	***Clause 4.4 Information security management system***
	besides requiring organizations to establish, implement, maintain, and continually improve their ISMS, it requires to do the same for the processes related to the ISMS and their interactions
c	***Clause 5.1 Leadership and commitment***
	provides a clarification regarding the term "business" used in the standard, which is used to refer to "those activities that are core to the purposes of the organization's existence."
d	***Clause 5.3 Organizational roles, responsibilities and authorities***
	Has some minor changes and specifies that the roles and responsibilities regarding information security should be communicated within the organization i.e. *"within the organization"*
e	***Clause 6.2 Information security objectives and planning to achieve them***
	introduces two new requirements. Item d) of this clause requires to monitor information security objectives i.e. *"be monitored"*
f	***Clause 6.3 Planning of changes***
	is a new requirement of ISO/IEC 27001:2022. It requires organizations to carry out the changes to the ISMS in a planned manner
g	***Clause 7.4 Communication has minor changes***
	Item (d) who shall communicate and item (e) the processes by which communication shall be affected have been merged to a new requirement: (d) how to communicate.

h	***Clause 8.1 Operational planning and control***
	The clause has been simplified and additional information has been provided on how to achieve the intended outcomes. This clause requires organizations to plan, carry out, and oversee processes that are essential to meet requirements by establishing criteria for the processes and implementing control of the processes in accordance with the criteria. The establishment of such criteria for ISMS processes allows organizations to evaluate the performance of the implemented processes and determine whether they conform to the established criteria.
i	***Clause 9.2 Internal audit***
	This clause has been divided into two subclauses: clause 9.2.1 General and clause 9.2.2 Internal audit programme to align with other management system standards; however, the requirements of this clause remain the same.
j	***Clause 9.3 Management review***
	This clause has been divided into three subclauses: clause 9.3.1 General, clause 9.3.2 Management review inputs, and clause 9.3.3 Management review results. This clause introduces a new requirement which states that the changes in needs and expectations of the interested parties that are relevant to the ISMS should be taken into account during management reviews. In addition, the new version of the standard refers to the outcomes of the management reviews as "results," and requires organizations to assure that evidence of such results is available as documented information.
k	***Clause 10 Improvement***
	This clause has been rearranged but its content remains unchanged.

Changes on Annex A of ISO/IEC 27001:2022

A control is defined as a measure that modifies or maintains risk. Some of the controls on ISO/IEC 27001:2022 are controls that modify risk, while others maintain risk. Annex A of ISO/IEC 27001:2022 contains information security controls that aim to ensure the confidentiality, integrity, and availability of information and information assets.

However, it should be noted that the information security controls listed in Annex A are not exhaustive and additional controls may be added as necessary by the organization. Annex A of ISO/IEC 27001:2022 has been updated and aligned with ISO/IEC 27002:2022 as some of the key changes include:

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

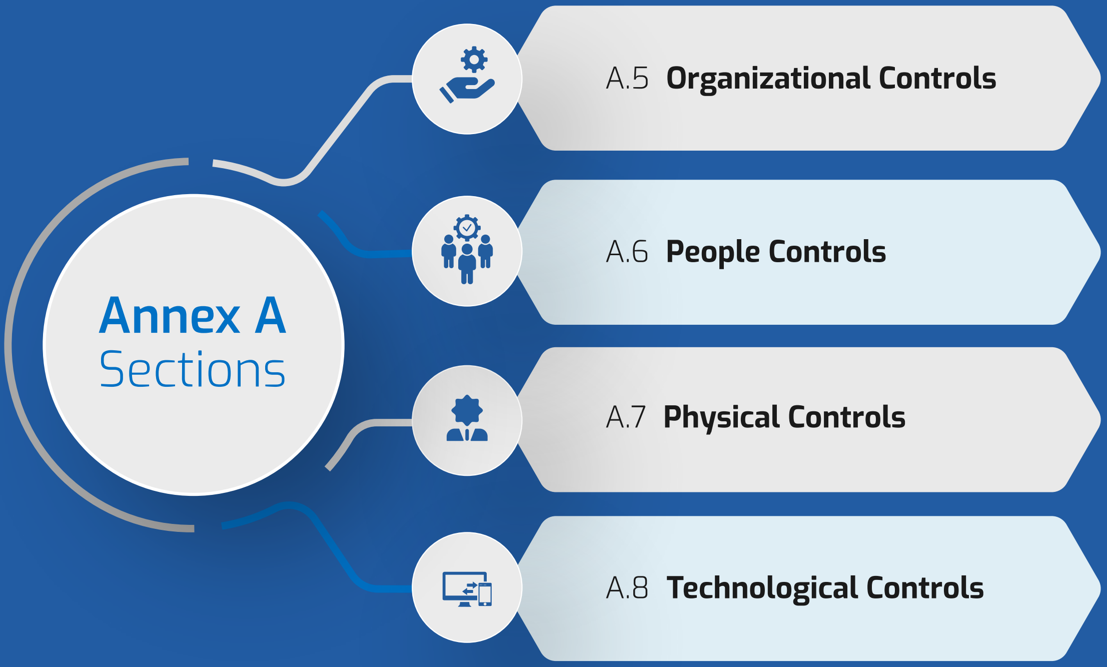
b) The number of controls in ISO/IEC 27002:2022 decreases from 114 controls in 14 clauses to 93 controls in 4 clauses.

c) On Annex A, 11 controls are new, 24 controls are merged from the existing controls, and 58 controls were updated.

d) Moreover, the control structure is revised, which introduces "attribute" and "purpose" for each control and no longer uses "objective" for a group of controls.

7.0 Themes re-organization

The new standard has re-organized and grouped controls into three themes based on functionality, including organizational, people, physical, and technological controls. This has been reduced from 14 themes to 4 themes as illustrated below.



Annex A Sections

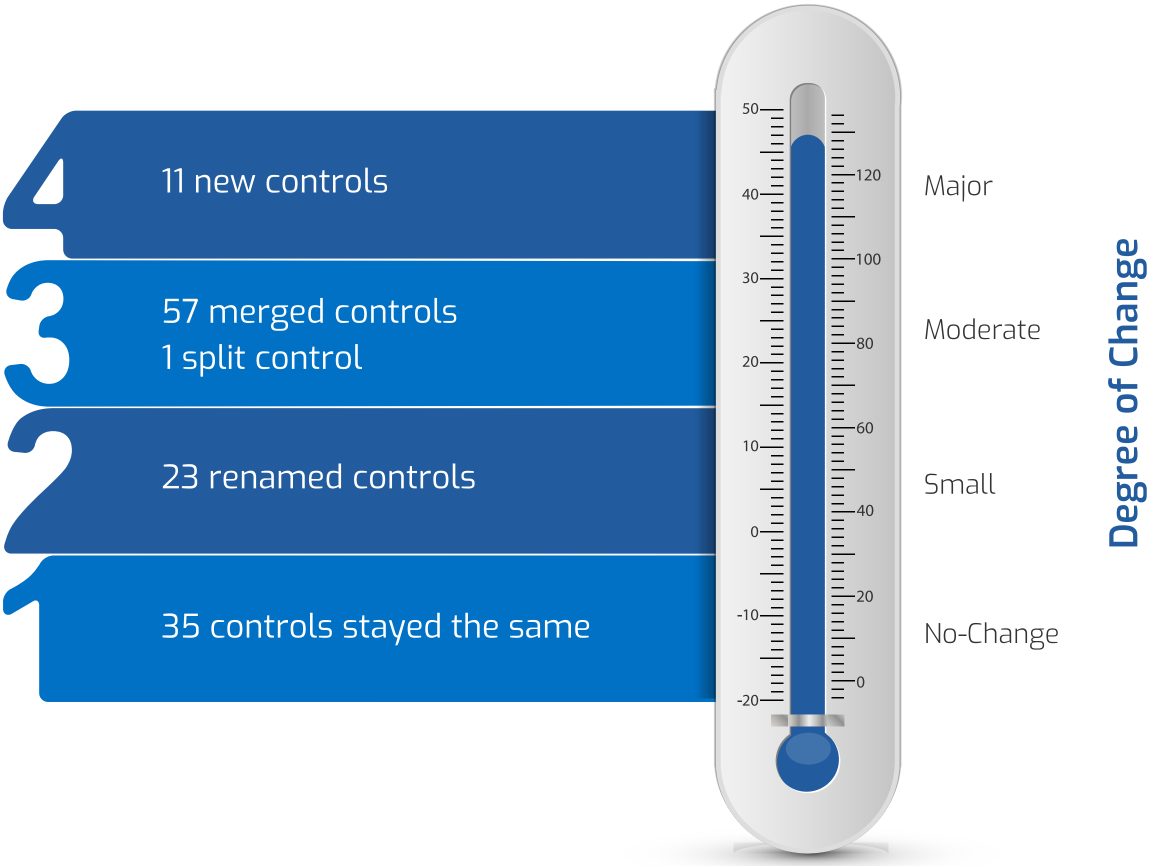
A.5 **Organizational Controls**

A.6 **People Controls**

A.7 **Physical Controls**

A.8 **Technological Controls**

8.0 Degree of change of Controls



4 — 11 new controls — Major

3 — 57 merged controls
1 split control — Moderate

2 — 23 renamed controls — Small

1 — 35 controls stayed the same — No-Change

Degree of Change

9.0 Controls Attributes

Attributes can be used to filter, sort or present controls in different views for different audiences. Each control on ISO/IEC 27001 Annex A has been associated with five attributes with corresponding attribute values. The following are five attributes associated with Annex A controls.

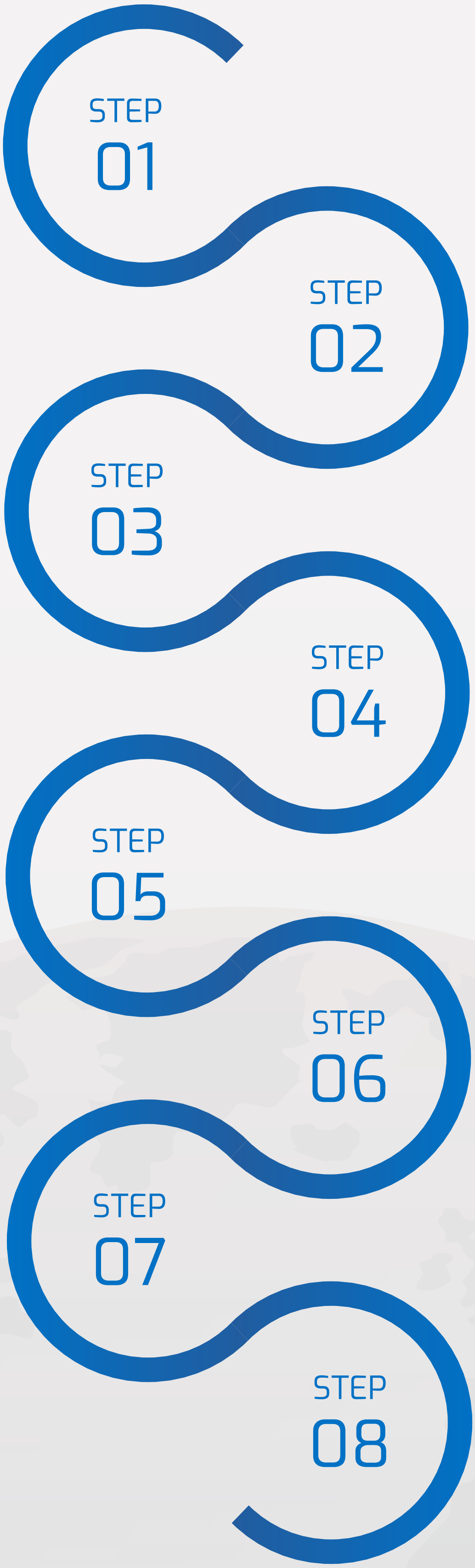
- Control types- consist of Preventive (the control that is intended to prevent the occurrence of an information security incident), Detective (the control acts when an information security incident occurs), Corrective (the control acts after an information security incident occurs) attributes values
- Information security properties (Confidentiality, Integrity, Availability)
- Cybersecurity concepts (Identity, Protect, Detect, Respond, Recover)
- Operational capabilities- an attribute to view controls from the practitioner's perspective of information security capabilities, consist of the following attribute values (Governance, Asset Management, Information protection, Human resource security, etc.)
- Security domains- Is an attribute to view controls from the perspective of four information security domains namely, Governance and Ecosystem, Ecosystem cybersecurity management, Protection and Defence.

10.0 The key timescale for Transition

KEBS certification body will start to certify and recertify clients on the new standard ISO/IEC 27001:2022 as from April 2023, Clients who were earlier certified to ISO/IEC 27001:2013 have 36 months to transit to the new standard from the day the new standard was released (October 2022). The following are the key activities and their key due dates for transition to ISO/IEC 27001:2022.

Activity	Due Date
Release of ISO/IEC 27001:2022 by ISO	***30th September 2022***
Initial certification by KEBS CB to ISO/IEC 27001: 2022 to begin no later than	6 months from the last day of publication month of ISO/IEC 27001:2022. ***April 2023***
Dateline for the certification body to issue initial or recertification audits against ISO/IEC 27001:2013	***29th April 2024***
KEBS CB transitions of certified clients completed by	36 months from the last day of publication month (September 2022) of ISO/IEC 27001:2022 ***The transition dateline is 31st October 2025***

Transition Steps



STEP 01

Purchase the revised standard ISO/IEC 27001:2022 from KEBS library of KEBS webstore *(webstore.kebs.org/)*

STEP 02

Build competence to implementers on new requirements, this can be acquired from our training department (NQI)

STEP 03

Gap analysis - Compare the current requirements against the changes in ISO/IEC 27001:2022

STEP 04

Review ISMS documentation to align with the revised and any new requirements

STEP 05

Sensitize all the staff on changes to ISMS documentation and the requirements of the standard

STEP 06

Implement the changes i.e. review IS risks, risk treatment plans and align controls as per the new standard.

STEP 07

Conduct Performance evaluation-collect data, analyze and evaluate, conduct internal audits, Management review and address any weakness in the management system

STEP 08

Apply for certification or recertification to the new standard ISO/IEC 27001:2022 by submitting your application to us on *https://ims.kebs.org/*

12.0 Further Information

For further information regarding certification and recertification to ISO/IEC 27001:2022 kindly contact Kimutai Davis Langat at *kimutaid@kebs.org* or write to the Head of the certification body on *certification@kebs.org*

Submit your applications for initial certification or recertification to ISO 27001 through KEBS CB online portal at ***https://ims.kebs.org***.

ISO / IEC 27001 REGISTERED FIRM
KEBS
INFORMATION SECURITY MANAGEMENT SYSTEMS

For any more information contact

Mr. Samson Ombok
HEAD OF CERTIFICATION BODY
KENYA BUREAU OF STANDARDS
P.O. BOX 54974-00200, NAIROBI
TEL: (254 20) 6948000 or 6005550 or (254 20) 6948263
E-mail: certification@kebs.org or omboks@kebs.org