ISO/IEC 27001:2022 ISMS Standard

Transition Guideline for Clients

Transition Guidance Document

Global Business Bureau Certification LLC ©

TESTING, INSPECTION & CERTIFICATION

The ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection - Information security management systems - Requirements" was published on October 25, 2022, and is set to replace ISO/IEC 27001:2013 via a three-year transition period. All organizations that wish to remain certified to ISO 27001 will need to transition to the 2022 revision of the standard within the set transition period which is expected to end in October 2025

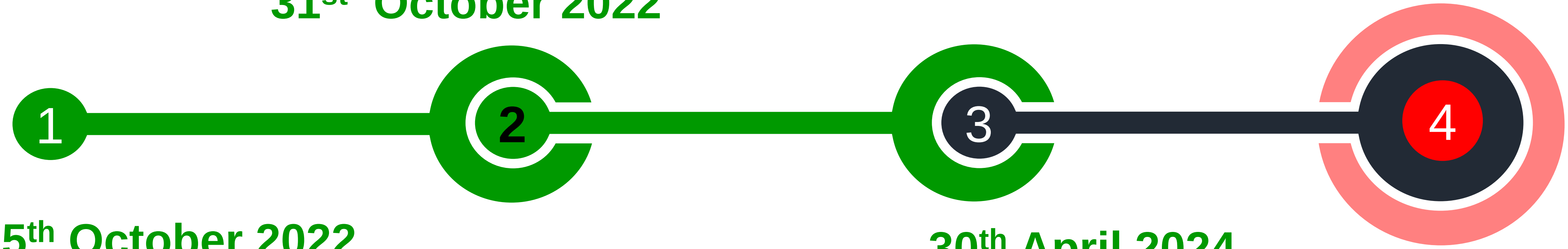
The new version of the standard features the controls outlined by ISO/IEC 27002:2022, and organizations will need to revisit their risk assessment to determine whether updates or new risk treatments need to be implemented.

Introduction

The goal of Global Business Bureau Certification LLC is to ensure a clear and smooth transition approach that is easy to our existing certified clients as well as clients who are certified with other reputable certification bodies accredited by recognized accreditation body. Our target is to provide our clients with the guidance and tools to make the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 as smooth as possible.

Transition Period

ISO 27001



25th October 2022

ISO/IEC 27001:2022, **released** as 3rd edition.

The transition period **starts**.

31st October 2022

30th April 2024

All initial (new) certifications should be according to the ISO/IEC 27001:2022 edition after this date and all recertification audits are recommended to use the ISO/IEC 27001:2022 edition after this date. GBBC will continue to accept applications for certification and issue new certificates against the ISO/IEC 27001:2013 standard until this date.

Transition period **ends**.

31st October 2025

ISO/IEC 27001:2013 certificates will no longer be valid after **31st October 2025.**

Changes reflected in ISO/IEC 27001:2022

The title of the standard was changed to *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* to align with the latest edition of ISO/IEC 27002. The title of the revised standard reflects its comprehensive scope, which includes both information security and cybersecurity. It is worth noting that while information security generally focuses on protecting information of all formats from unauthorized access, use, or modification, cybersecurity focuses on protecting digital assets from various threats, such as malware, hacking, and cyberattacks.

ISO/IEC 27001:2013

Information technology – security techniques – Information security management systems – Requirements

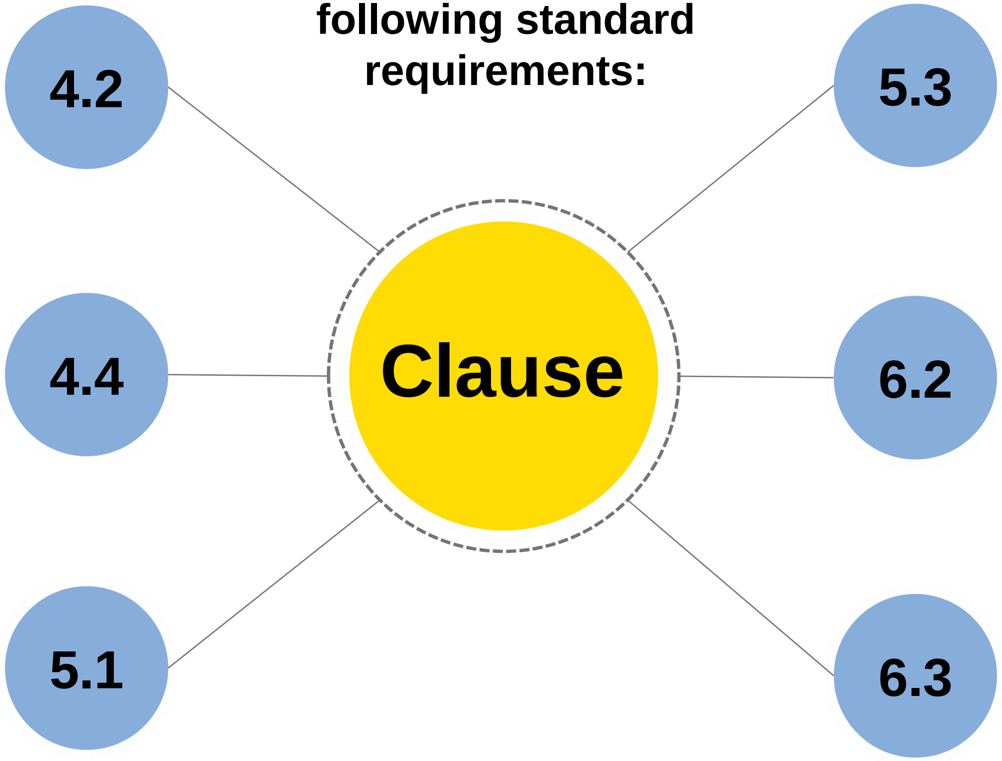
ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection – Information security management systems – Requirements

The Main Changes

ISO 27001

The main changes have been made in the following standard requirements:



4.2

Added new requirements.

Item c): to determine the requirements of interested parties that need to be addressed through the information security management system.

4.4

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.

5.1

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.”

5.3

has some minor changes and specifies that the roles and responsibilities regarding information security should be communicated within the organization.

6.2

Introduces two new requirements.

Item d) of this clause requires to monitor information security objectives,
Item g) requires ensuring they are available as documented information.

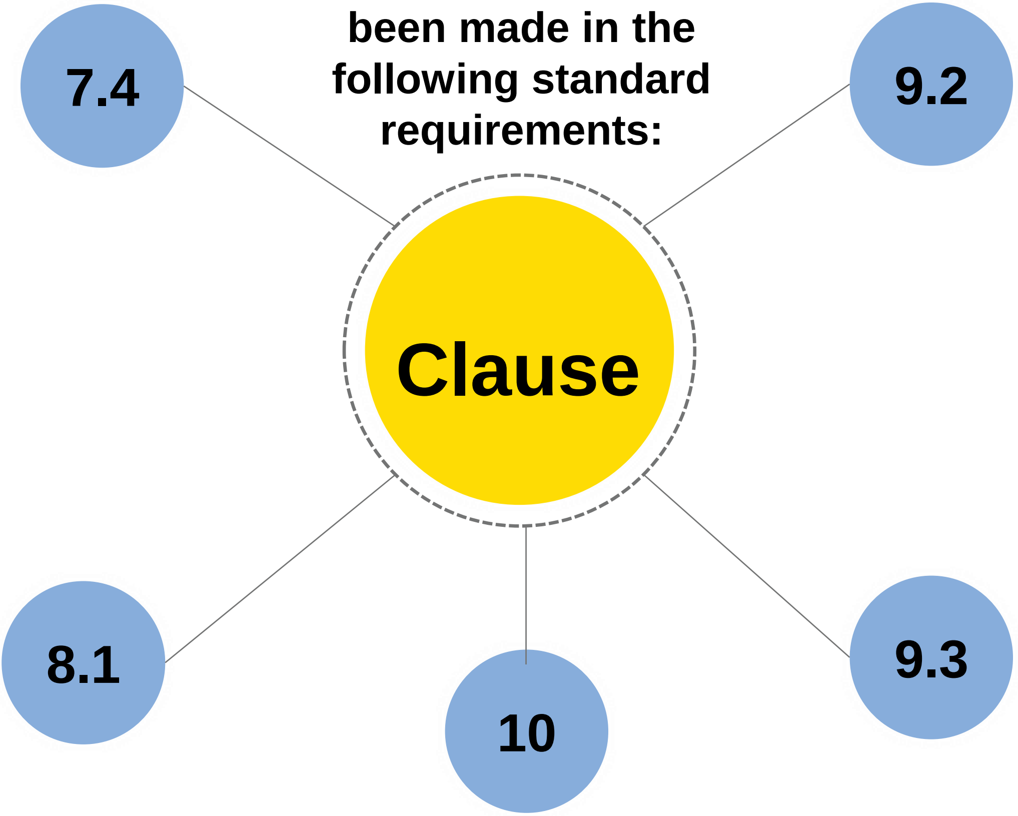
6.3

a new requirement of ISO/IEC 27001:2022. It requires organizations to carry out the changes to the ISMS in a planned manner.

The Main Changes

ISO 27001

The main changes have been made in the following standard requirements:



has minor changes. **Item (d)** who shall communicate, **Item (e)** the processes by which communication shall be affected have been merged to a new requirement: (d) how to communicate.

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.

has been rearranged but its content remains unchanged.

has been divided into two subclauses:

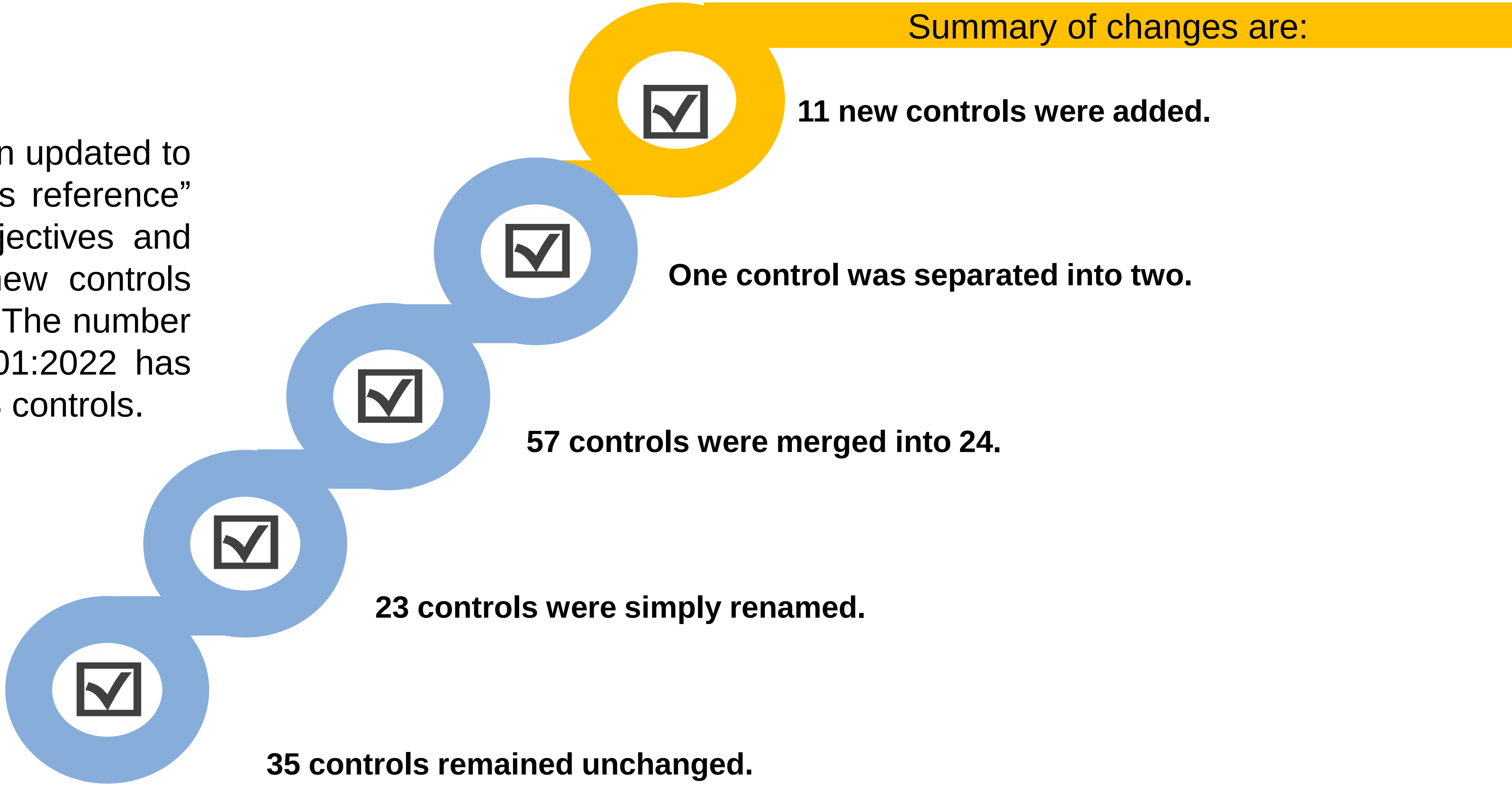
Clause 9.2.1 General and
Clause 9.2.2 Internal audit programme to align with other management system standards; however, the requirements of this clause remain the same.

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 considered during management review. In addition, the new version of the standard refers to the outcomes of the management review as “results,” and requires organizations to assure that evidence of such results is available as documented information.

The Annex A Key Changes

The title of Annex A has been updated to “Information security controls reference” from “Reference control objectives and controls”. Additionally, 11 new controls were added to the Annex A. The number of controls in ISO/IEC 27001:2022 has been reduced from 114 to 93 controls.



Summary of changes are:

- ☑ 11 new controls were added.
- ☑ One control was separated into two.
- ☑ 57 controls were merged into 24.
- ☑ 23 controls were simply renamed.
- ☑ 35 controls remained unchanged.

Transitioning to ISO/IEC 27001:2022

ISO 27001

Organizations that are certified against ISO/IEC 27001:2013 can initiate to update their ISMS based on ISO/IEC 27001:2022 at any time.

GBBC will provide transition audits against ISO 27001:2022 after the successful assessment by the associated accreditation body.

Initial audit and Recertification audit against ISO 27001:2022 standard will only commence on **30th April 2024.**

There are steps that the Organizations can do…

Steps in transitioning to ISO/IEC 27001:2022

ISO 27001

Conduct a gap analysis to understand their existing ISMS and determine the changes required to fulfil the requirements of the ISO/IEC 27001:2022 standard.

Documentation and certain processes will likely need to be updated, including evidence of new or modified process changes.

Management needs to have confidence that it can produce evidence to support the implementation of any new or modified processes.

Additionally, the Statement of Applicability (SoA) will need to be updated to reflect changes to implemented controls and to conform with ISO/IEC 27001:2022.

Assess the information security risks and determine the information security controls that should be implemented.

Review and update the risk treatment plan (where required).

Plan and conduct role-based training regarding the new standard requirements, if necessary.

Implement controls to meet new requirements.

Conduct an internal audit to assess the ISMS compliance.

Conduct management review.

Contact GBBC to conduct ISO/IEC 27001:2022 transition audit and obtain certification.

How Global Business Bureau Certification Can Assist You?

ISO 27001

Global Business Bureau Certification LLC (GBBC) team is available to support you throughout the transition process. If you have any questions or need any help, we can support you with:

01

Pre-Assessment / Gap Analysis: GBBC can provide a Pre-Assessment or Gap Analysis of your revised ISMS to determine the level of compliance of your ISMS to the requirements of ISO/IEC 27001:2022.

02

Awareness and Training: GBBC can provide a transition guidance awareness and implementation training for your management and staff for better understanding of the revised ISO/IEC 27001 standard.

Thank you!

Please contact us:

☎ 00971503224246

✉ info@gbbcert.com