

Release No. 48: **ISO/IEC 27001:2013 transition to ISO/IEC 27001:2022**

Applicable for: Prospects and clients with an ISO/IEC 27001 certification

Date: March 23, 2023

Update date: February 20, 2024

Dear Customer:

We hereby wish to inform you that we are currently in transition from the ISO/IEC 27001 standard from version 2013 to 2022, so it is important that all organizations with a certification in this scheme consider the following points:

1. General requirements for transition from ISO/IEC 27001:2022:

- The transition period is 3 years from the publication of ISO/IEC 27001:2022, this period will expire on October 25, 2025.
- Initial, surveillance, and recertification audits under ISO/IEC 27001:2013 version may be conducted until October 25, 2024. Starting from that date, Global Standards will only conduct audits under the ISO/IEC 27001:2022 version.
- Transition audits to ISO/IEC 27001:2022 version may be conducted until August 25, 2025, allowing sufficient time for the closure of non-conformities before the certificates under ISO/IEC 27001:2013 version become invalid (on October 25, 2025).

2. Main changes.

- The standard change its title to ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management System - Requirements.
- Extension of the subsections of clauses 6. Planning, 7. Support, 9. Performance evaluation and 10. improvement.
- Sections 4.2 Understanding stakeholders needs and expectations, 6.1.3 Information security risk management, 6.2 Information security objectives and planning to achieve them are added and or modified.
- 7.4 Communication and 9.2.2 Internal Audit Program are added
- ANNEX A is modified and renamed as reference of information security controls; a reduction from 114 controls to 93 controls is made. 11 new controls are added: 5.7 Threat intelligence, 5.23 Information security for use of cloud services, 5.30 ICT preparedness for business continuity, 7.4 Physical security monitoring, 8.9 Configuration management, 8.10 ICT disposal for business continuity, 8.11 Data masking, 8.12 Data leakage prevention, 8.16 Tracking activities, 8.23 web filtering, 8.28 secure encryption.

3. Recommendations for organizations / clients under ISO 27001:2013.

- Acquire / obtain the ISO 27001:2022 Standard.
- Identify the issues / requirements in your Management System that must be addressed to meet the new requirements.
- Develop and carry out an implementation plan.
- Be sure to meet and / or update the new competition needs and raise awareness among the personnel involved about the impact of said changes and their effectiveness within the Management System.
- Perform an internal audit and management review on the changes implemented to validate the effectiveness of the Management System.
- When appropriate and ready, contact your GlobalSTD Business Executive to make the necessary arrangements for your transition event.

4. Issuance of certificates in the ISO/IEC 27001:2022 standard

- After the transition period expires (October 25, 2025) only ISO/IEC 27001:2022 accredited certificates will be valid.
- The expiration date of the certificates in ISO/IEC 27001:2013 issued during the transition period will be October 25, 2025 (end of the transition period).

For more information, please contact us by phone: 33 3630 4546 Ext 163, 174 o 151 or by email:
comite@globalstd.com, staff_sgi@globalstd.com.

Regards,

Certification Committee
Global Standards

End of transition announcement ISO/IEC 27001:2013 to ISO/IEC 27001:2022