TRANSITION TO ISO 27001:2022

This document explains the transition guideline for ISO 27001-2022 and intent to be used by the certified client of the TNV System Certification Pvt. Ltd

This document is based on the following requirement:

- ISO 27001-2022
- ISO 27000-2022
- IAF MD 26 for Transition of ISO 270011-2022

Introduction of ISO 27001-2022

The new ISO/IEC 27001:2022 has been published on October 25, 2022. Some of the main new 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 (Information security, cybersecurity and privacy protection — Information security controls) has been published at the beginning of 2022, and its latest changes have also impacted ISO/IEC 27001.

The new changes of ISO/IEC 27001:2022

- in response to the ever-changing security landscape, the globally acknowledged standard ISO/IEC 27001, designed to safeguard the confidentiality, availability, and integrity of an organization's information assets, has been refreshed and unveiled in its newest, more pertinent version.
- While ISO/IEC 27001:2013 is its predecessor, the latest edition is officially titled ISO/IEC 27001:2022 Information Security, Cybersecurity, and Privacy Protection.
- The section undergoing the most substantial revisions is Annex A of ISO/IEC 27001, reflecting the updates made in ISO/IEC 27002:2022 released earlier this year.
- Regarding other sections, clauses 4 through 10 have seen a range of subtle modifications, with notable additions in clauses 4.2, 6.2, 6.3, and 8.1. Further refinements include slight terminology adjustments and rephrasing within various sentences and clauses.

What is unchanged?

Nonetheless, the sequence and titles of these clauses have been retained unchanged.

- Clause 4 Context of the organization
- Clause 5 Leadership
- Clause 6 Planning
- Clause 7 Support
- Clause 8 Operation
- Clause 9 Performance evaluation
- Clause 10 Improvement

What are the main control changes in Annex A?

- Annex A in ISO/IEC 27001:2022 has experienced alterations in the quantity of controls and their organization into groups. The title for this Annex has been updated from "Reference control objectives and controls" to "Information security controls reference." As a result, the reference objectives once associated with each control group in the prior version have now been eliminated.
- The control count in Annex A has been reduced from 114 down to 93. This reduction largely stems from the consolidation of several controls: 35 controls remain unchanged, 23 have been renamed, 57 have been combined into 24, and one control has been split into two. These 93 controls are now organized into four distinct control groups or categories.

Highlight of the changes in controls

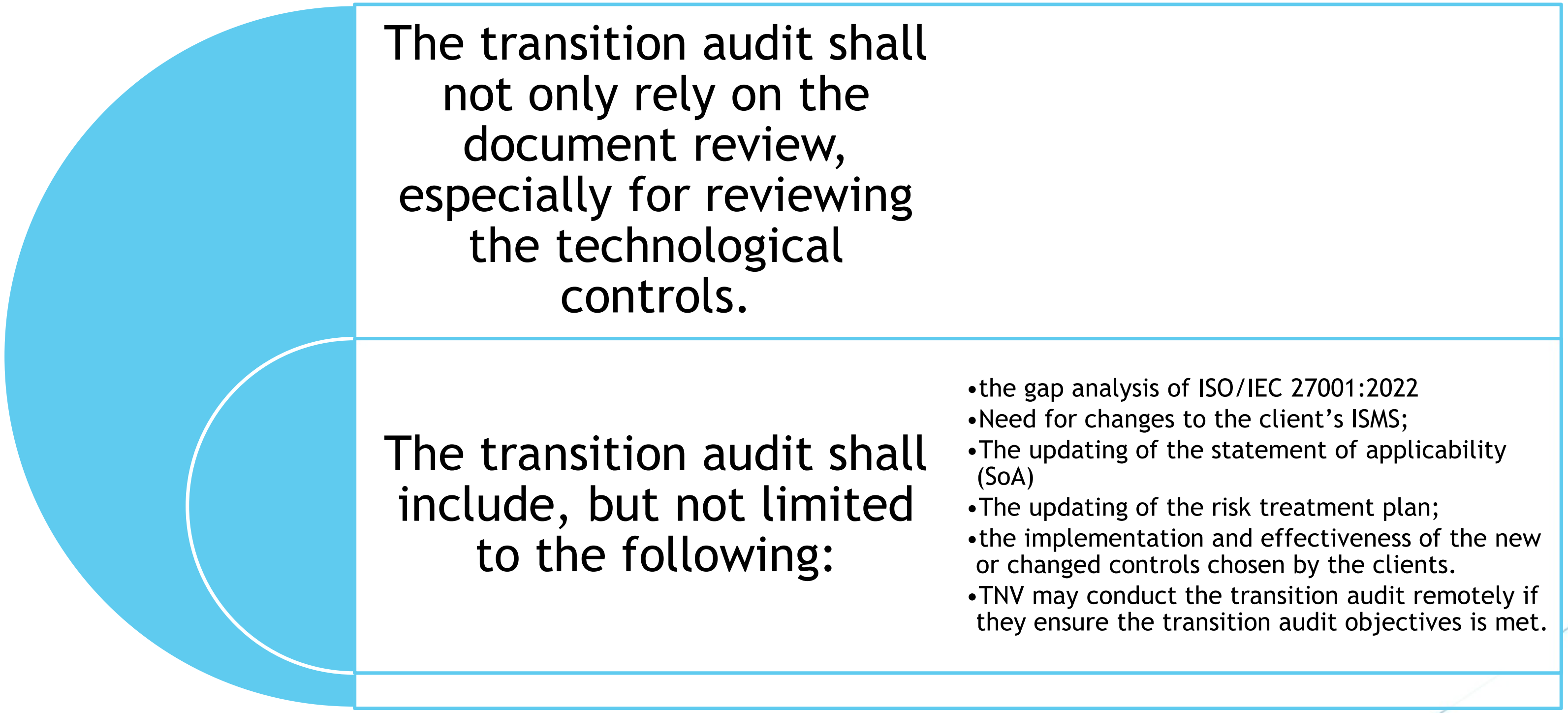
The new control groups of ISO/IEC 27001:2022 are:

- A.5 Organizational controls - contains 37 controls
- A.6 People controls - contains 8 controls
- A.7 Physical controls - contains 14 controls
- A.8 Technological controls - contains 34 controls

ISO/IEC 27001:2022 added the 11 new controls to its Annex A:

- Threat intelligence
- Information security for the 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

The transition method



The transition audit shall not only rely on the document review, especially for reviewing the technological controls.

The transition audit shall include, but not limited to the following:

- the gap analysis of ISO/IEC 27001:2022
- Need for changes to the client's ISMS;
- The updating of the statement of applicability (SoA)
- The updating of the risk treatment plan;
- the implementation and effectiveness of the new or changed controls chosen by the clients.
- TNV may conduct the transition audit remotely if they ensure the transition audit objectives is met.

Audit duration for Transition Audit

As a minimum, the audit shall include an additional 0.5 auditor day to confirm transition of the certified clients when the transition is done during a surveillance audit or as a separate audit. But if planned with recertification, no addition of mandays is required.

Consequence of Transition

- TNV have defined the timeline for submitting the transition application by the certified clients in the transition audit programme;
- TNV shall make the transition decision based on the result of transition audit;
- TNV shall update the certification documents for the certified client if its ISMS meets the requirements of ISO/IEC 27001:2022;
- On the certification document is updated because the client successfully completed only the transition audit, the expiration of its current certification cycle will not be changed.
- All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period that is October 2025.

The transition Audit may be planned:

- As special transition assessment of ISO 27001:2022.
- Along with surveillance assessment;
- Along with recertification of the client;

Transition Timeline

Submit the Transition Plan by March 2024

Complete the transition by October 2024

Last date of validity of the certificate ISO 27001-2013 is October 2025

Analytics of Changes

ISO 27001-2022

Clause 4 to 10 have minor update only

Number of control decreased to 93

93 controls are restructured in 4 Group

11 New Controls have been introduced

Revise your SOA

Transition Need to be completed by Client October 2024

ISO 27001-2013 Validity will be limited to October 2025

How to plan the Transition?

Review the changes

- Review the new requirement from changes
- Conduct the Gap Analysis

Plan the implementation

- Train the people based on GAP
- Change your document, process and review the effectiveness

Verification of Transition

- Request a independent Verification by TNV
- Or Plan it with Surveillance audit or recertification

Plan your Transition

Review the changes

- Review the new requirement from changes
- Conduct the Gap Analysis

Plan the implementation

- Train the people based on GAP
- Change your document, process and review the effectiveness

Verification of Transition

- Request a independent Verification by TNV
- Or Plan it with Surveillance audit or recertification

Need any help

- In case you need any help, please feel free to contact us at tnvceo@gmail.com
- You may download the transition plan, guideline and related document on https://tnvgroup.org/iso_downloads.php?category=Transition%20Documents