NQA, USA ISO 27001:2022 Transition Plan

ISO 27001:2022 "Information security, cybersecurity and privacy protection – Information Security Management Systems – Requirements" was released in October 2022 and is set to replace ISO 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 ends in October 2025.

It is NQA's goal to maintain a straightforward transition approach that is easy for all of our clients to apply, along with the guidance and tools to make the transition from ISO 27001:2013 to ISO 27001:2022 as smooth as possible.

The overall allowable transition period will span the three years from October 2022 through October 31, 2025. During that period both versions of the ISO 27001 standard remain valid and audits to either version of the standard may be conducted subject to the rules noted below, but plans should be made for an organization's transition to fully occur prior to the transition period ending.

Detailed Transition Period:

- **October 25, 2022** – ISO/IEC 27001:2022 3rd edition - **Release date**
- **October 31, 2022 – Transition period begins.**
    - All existing certificates to ISO 27001:2013 will expire 36 months from the last day of the month of publication of ISO 27001:2022.
- **April 1, 2024** - All initial (new) certification audits *should* be conducted against the ISO 27001:2022 edition after this date and all recertification audits are recommended to be conducted to the ISO 27001:2022 edition after this date.
    - NQA will continue to accept applications for certification and issue new certificates against the ISO 27001:2013 standard until this date.
- **August 31 2025** – Target date for all transition audits to be conducted by.
- **October 31, 2025** - **Transition period ends.**
    - Certificates for ISO 27001:2013 will no longer be valid after this date.

NQA, USA ISO 27001:2022 and ISO 27002:2022 Change Analysis:

NQA, USA views the ISO 27001:2022 revision as a moderately significant set of changes. This is due in-part to the changes within the structure of Annex A:

- The **Annex A** controls have been *regrouped from 14 control objectives to 4 broad themes* that include: **Organizational, People, Physical, and Technological Controls.**

The information and concepts provided within **ISO 27002:2022** is worth noting in respect to the transition. While ISO 27002:2022 is not auditable, NQA highly recommends that organizations use ISO 27002:2022 in conjunction with ISO 27001:2022 in their implementation of the changes.

- Each control is greatly expounded upon within ISO 27002:2022 providing additional background, guidance and examples that will aid in the implementation of said controls.
- ISO 27002:2022 provides two cross-reference tables which map forward (2013 to 2022) and backward (2022 to 2013) the full set of controls within Annex A. This in itself, will save organizations hours of time in trying to do this on their own.
- ISO 27002:2022 also introduces the concept of attributes by which organizations can create tags for the ISMS controls to more easily review their ISMS posture through various perspectives. While this is not required within ISO 27001:2022, it may be a useful exercise for organizations.

Beyond the structural changes in Annex A, 11 new controls have been introduced within Annex A including:

- Threat Intelligence
- Information Security for use of Cloud Services
- Physical Security Monitoring
- Configuration Management
- Information Deletion
- Data Masking
- Data Leakage Prevention
- Web Filtering
- Secure Coding

The overall number of controls within Annex A stands at **93 controls** compared to the 114 controls in the previous edition. This is NOT to say the controls have been eliminated, rather several previous controls have been consolidated into broader new single controls. The cross-reference tables noted in ISO 27002:2022 show that no controls have been deleted per se.

Finally, in addition to the significant structural changes to Annex A, **several changes have been made within the body of the ISO 27001 standard's requirements** to better align with the harmonized structure for management system standards (i.e. Annex SL).

Of note, **changes have been made in the following requirements**:

- 4.2 Understanding the needs and expectations of interested parties
- 4.4 Information security management system
- 6.2 Information security objectives and planning to achieve them
- 6.3 Planning of changes
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.3.2 Management Review inputs
- 10.1 Continual Improvement & 10.2 Nonconformity and Corrective Action (numbering change only)

NQA, USA has developed the **ISO 27001:2022 Transition Checklist** in order to provide more detailed interpretation and guidance on the changes within the standard. We encourage organizations to use this checklist as a tool to facilitate and record the changes within their management system and to retain this document for review at their transition audit. NQA auditors will use this very same Transition Checklist during the transition audits.

CLENT PREPARATION and CERTIFICATION

Preparing for transition:

- Organizations must transition their management system in accordance with the requirements to ISO 27001:2022 before their NQA transition audit is conducted. This should include any documentation changes, along with evidence of any new or changed process requirements and controls.
- Of note, organizations must conduct an internal audit and management review of the new/changed requirements and controls prior to their NQA transition audit being conducted.
- Prior to their NQA transition audit, organizations may elect to schedule an NQA transition gap assessment audit to test their readiness. This could be conducted in conjunction with a scheduled ISO 27001:2013 audit, or may be conducted as a stand-alone event prior to their NQA transition audit.

Transition Audits:

- All organizations must complete a successful NQA transition audit to confirm the effective implementation of the revised standard. The transition audit may be conducted in conjunction with an existing surveillance or re-assessment audit, or may be conducted as a stand-alone audit.
- Due to the nature and volume of the changes, additional audit time will be required to be added to audit durations in order to verify the new and changed requirements and controls introduced by ISO 27001:2022 have been met.
  - Generally, 0.5 day additional time will be added for transitions conducted in conjunction with a Transition Re-Assessment.
  - Generally, 1.0 day additional time will be added for transitions conducted in conjunction with a Transition Surveillance.
- If a stand-alone audit is requested for the transition audit, the duration will be calculated on an individual organization basis*.

***Note:** Specific audit durations for transition will depend on the actual situation of the organization including the organization's size and the complexity of the ISMS. Your NQA CSR will advise you of your specific transition audit duration.*

Issuing ISO 27001:2022 Certificates:

- As with any audit, non-conformances identified during a transition audit will require all corrective action plans to be submitted to NQA and approved. An updated ISO 27001:2022 certificate will be issued following all corrective action plan(s) approval.
- Updated ISO 27001:2022 certificate issuance and validity will be as follows:
    - All current ISO 27001:2013 certificates have been revised to reflect a Valid Until Date of no later than October 31, 2025.
    - Transition Surveillance –The organization's original Valid Until Date will be restored (maintaining the existing 3 –year certification cycle).
    - Transition Re-assessment – A new Valid Until Date will be issued for the renewed 3-year period (based on existing certification cycle).
    - Stand-alone Transition Audit – The organization's original Valid Until Date will be restored (maintaining the existing 3 –year certification cycle).

Additional support

The NQA Team is here to support clients throughout the transition process and can answer questions or provide resources as needed.

- **Technical Advice-** Please call us with any questions you have: CSRs are well-versed in many of the transition aspects and can address many initial questions. The NQA technical team of CTO’s and Business Unit leaders are just a quick call away if more in-depth conversations are needed.

- **Transition Training-** NQA will be providing 27001:2022 Transition Training in both on-demand (e-learning) and live (virtual) formats; please see the NQA website to sign up. (www.nqa.com)

- **Outside Assistance (Training/Consulting)**- While NQA does not provide consulting services, CSR’s can provide connections for many reputable training and consulting firms that NQA is aware of.

- **Transition Gap Assessment-** CSR’s can schedule a transition gap assessment to determine the level of conformance to the requirements of ISO 27001:2022 prior to your transition audit.

For any questions or to speak to someone regarding transitions
please contact the NQA Team!