Inspired by
Knowledge

Customer Information ISO/IEC 27001:2022 - Transition

Important information about your existing ISO 27001 certification

Dear ISO 27001 Certification Customer,

As you may have heard, ISO/IEC 27001 was revised and published as the international standard ISO/IEC 27001:2022 in October 2022.

The "International Accreditation Forum" (IAF) has defined
in IAF document MD 26 of 15.02.2023, a three-year transition period and some transitional measures. This means that after the transition period, all ISO 27001 certifications must be based solely on the revision of the standard and all certificates based on the old edition of the standard will become invalid, regardless of the expiry date stated on the certificate.

The national accreditation bodies that are part of the IAF have published rules for the transition of certification from the original version of ISO/IEC 27001:2013 to ISO/IEC 27001:2022.
One of the responsibilities of certification bodies is to inform certified customers of the arrangements for transition to ISO/IEC 27001:2022 certification.

Note

Both the certification bodies TÜV NORD CERT and TÜV NORD Czech have applied for extension and transition of accreditation to the revision of the standard.

Continuation of ISO 27001 certification with revision of the standard

Please note the following general conditions defined by the IAF: All existing ISO/IEC 27001:2013 certificates expire on
31.10.2025, unless the transfer is made before that date. Each initial certification audit and recertification audit commencing on or after 1 May 2024 shall be conducted against the ISO/IEC
27001:2022. The starting point is the first day of the on-site audit (audit phase 1).

All certification decisions for the transfer of existing ISO/IEC 27001:2013 certifications must be completed by 31 October 2025 at the latest. Otherwise, a new full initial certification shall be made.

Transition audits require additional on-site audit coverage. This additional scope is one-off and applies only to the transition audit.

We will charge certified customers for the cost of this additional audit scope.

The transition may be carried out in the form of a recertification or surveillance audit, or as an extraordinary audit.

Audits according to the revision of ISO/IEC 27001 can only be performed by audit teams that have been in the new
requirements trained and formally approved for audits under the new standard.

Activities of organisations seeking to move to ISO/IEC 27001 certification

The extent of change required depends on the maturity and effectiveness of the existing Information Security Management System (ISMS), organisational structures and processes/procedures in each organisation. Therefore, an impact assessment/weakness analysis is strongly recommended to determine the impact on resources and timelines.

Organizations that have an ISMS based on ISO/IEC 27001:2013 are recommended to take the following measures:

- identify gaps in the company that need to be addressed to meet the new requirements;
- Prepare a transition plan.
- Ensure adequate training and build awareness of all stakeholders that have an impact on the effectiveness of the organisation;
- update the existing ISMS to meet the revised requirements and provide evidence of effectiveness.

Please note that the transition audit must demonstrate a full internal audit and assessment of the management system in accordance with the revision of ISO/IEC 27001:2022.

Rules for calculating the additional audit scope

In the transitional requirements of the IAF and national accreditations, Chapter 4.2 of IAF MD 26:2022 contains a modification the additional audit scope required for transitional audits. We have decided to adopt this approach and to adapt it to the type of audit (single site or multi-site audit). Finally, the following result for the additional audit scope (as time spent on site)

	AUDIT TO 1 LOCATED AT	AUDIT FOR MORE LOCATIONS
Transition at recertification audit	0.5 man-days Plus	0.5 extra man-days for the head office a 0.125 man-days in addition to one workplace at sampling
Transition at Regular by checking audit	1.0 man-day Plus	1.0 extra man-day for the head office a 0.125 man-days in addition to one workplace at sampling
Transition in within extraordinary (separate) audit	1.0 man-day Plus	1.0 extra man-day for headquarters and 0.125 man-days in addition to one workplace at

Note

If the transition takes place as part of an extraordinary audit, its scope should be calculated as a control audit with the increase in scope mentioned here, which is definitely a more costly solution.

The initial certification audit (Phases 1 and 2) for ISO/IEC 27001:2022 requires no additional transition time and can replace any other transition audit.

In exceptional circumstances, this approach may be modified.

In the case where transfer of certification to another certification body is intended, the transfer of certification according to ISO/IEC 27001:2013 before proceeding in planning the transition audit described above.

After an extraordinary, control or recertification transition audit, a new certificate is issued with the same validity date as the previous certificate according to ISO/IEC 27001:2013.

A new three-year certification cycle can only be started after a recertification audit has been carried out.

Summary

In order to continue the successful certification of the ISMS according to ISO/IEC 27001, the system must be adapted to the updated standard. This requires effort, time and money, but results in increased resilience to unwanted influences.

We look forward to working with you again.

Contact

Mgr. Viktor Šaroch, Ph.D.

TÜV NORD Czech, s.r.o.
Českomoravská 2420/15
190 00 Prague 9
Czech Republic

T 602 664 895

viktor.saroch@tuev-nord.cz
www.tuev-nord.cz