TÜVNORD

Inspired by
Knowledge

Client Information
“ISO/IEC 27001:2022” – Transition

Important information about your existing ISO 27001 certification

Dear ISO 27001 certification client,

As you have probably heard already, ISO/IEC 27001 was revised and published as International Standard ISO/IEC 27001:2022 in October 2022.

The “International Accreditation Forum” (IAF) has defined in IAF document IAF MD 26, dated 15.02.2023, a three-year transition period and some transitional arrangements. That means that after the transition period, any certification according to ISO 27001 must be based exclusively on the new edition, and all certificates based on the old edition become invalid, independent of the expiry date noted in the certificate.

The German Accreditation Body (DAkkS) published a transition guide for ISO/IEC 27001:2022 accreditations on 01.01.2023. Informing certified clients about the transitional arrangements for certification to ISO/IEC 27001:2022 is one of the obligations set out therein.

Note
The statements made in this letter regarding ISO/IEC 27001:2013 also apply analogously to the German translation of ISO/IEC 27001:2013, the standard DIN EN ISO/IEC 27001:2017.

TÜV NORD CERT has submitted an application for extension and transition of accreditation to the new edition of the standard.

Continuation of ISO 27001 certification with new standard edition

Please note the following general conditions defined by IAF: All existing ISO/IEC 27001:2013 certificates will become invalid on 31.10.2025, if transition has not been completed before. Any initial certification audit and recertification audit starting on 01.05.2024 or later shall be performed based on ISO/IEC 27001:2022. The starting point is the first day of the on-site audit (audit stage 1).

Any certification decisions to convert existing ISO/IEC 27001:2013 certifications shall be completed by 31.10.2025 at the latest. Otherwise, a new full initial certification shall be performed.

Transition audits shall require an additional audit duration on site. This extra duration is a single event only valid for the transition audit.

We will charge certified clients for the cost of this additional audit duration.

Transition can be performed in the form of recertification or surveillance audits or as a “special case” audit.

Audits according to the new edition of ISO 27001 may only be carried out by audit teams that have been trained on the new requirements and have been appointed for the new standard.

Activities of organizations seeking a transition of their ISO 27001 certification

For each organization, the extent of change required depends on the maturity and effectiveness of the current information security management system (ISMS), organizational structures and processes/procedures. Therefore, in order to identify the impact on resources and deadlines, it is strongly recommended to perform an impact analysis/gap assessment.

Organizations using an ISMS based on ISO 27001:2013 are recommended to take the following actions:

- Identify organizational gaps that need to be addressed in order to meet new requirements.
- Preparation of a transition plan.
- Provide appropriate training and build awareness for all parties that influence the effectiveness of the organization.
- Update the existing ISMS to meet the revised requirements and provide evidence of effectiveness.

Please keep in mind that a full internal audit and an evaluation of the management system according to the new edition of ISO/IEC 27001:2022 must be demonstrated in the transition audit.

Calculation rules for additional audit duration

In the transition requirements of IAF and DAkkS, chapter 4.2 of the IAF document IAF MD 26:2022 contains a regulation on the additional audit time required in transition audits. We have decided to adopt this approach and modify it with regard to the type of audit (single-site audit or multi-site audit). This leads to the following result for the additional duration (as on-site time):

	SINGLE-SITE-AUDIT	MULTI-SITE-AUDIT
Transition in arecertification audit	0.5 man days of additional duration	0.5 man days of additional duration for the headquarters and 0.125 man days of additional duration per site in the sample
Transition in aregular surveillance audit	1.0 man days of additional duration	1.0 man days of additional duration for the headquarters and 0.125 man days of additional duration per site in the sample
Transition in a special (separate) audit	1.0 man days of additional duration	1.0 man days of additional duration for the headquarters and 0.125 man days of additional duration per site in the sample

Note
If the transition is carried out in a special case audit, then this must be calculated as a surveillance audit with the additional duration described here – this definitely represents a more expensive solution.

A full initial certification audit (stage 1 and 2) for ISO/IEC 27001:2022 does not require any additional audit time for transition and can replace any other transition audit.

Under special circumstances, it may be necessary to adapt this approach.

If a transfer from one certification body to another is intended, the transfer of certification according to ISO/IEC 27001:2013 must be fully completed before the planning of a transition audit (as described above) may continue.

After a transition in the form of a special case audit, a surveillance audit or a recertification audit, a new certificate is issued containing the same expiry date as the former certificate for ISO/IEC 27001:2013.

A new full three year certification cycle shall only be granted after a recertification audit.

Summary
In order to continue a successful certification of an ISMS according to ISO 27001, it is necessary to adapt the system according to the updated standard. This requires work, time and money – but creates resilience against unauthorized influences.

We look forward to continuing our cooperation with you.

Contact

Dr. Karsten Grans

TÜV NORD CERT
Am TÜV 1
45307 Essen
Germany

P 0800 245-7457
F 0511 9986 69-1900

kgrans@tuev-nord.de
tuev-nord-cert.com

24-0554-03/23