Client Information
"ISO/IEC 27006-1:2024" – Transition

Important information about your existing ISO 27001 certification!

Dear ISO 27001 certification client,

As you have probably heard already, ISO 27006 was revised and published as International Standard ISO/IEC 27006-1:2024 in March 2024. This standard defines the rules for audits and certifications of management systems based on ISO 27001.

The "International Accreditation Forum" (IAF) defined in IAF document "IAF MD 29 - TRANSITION REQUIREMENTS FOR ISO/IEC 27006-1:2024" dated 21 May 2024 (IAF_MD_29_27006-1_Transition_21052024.pdf) a two-year transition period and some transitional arrangements. This means that after the end of the transition period on 31 March 2026, any certification in accordance with ISO 27001 must be based exclusively on the new edition of ISO 27006.

On 7 August 2024, the German Accreditation Body (DAkkS) published transition rules in the form of the notification "DAkkS enables transition to standard ISO/IEC 27006-1:2024" (DAkkS ermöglicht Umstellung auf Norm ISO/IEC 27006-1:2024 - DAkkS - Deutsche Akkreditierungsstelle). This essentially refers to the above-mentioned IAF document "IAF MD 29". Informing certified clients about the transition process and further details is one of the obligations of the conformity assessment bodies specified therein.

ⓘ Notes

The German version of ISO/IEC 27006-1:2024, DIN EN ISO/IEC 27006-1:2024, was published in August 2024 – the content of both versions is equivalent, and the statements made in this letter for ISO/IEC 27006-1:2024 also apply analogously to the German version.

Furthermore, the statements made in this letter for ISO/IEC 27001 also apply analogously to the German translation of ISO/IEC 27001, the standard DIN EN ISO/IEC 27001.

TÜV NORD CERT will submit an application to the DAkkS for extension and transition of accreditation to the new edition ISO/IEC 27006-1:2024 of the standard.
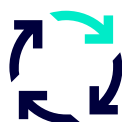
Continuation of ISO 27001 certification with the new edition of ISO 27006

The new standard version ISO/IEC 27006-1:2024 does not require any adaptation of your information security management system (ISMS) because ISO 27001 itself is not affected by the revisions in ISO/IEC 27006-1:2024.

Neither the validity nor the expiry date of existing certificates is affected by the revisions in ISO/IEC 27006-1:2024.

Here are some of the specifications made by the IAF and DAkkS for your information:

- Audits in accordance with the requirements of ISO/IEC 27006-1:2024 may only be carried out once the extension and transition of the accreditation has been completed.
- As soon as the extension and transition of the accreditation to ISO/IEC 27006-1:2024 by the DAkkS is available (accreditation transition), TÜV NORD CERT must carry out every audit for initial certification and recertification according to the new version ISO/IEC 27006-1:2024.
- Every audit that begins after 31 March 2026 must be carried out in accordance with the new version ISO/IEC 27006-1:2024.
- For the clients certified before the date of the accreditation transition, TÜV NORD CERT may use either ISO/IEC 27006:2015 or ISO/IEC 27006-1:2024 for surveillance audits after accreditation for ISO/IEC 27006-1:2024.
- As there are no additional or changed requirements for your ISMS, no additional audit time is required in the transition audits.

Certificates that are issued after the transition to the new standard version ISO/IEC 27006-1:2024 contain a reference to the certification rules then applied from ISO/IEC 27006-1:2024 for clear identification.

Key changes in the new edition of ISO 27006

Updating the audit time calculation requirements

New concepts impact how the audit time is calculated, particularly concerning determination of the initial number of persons (see C.2.1 and C.3.4 of ISO/IEC 27006-1:2024) and clarification of calculating audit time of multiple site organizations (see C.6 of ISO/IEC 27006-1:2024).

Refinement of the requirements for remote audits

A remote audit is defined by the fact that the auditor does not carry out the audit on site but is connected digitally. Previously, the remote part of ISMS audits was limited to 30 per cent of the total on-site audit time.

This limit has been lifted with the new version of the standard and it is now even possible for up to 100 per cent of the audit to be conducted remotely. The exact share is determined by a "risk analysis regarding the use of a remote audit for the client", whereby various factors (available infrastructure, sector, type of audit, scope, type of organization, etc.) are included in this risk analysis (see 9.1.3.3 of ISO/IEC 27006-1:2024).

The changes addressed here mean that the information to be obtained from the client during the quotation phase is somewhat more extensive than before.

Conclusion

In order to continue a successful certification of an ISMS according to ISO 27001, it is not necessary to adapt the system according to the updated standard ISO/IEC 27006-1:2024, even if some aspects of the certification processes change. Furthermore, no additional audit time is required in the transition audits.

We are looking forward to continuing our cooperation with you.

Contact
Dr. Karsten Grans
TIC Manager ISO 27001

TÜV NORD CERT
Am TÜV 1
45307 Essen

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

All locations.