Inspired by
Knowledge

Informace pro zákazníky

ISO/IEC 27001:2022 – Přechod

Důležité informace o vaší stávající certifikaci ISO 27001

Vážený zákazníku certifikace ISO 27001,

jak jste již pravděpodobně slyšeli, norma ISO/IEC 27001 byla revidována a v říjnu 2022 byla zveřejněna jako mezinárodní norma ISO/IEC 27001:2022.

„Mezinárodní akreditační fórum“ (IAF) definovalo v dokumentu IAF MD 26 ze dne 15. 02. 2023 tříleté přechodné období a některá přechodná opatření. To znamená, že po uplynutí přechodného období musí všechny certifikace podle ISO 27001 vycházet výhradně z revize normy a všechny certifikáty založené na starém vydání normy se stanou neplatnými, nezávisle na datu ukončení platnosti uvedeném na certifikátu.

Národní akreditační orgány, které jsou součástí IAF, zveřejnily pravidla pro přechod certifikace z původní verze ISO/IEC 27001:2013 na ISO/IEC 27001:2022. Jednou z povinností certifikačních orgánů je informovat certifikované zákazníky o opatřeních pro přechod na certifikaci podle ISO/IEC 27001:2022.

Poznámka

Certifikační orgány TÜV NORD CERT i TÜV NORD Czech podaly žádost o rozšíření a přechod akreditace na revizi normy.

Pokračování certifikace ISO 27001 s revizí normy

Vezměte, prosím, na vědomí následující obecné podmínky definované IAF: Všechny stávající certifikáty ISO/IEC 27001:2013 pozbývají platnosti k 31. 10. 2025, pokud nebyl přechod uskutečněn před tímto termínem. Každý počáteční certifikační audit a recertifikační audit začínající 1. 5. 2024 nebo později musí být proveden na základě normy ISO/IEC 27001:2022. Výchozím bodem je první den auditu na místě (fáze auditu 1).

Veškerá rozhodnutí o certifikaci za účelem převodu stávajících certifikací ISO/IEC 27001:2013 musí být dokončena nejpozději do 31. 10. 2025. V opačném případě se provede nová úplná počáteční certifikace.

Přechodové audity vyžadují dodatečný rozsah auditu na místě. Tento dodatečný rozsah je jednorázový a platí pouze pro přechodový audit.

Náklady na tento dodatečný rozsah auditu budeme certifikovaným zákazníkům účtovat.

Přechod může být proveden formou recertifikačního nebo kontrolního auditu, případně jako mimořádný audit.

Audity podle revize normy ISO/IEC 27001 mohou provádět pouze auditorské týmy, které byly v nových požadavcích vyškoleny a které byly pro audity podle nové normy formálně schváleny.

Činnosti organizací ucházejících se o přechod na certifikaci ISO/IEC 27001

Rozsah potřebných změn závisí u každé organizace na vyspělosti a efektivitě stávajícího systému řízení bezpečnosti informací (ISMS), organizačních struktur a procesů/postupů. Proto se pro určení dopadu na zdroje a termíny důrazně doporučuje provést posouzení dopadu/analýzu slabých míst.

Organizacím, které mají systém ISMS založený na normě ISO/IEC 27001:2013, se doporučuje přijmout následující opatření:

- identifikovat nedostatky ve společnosti, které je třeba odstranit, aby byly splněny nové požadavky;
- Připravit plán přechodu.
- zajistit odpovídající školení a budovat povědomí všech zúčastněných stran, které mají vliv na efektivitu organizace;
- aktualizovat stávající ISMS tak, aby splňoval revidované požadavky a poskytnout důkazy o účinnosti.

Mějte, prosím, na paměti, že při přechodovém auditu musí být prokázán úplný interní audit a hodnocení systému řízení podle revize normy ISO/IEC 27001:2022.

Pravidla pro výpočet dodatečného rozsahu auditu

V přechodných požadavcích IAF a národních akreditací obsahuje kapitola 4.2 dokumentu IAF MD 26:2022 úpravu dodatečného rozsahu auditu požadovaného při přechodných auditech. Rozhodli jsme se tento přístup přijmout a upravit jej s ohledem na typ auditu (audit na jednom místě nebo audit na více místech). Závěrem je následující výsledek pro dodatečný rozsah auditu (jako čas strávený na místě)

	AUDIT NA 1 MÍSTĚ	AUDIT NA VÍCE MÍSTECH
Přechod při recertifikačním auditu	0,5 člověkodne navíc	0,5 člověkodne navíc pro centrálu a 0,125 člověkodne navíc na jedno pracoviště při vzorkování
Přechod při pravidelném kontrolním auditu	1,0 člověkoden navíc	1,0 člověkoden navíc pro centrálu a 0,125 člověkodne navíc na jedno pracoviště při vzorkování
Přechod v rámci mimořádného (samostatného) auditu	1,0 člověkoden navíc	1,0 člověkoden navíc pro centrálu a 0,125 člověkodne navíc na jedno pracoviště při vzorkování

Poznámka

Pokud probíhá přechod v rámci mimořádného auditu, je třeba jeho rozsah vypočítat jako kontrolní audit se zde uvedeným navýšením rozsahu, což je rozhodně finančně nákladnější řešení.

Úvodní certifikační audit (fáze 1 a 2) pro ISO/IEC 27001:2022 nevyžaduje žádný dodatečný čas na přechod a může nahradit jakýkoli jiný přechodový audit.

Při výjimečných podmínkách může být tento přístup upraven.

V případě, kdy je zamýšlen transfer certifikace k jinému certifikačnímu orgánu, musí být plně dokončen transfer certifikace podle ISO/IEC 27001:2013, než bude možné pokračovat v plánování výše popsaného přechodového auditu.

Po mimořádném, kontrolním nebo recertifikačním přechodovém auditu je vydán nový certifikát se stejným datem platnosti, jaký měl předchozí certifikát podle ISO/IEC 27001:2013.

Nový tříletý certifikační cyklus je možno zahájit až po provedení recertifikačního auditu.

Shrnutí

Aby bylo možné pokračovat v úspěšné certifikaci ISMS podle ISO/IEC 27001, je nutné systém přizpůsobit aktualizované normě. To vyžaduje úsilí, čas a peníze, ale výsledkem je zvýšená odolnost vůči nežádoucím vlivům.

Těšíme se na další spolupráci s vámi.

Kontakt
Mgr. Viktor Šaroch, Ph.D.

TÜV NORD Czech, s.r.o.
Českomoravská 2420/15
190 00 Praha 9
Česká republika

T 602 664 895

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