Inspired by
Knowledge

Informácie pre zákazníkov

ISO/IEC 27001:2022 – Prechod

Dôležité informácie o vašej existujúcej certifikácii ISO 27001

Vážený zákazník s certifikáciou ISO 27001,

Ako ste už pravdepodobne počuli, norma ISO/IEC 27001 bola revidovaná a v októbri 2022 bola zverejnená ako medzinárodná norma ISO/IEC 27001:2022.

"Medzinárodné akreditačné fórum" (IAF) definovalo v dokumente IAF MD 26 z 15. 2. 2023 trojročné prechodové obdobie a niektoré prechodové opatrenia. To znamená, že po prechodovom období musia byť všetky certifikácie ISO 27001 založené výlučne na revízii normy a všetky certifikáty založené na starom vydaní normy sa stanú neplatnými bez ohľadu na dátum skončenia platnosti uvedeného na certifikáte.

Národné akreditačné orgány, ktoré sú súčasťou IAF, zverejnili pravidlá prechodu certifikácie z pôvodnej verzie ISO/IEC 27001:2013 na ISO/IEC 27001:2022. Jednou z povinností certifikačných orgánov je informovať certifikovaných zákazníkov o opatreniach prechodu na certifikáciu ISO/IEC 27001:2022.

Poznámka

Certifikačné orgány TÜV NORD CERT a TÜV NORD Czech predložili žiadosť o rozšírenie a prechod akreditácie na revíziu normy.

Pokračovanie certifikácie ISO 27001 s revíziou noriem

Upozorňujeme na nasledujúce všeobecné obchodné podmienky definované IAF: Platnosť všetkých existujúcich certifikátov ISO/IEC 27001:2013 vyprší 31.10.2025, ak sa prechod neuskutočnil pred týmto dátumom. Každý počiatočný certifikačný audit a recertifikačný audit začínajúci dňom 01.05.2024 alebo neskôr musí byť vykonaný v súlade s ISO/IEC 27001:2022. Východiskovým bodom je prvý deň auditu na mieste (fáza auditu 1).

Všetky rozhodnutia o certifikácii za účelom prevodu existujúcich certifikácií ISO / IEC 27001: 2013 musia byť dokončené najneskôr do 31.10.2025. V opačnom prípade sa vykoná nová úplná počiatočná certifikácia.

Prechodové audity si vyžadujú dodatočný rozsah auditov na mieste. Tento dodatočný rozsah je jednorazový a vzťahuje sa len na prechodový audit.

Náklady na tento dodatočný rozsah auditu budeme účtovať certifikovaným zákazníkom.

Prechod sa môže uskutočniť formou recertifikácie alebo kontrolného auditu alebo ako mimoriadny audit.

Audity podľa revízie ISO / IEC 27001 môžu vykonávať iba audítorské tímy, ktoré boli vyškolené na nové požiadavky a ktoré boli formálne schválené na audity podľa nového štandardu.

Činnosti organizácií žiadajúcich o prechod na certifikáciu ISO/IEC 27001

Rozsah zmien potrebných pre každú organizáciu závisí od vyspelosti a efektívnosti existujúceho systému manažérstva informačnej bezpečnosti (ISMS), organizačných štruktúr a procesov/postupov. Preto sa dôrazne odporúča vykonať posúdenie vplyvu/analýzu slabých miest s cieľom určiť dopad na zdroje a termíny.

Organizáciám, ktoré majú ISMS založenú na norme ISO / IEC 27001: 2013, sa odporúča, aby prijali nasledujúce opatrenia:

- identifikovať nedostatky v spoločnosti, ktoré je potrebné odstrániť, aby sa splnili nové požiadavky;
- pripraviť plán prechodu;
- zabezpečiť primeranú odbornú prípravu a budovať informovanosť medzi všetkými zainteresovanými stranami, ktoré majú vplyv na efektívnosť organizácie;
- aktualizovať existujúci ISMS tak, aby spĺňal revidované požiadavky a poskytoval dôkaz o účinnosti.

Upozorňujeme, že počas prechodového auditu musí byť preukázaný úplný interný audit a hodnotenie systému manažérstva podľa revízie normy ISO/IEC 27001:2022.

Pravidlá výpočtu dodatočného rozsahu auditu

V prechodových požiadavkách IAF a národných akreditáciách obsahuje kapitola 4.2 IAF MD 26:2022 úpravu dodatočného rozsahu auditu požadovaného pri prechodových auditoch. Rozhodli sme sa prijať tento postup a prispôsobiť ho typu auditu (audit na jednom mieste alebo audit na viacerých miestach). Záverom je nasledujúci výsledok pre dodatočný rozsah auditu (ako je čas strávený na mieste)

	AUDIT NA 1 MIESTE	AUDIT NA VIACERÝCH MIESTACH
Prechod počas recertifikačného auditu	0,5 človekodeň viac	0,5 človekodňa navyše v centrále a 0,125 človekodňa navyše na pracovisku pre vzorkovanie
Prechod počas pravidelného kontrolného auditu	1,0 človekodeň viac	1,0 človekodňa navyše v centrále a 0,125 človekodňa navyše na pracovisku pre vzorkovanie
Prechod v rámci mimoriadneho (samostatného) auditu	1,0 človekodeň viac	1,0 človekodňa navyše v centrále a 0,125 človekodňa navyše na pracovisku pre vzorkovanie

Poznámka

Ak sa prechod uskutoční ako súčasť mimoriadneho auditu, jeho rozsah sa musí vypočítať ako kontrolný audit s navýšeným rozsahom, ktorý je v tabuľke, čo je určite nákladnejšie riešenie.

Počiatočný certifikačný audit (fázy 1 a 2) pre ISO/IEC 27001:2022 nevyžaduje žiadny dodatočný prechodový čas a môže nahradiť akýkoľvek iný prechodový audit.

Za výnimočných okolností sa tento postup môže upraviť.

V prípade, že sa plánuje prevod certifikácie na iný certifikačný orgán, prechod certifikácie podľa ISO/IEC 27001:2013 musí byť úplne dokončený predtým, ako bude možné pokračovať v plánovaní auditu prechodu opísaného vyššie.

Po mimoriadnom, kontrolnom alebo recertifikačnom prechodovom audite sa vydá nový certifikát s rovnakým dátumom platnosti ako predchádzajúci certifikát ISO/IEC 27001:2013.

Nový trojročný certifikačný cyklus sa môže začať až po vykonaní recertifikačného auditu.

Súhrn

Aby bolo možné pokračovať v úspešnej certifikácii ISMS podľa ISO/IEC 27001, systém musí byť prispôsobený aktualizovanej norme. To si vyžaduje úsilie, čas a peniaze, ale vedie to k zvýšenej odolnosti voči nežiaducim vplyvom.

Tešíme sa na ďalšiu spoluprácu s vami.

Kontakt

Mgr. Viktor Šaroch, Ph.D.
T 00420 602 664 895
saroch@tuev-nord.cz

Mgr. Marcela Markovičová
T 00421 905 613 857
mmarkovicova@tuv-nord.com

TÜV NORD Slovakia, s.r.o.
Dúbravská cesta 2
SK – 841 04 Bratislava
www.tuvnord.sk