Klientske informácie – Prechod na „ISO/IEC 27006 Amd1:2020“

Dôležité informácie o vašej súčasnej certifikácií ISMS!

Vážený klient certifikácie ISMS,

ako ste už pravdepodobne boli informovaný, norma ISO 27006 bola v marci 2020 revidovaná novelou. Táto norma definuje pravidlá pre vykonávanie auditov a poskytovanie certifikácie ISMS na základe ISO 27001.

Medzinárodné fórum pre akreditáciu (IAF) vo svojom uznesení „ISO/IEC 27006:2015 AMD 1:2020 Prechodné dojednania“ uverejnené 27.07.2020 definovalo dvojročné prechodné obdobie a tiež niektoré opatrenia pre akreditačné a certifikačné orgány.

Dňa 14.08.2020 zverejnil náš akreditačný orgán DAkkS podrobnejšie pravidlá pre prechod, ktoré definujú termíny a činnosti pre strany zapojené do certifikácie ISMS.

Jednou z povinností je informovanie certifikovaných klientov o procese prechodu a ďalších podrobnostiach.

Poznámka: Bohužiaľ k vydaniu medzinárodnej, európskej a nemeckej (aj slovenskej – pozn. prekladateľa) verzie nedošlo v rovnakom roku - ale obsah ISO 27001:2013 je vo všetkých verziách ekvivalentný. Na zlepšenie čitateľnosti sa obvykle na identifikáciu normy používa všeobecný termín „ISO 27001“.

Nemecká verzia ISO 27006:2015 s názvom DIN EN ISO/IEC 27006:2021 bola zverejnená v máji 2021 a už obsahuje obsah zmeny 1 ako konsolidovanej normy.

Poznámka prekladateľa: STN EN ISO/IEC 27006 Informačné technológie. Bezpečnostné metódy. Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti- bola vydaná 1.7.2021.

Uvedomte si prosím, že nemôžeme distribuovať kópie žiadnej normy kvôli autorským právam.

TÜV NORD CERT požiadala o akreditáciu podľa nového vydania normy a táto bola udelená DAkkS v marci 2022.

Pokračovanie certifikácie ISMS v súlade s novo vydanou normou

Platnosť certifikácie:

Platnosť ani dátum ukončenia platnosti existujúcich certifikátov nie sú zmenou dotknuté.

Úprava vášho ISMS:

Úpravy v dôsledku tohto dodatku nevyžadujú žiadnu úpravu vášho ISMS, pretože samotná ISO 27001 nie je touto úpravou ovplyvnená.

Označenie štandardu:

V roku 2017 došlo k zmene označenia normy z dôvodu jej integrácie do systému európskych noriem – norma sa teraz volá „EN ISO/IEC 27001:2017“ avšak stále plne zodpovedá verzii normy ISO/IEC 27001: 2013 (vrátane oboch zverejnených opráv).

Akýkoľvek nový certifikát bude aj naďalej vydávaný s použitím tejto identifikácie „ISO/IEC 27001:2013“.

Pre jednoznačnú identifikáciu budú certifikáty vydané po prechode na novelu obsahovať odkaz na aplikované certifikačné pravidlá obsiahnuté v norme ISO/IEC 27006 Amd1:2020.

Certifikácia viacerých miest:

Novela upravuje metódu výpočtu na stanovenie doby auditu pre organizácie prevádzkujúce viac pracovísk. Všeobecne platí, že dokončíme aktuálne prebiehajúci certifikačný cyklus tak, ako už bolo dohodnuté, naplánované a pripravené, ale pre ďalší cyklus už použijeme novú metódu.

Odvetvové štandardy ako zdroj dodatočných kontrol, ako je uvedené v SoA:

Pokiaľ vaša SoA *(Statement of Applicability – v slovenčine Vyhlásenie o aplikovateľnosti – PoA – pozn. prekladateľa)* obsahuje odkazy na ďalšie opatrenia, ako sú definované v medzinárodných alebo národných normách, je možné na tieto normy v certifikáte ISO 27001 odkazovať. Tento odkaz v certifikátoch musí jasne uvádzať, že opatrenia podľa týchto noriem definované v SoA sú len doplnkové a že nejde o certifikáciu podľa týchto noriem.

V prípade, že ste vo vašom SoA použili medzinárodné alebo národné (odvetvovo špecifické) normy (pozri tiež ISO 27009) ako ďalší zdroj opatrenia, certifikáty odkazujúce na tieto normy/kontroly budú vydané znovu, aby boli splnené nové požiadavky, a všetky neplatné certifikačné dokumenty budú zrušené/stiahnuté.

V závislosti od použitej normy môžu platiť ďalšie špecifické požiadavky, ako napríklad pre dobu auditu alebo kompetencie audítorského tímu.

Vezmite prosím na vedomie: v súlade s aktuálne platnými pravidlami nevydávame žiadny samostatný certifikačný dokument zodpovedajúci takejto sektorovo špecifickej norme.

Pravidlá výpočtu pre ďalšie trvanie auditu

Vzhľadom na skutočnosť, že pre váš ISMS neexistujú žiadne upravené alebo dodatočné požiadavky, nie je potrebný dodatočný čas na prechodové audity. Budúci pravidelný audit alebo najneskôr ďalší recertifikačný audit však bude obvykle vykonaný ako prechodový audit.

Záver

Pre úspešné pokračovanie vášho ISMS, nie je nutné, kvôli vydaniu novej akreditačnej normy, aktualizovať váš ISMS, hoci sa niektoré aspekty certifikačných postupov menia. Prechodový audit si preto nevyžiada z Vašej strany žiadne zvláštne opatrenia.
Tešíme sa na úspešné pokračovanie našej spolupráce.

Zodpovedný za obsah:
Dr. Karsten Grans
TIC Manager ISO 27001
kgrans@tuev-nord.de

Za SK preklad:
Viktor Šaroch/Marcela Markovičová

01/04/2022