Klientské informace – Přechod na „ISO/IEC 27006 Amd1:2020“

Důležité informace o vašich stávajících certifikacích ISMS!

Vážený kliente certifikace ISMS,

Jak jste již pravděpodobně slyšeli, norma ISO 27006 byla v březnu 2020 revidována novelou. Tato norma definuje pravidla pro provádění auditů a poskytování certifikace ISMS na základě ISO 27001.

Mezinárodní fórum pro akreditaci (IAF) ve svém usnesení „ISO/IEC 27006:2015 AMD 1:2020 Přechodná ujednání“ zveřejněné dne 27.07.2020 definovalo dvouleté přechodné období a také některá opatření pro akreditační a certifikační orgány.

Dne 14.08.2020 zveřejnil náš akreditační orgán DAkkS podrobnější pravidla pro přechod, které definují termíny a činnosti pro strany zapojené do certifikace ISMS.

Jednou z povinností v něm definovaných je informování certifikovaných klientů o procesu přechodu a dalších podrobnostech.

Poznámka: Bohužel k vydání mezinárodní, evropské a německé (i české – pozn. překladatele) verze nedošlo ve stejném roce - ale obsah ISO 27001:2013 je ve všech verzích ekvivalentní. Pro zlepšení čitelnosti se obvykle k identifikaci normy používá obecný termín „ISO 27001“.

Německá verze ISO 27006:2015 s názvem DIN EN ISO/IEC 27006:2021 byla zveřejněna v květnu 2021 a již obsahuje obsah změny 1 jako konsolidované normy.

Poznámka překladatele: ČSN EN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací – byla vydána 1.5.2021.

Uvědomte si prosím, že nemůžeme distribuovat kopie žádné normy kvůli autorským právům.

TÜV NORD CERT požádal o akreditaci podle nového vydání normy a tato byla udělena DAkkS v březnu 2022.

Pokračování certifikace ISMS v souladu s nově vydanou normou

Platnost certifikace:

Platnost ani datum ukončení platnosti stávajících certifikátů nejsou změnou dotčeny.

Úprava vašeho ISMS:

Úpravy v důsledku tohoto dodatku nevyžadují žádnou úpravu vašeho ISMS, protože samotná ISO 27001 není touto úpravou ovlivněna.

Označení standardu:

V roce 2017 došlo ke změně označení normy z důvodu její integrace do systému evropských norem – norma se nyní jmenuje „EN ISO/IEC 27001:2017“ avšak stále plně odpovídá verzi normy ISO/IEC 27001: 2013 (včetně obou zveřejněných oprav).

Jakýkoli nový certifikát bude i nadále vydáván s použitím této identifikace „ISO/IEC 27001:2013“.

Pro jednoznačnou identifikaci budou certifikáty vydané po přechodu na novelu obsahovat odkaz na aplikovaná certifikační pravidla obsažená v normě ISO/IEC 27006 Amd1:2020.

Certifikace více míst:

Novela upravuje metodu výpočtu pro stanovení doby auditu pro organizace provozující více pracovišť. Obecně platí, že dokončíme aktuálně probíhající certifikační cyklus tak, jak již bylo dohodnuto, naplánováno a připraveno, ale pro další cyklus již použijeme novou metodu.

Odvětvové standardy jako zdroj dodatečných kontrol, jak je uvedeno v SoA:

Pokud vaše SoA (Statement of Applicability – *v češtině Prohlášení o aplikovatelnosti – PoA – pozn. překladatele*) obsahuje odkazy na další opatření, jak jsou definována v mezinárodních nebo národních normách, je možné na tyto normy v certifikátu ISO 27001 odkazovat. Tento odkaz v certifikátech musí jasně uvádět, že opatření podle těchto norem definovaná v SoA jsou pouze doplňkovými a že se nejedná o certifikaci podle těchto norem.

V případě, že jste ve vašem SoA použili mezinárodní nebo národní (odvětvově specifické) normy (viz také ISO 27009) jako další zdroj opatření, certifikáty odkazující na tyto normy/kontroly budou vydány znovu, aby byly splněny nové požadavky, a všechny neplatné certifikační dokumenty budou zrušeny/staženy.

V závislosti na použité normě mohou platit další specifické požadavky, jako například pro dobu auditu nebo kompetence auditorského týmu.

Vezměte prosím na vědomí: v souladu s aktuálně platnými pravidly nevydáváme žádný samostatný certifikační dokument odpovídající takovéto sektorově specifické normě.

Pravidla výpočtu pro další trvání auditu

Vzhledem k tomu, že pro váš ISMS neexistují žádné upravené nebo dodatečné požadavky, není nutný dodatečný čas na přechodové audity. Příští pravidelný audit nebo nejpozději další recertifikační audit však bude obvykle proveden jako přechodový audit.

Závěr

Chcete-li pokračovat v úspěšném udržování vašeho ISMS, není nutné kvůli vydání nové akreditační normy aktualizovat váš ISMS, přestože se některé aspekty certifikačních postupů mění. Přechodový audit si proto nevyžádá z Vaší strany žádná zvláštní opatření. Rádi budeme tedy pokračovat v naší úspěšné spolupráci.

Zodpovědný za obsah:
Dr. Karsten Grans
TIC Manager ISO 27001
kgrans@tuev-nord.de
01/04/2022