SNAS SLOVENSKÁ NÁRODNÁ AKREDITAČNÁ SLUŽBA

Politika

PL - 62

POLITIKA A POSTUP SNAS PRI POSUDZOVANÍ CERTIFIKAČNÝCH ORGÁNOV CERTIFIKUJÚCICH ISMS PODĽA POŽIADAVIEK NORMY ISO/IEC 17021-1: 2015 a ISO/IEC 27006-1: 2024 V SÚLADE S IAF MD 29: 2024

Schválil: **Ing. Štefan Král, PhD.**
Riaditeľ SNAS

Účinnosť od: 15.09.2024	Vydanie: 1 Aktualizácia: 0	Označenie RD: PL - 62

- **Tento dokument bol vytvorený elektronicky -**

ÚČEL: Tento dokument určuje politiku a postup SNAS pri posudzovaní požiadaviek prechodu certifikačných orgánov certifikujúcich systémy manažérstva informačnej bezpečnosti podľa požiadaviek normy ISO/IEC 17021-1: 2015 a ISO/IEC 27006-1: 2024, v súlade s dokumentom IAF MD 29: 2024. Issue 1, Transition requirements for ISO/IEC 27006-1: 2024.

Spracoval: **Ing. Jana Mária Obernauer, MSc.**
Dátum spracovania: 01.09.2024

Preskúmal: **Ing. Jaroslav Remža, PhD.**

Obsah

1 POLITIKA

SNAS posudzuje kompetentnosť certifikačných orgánov certifikujúcich systémy manažérstva informačnej bezpečnosti (ISMS) podľa požiadaviek noriem ISO/IEC 17021-1: 2015 a ISO/IEC 27006: 2015/Dodatok 1: 2020.

Dňa 01.03.2024 bola publikovaná norma ISO/IEC 27006-1: 2024 – Požiadavky na orgány zabezpečujúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti – Časť 1: Všeobecne. Toto vydanie normy ISO/IEC 27006-1: 2024 nahrádza akreditačnú normu ISO/IEC 27006: 2015/Dodatok 1: 2020.

SNAS v súlade s rezolúciou IAF MD 29: 2024, schválenou členmi IAF zo dňa 21.05.2024 stanovil prechodné obdobie dva roky na implementáciu normy ISO/IEC 27006-1: 2024, ktoré končí 31.03.2026.

V rámci tohto času, splnením podmienok uvedených nižšie, musia všetky akreditované CAB plniace požiadavky normy ISO/IEC 17021-1: 2015 a ISO/IEC 27006: 2015 / Dodatok 1: 2020 preukázať spôsobilosť vykonávať certifikáciu ISMS podľa požiadaviek normy ISO/IEC 27006-1: 2024, čo SNAS preverí a v prípade ich plnenia, rozhodne o ponechaní akreditácie na výkon certifikácie ISMS v platnosti podľa požiadaviek normy ISO/IEC 27001: 2022**.**

2 POSTUP PRI POSUDZOVANÍ A TERMÍNY

Pri podaní novej žiadosti o akreditáciu alebo žiadosti o reakreditáciu bude SNAS **od 31.03.2025** posudzovať plnenie požiadaviek normy ISO/IEC 17021-1: 2015 a ISO/IEC 27006-1: 2024**.**

CAB akreditované na výkon certifikácie ISMS plniace požiadavky normy ISO/IEC 17021-1: 2015 a ISO/IEC 27001 musia **najneskôr do 31.03.202**5 písomne oznámiť na SNAS, či realizovali vo svojom systéme manažérstva požiadavky ISO/IEC 27006-1: 2024 alebo oznámiť, do akého termínu tieto požiadavky realizujú, avšak tento termín **nesmie prekročiť 30.06.2025**. SNAS preverí plnenie požiadaviek požiadavky ISO/IEC 27006-1: 2024 počas plánovaných posudzovaní, mimoriadnych posudzovaní alebo preskúmaním dokumentácie. Všetky posudzovania s cieľom preverenia plnenia požiadaviek požiadavky ISO/IEC 27006-1: 2024 budú vykonané **najneskôr do 30.11.2025**.

CAB akreditované na výkon certifikácie ISMS musia preukázať pripravenosť na výkon certifikácie podľa ISO/IEC 17021-1: 2015 a požiadavky ISO/IEC 27006-1: 2024 **k 31.01.2026** a SNAS **najneskôr do 31.03. 2026** rozhodne o udelení akreditácie na výkon certifikácie ISMS podľa normy ISO/IEC 17021-1: 2015 a požiadavky ISO/IEC 27006-1: 2024.

Zistenia z posudzovaní budú klasifikované v súlade so systémom zverejneným SNAS a musia byť odstránené v lehote, ktorý je uvedený v zákone č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, a to najneskôr do dvoch mesiacov od ich zistenia a zaznamenania.

3 ZHRNUTIE KĽÚČOVÝCH ZMIEN

3.1 HLAVNÉ ZMENY

Hlavné zmeny medzi normami ISO/IEC 27006: 2015 a ISO/IEC 27006-1: 2024 zahŕňajú, ale nie sú obmedzené na:

i) Spresnenie požiadaviek na audity na diaľku.

a) Nové požiadavky na nasadenie vzdialeného auditu v článku 9.1.3.3.

b) Rozsah a účinnosť uplatňovania auditu na diaľku sa uvedie v audítorskej správe v článku 9.4.3.2.

c) Odstránenie požiadaviek na získanie súhlasu od Akreditačného orgánu (AB), ak audity na diaľku predstavujú viac ako 30 % plánovaného času auditu na mieste.

d) Pre klienta, ktorý má málo alebo žiadne fyzické relevantné miesta, správa o audite (článok 9.4.3.2) a certifikačný dokument (článok 8.2.2) musia uvádzať, že aktivity klienta sa vykonávajú na diaľku.

ii) Aktualizácia požiadavky na výpočet času auditu (pozri **prílohu C** normy ISO/IEC 27006-1: 2024). .

a) Zavedenie pojmu osoby vykonávajúce určité identické činnosti v **C.2.1** a definovanie požiadavky na to, ako primerane určiť počiatočný počet osôb v **C.3.4.**

b) Nové požiadavky na čas auditu pre rozšírenie rozsahu v **C.7.**

c) Ďalšie objasnenie prístupov k výpočtu času auditu viacerých pracovísk v **C.6.**

iii) Aktualizácia prílohy D k norme ISO/IEC 27006:2015, aby sa zosúladila s kontrolami bezpečnosti informácií uvedenými v prílohe A k norme ISO/IEC 27001: 2022 a jej prenos ako príloha E k norme ISO/IEC 27006-1: 2024. Tabuľka D bola preznačená ako tabuľka E.

iv) Spresnenie požiadaviek na odkazovanie na iné normy v certifikačných dokumentoch ISMS (článok 8.2.3).

v) Odstránenie nadbytočnosti s ISO/IEC 17021-1:2015. Napríklad boli aktualizované články 5.2, 7.1.3, 9.3.2.2 a 9.4 (ISO/IEC 27006-1: 2024).

vi) Vypustenie kvantitatívnej požiadavky na pracovné skúsenosti a školenia audítorov ISMS, napríklad 4-ročná prax na pracovisku na plný úväzok.

3.2 KĽÚČOVÝ ČASOVÝ ROZVRH

ISO/IEC 27006-1: 2024 bola zverejnená v marci 2024. Podľa rozhodnutia IAF sa dátumy uvedené nižšie počítajú od 31. marca 2024.

Činnosť	Termín plnenia
Akreditačný orgán (AB)	
AB bude pripravený na posúdenie podľa ISO/IEC 27006-1:2024 najneskôr do	9 mesiacov od konca mesiaca zverejnenia – 31. decembra 2024.
AB použije ISO/IEC 27006-1:2024 pre všetky počiatočné (alebo rozšírenie existujúcich) akreditačných hodnotení najneskôr do	12 mesiacov od konca mesiaca zverejnenia – 31.marca 2025.
Prechod AB všetkých CAB bude ukončený najneskôr do	24 mesiacov od konca mesiaca zverejnenia – 31.marca 2026.
CAB	
CAB používa ISO/IEC 27006-1: 2024 pre všetky počiatočné a recertifikačné audity po akreditácii podľa ISO/IEC 27006-1: 2024.	Dátum sa určí pre každý CAB na základe dátumu prechodu jeho akreditácie.
CAB používa ISO/IEC 27006-1: 2024 pre všetkých klientov najneskôr do	24 mesiacov od konca mesiaca zverejnenia – 31.marca 2026.

Poznámka: Pre klientov certifikovaných pred dátumom prechodu akreditácie môže orgán posudzovania zhody použiť buď ISO/IEC 27006:2015 alebo ISO/IEC 27006-1:2024 na dozorné audity po akreditácii na ISO/IEC 27006-1:2024

4 OPATRENIA PROCESU PRECHODU

4.1 OPATRENIA AKREDITAČNÉHO ORGÁNU (AB)

Činnosť	Áno/Nie	Poznámky/záznamy:
Opatrenia AB	ÁNO	- AB plánuje svoju pripravenosť na posúdenie novej verzie normy pri najbližšej príležitosti a najneskôr podľa stanoveného termínu. - AB identifikuje zmeny medzi novou a starou verziou. - AB zabezpečí včasné informovanie orgánov posudzovania zhody o požadovaných prechodných opatreniach vrátane akýchkoľvek predbežných termínoch v rámci prechodného obdobia. - AB zabezpečí, aby príslušní pracovníci ovplyvnení zmenami boli kompetentní pre revidovanú verziu a proces prechodu. - AB sa odporúča, aby naplánovali a začali požadované činnosti pri najbližšej príležitosti.
Posúdenie dokumentácie CAB	NIE	
Posúdenie technickej dokumentácie CAB	ÁNO	Preskúmanie GAP analýzy CAB, plánu prechodu /implementácie, príslušnej dokumentácie k zmenám vrátane potrebných dôkazov o implementácii a iných relevantných informácií, ktoré AB považuje za potrebné.
Je pravdepodobné, že na prechod bude potrebný čas navyše?	ÁNO	Minimálne jeden deň posudzovania na potvrdenie prechodu CAB.
Technické posúdenie v sídle CAB (posudzovanie na mieste alebo na diaľku)	ÁNO	Ak je AB schopný preskúmať požadované zmeny a implementáciu CAB ako výsledok preskúmania technickej dokumentácie CAB, potom sa hodnotenie sídla CAB nevyžaduje. Ak AB nie je schopný, potom je potrebné posúdenie na mieste v sídle CAB.
Svedecké posúdenie CAB	NIE	

Činnosť	Áno/Nie	Poznámky/záznamy:
Rozhodnutie o prechode AB	ÁNO	AB prijme rozhodnutie o prechode na ISO/IEC 27006-1: 2024, keď budú všetky identifikované nevyriešené problémy náležite vyriešené a bude preukázaná spôsobilosť.

4.2 ČINNOSTI ORGÁNU POSUDZOVANIA ZHODY (CAB)

Činnosť	Áno/Nie	Poznámky/záznamy:
Opatrenia CAB	ÁNO	- CAB naplánuje svoju pripravenosť na predloženie prechodných opatrení AB (v súlade so špecifikovanými prechodnými požiadavkami AB) a svoju pripravenosť aplikovať nové požiadavky podľa stanovených termínov plnenia. - CAB vykoná kompletnú GAP analýzu. - CAB vypracuje plán prechodu na riešenie nasledujúcich problémov: i) CAB Identifikujte zmeny medzi novou a starou verziou. Typické procesy zvažované pre zmeny môžu zahŕňať predaj/ponuku, proces auditu, certifikačný dokument, riadenie kompetencií a komunikáciu s existujúcimi certifikovanými klientmi. ii) CAB analyzuje vplyv zmien na relevantné činnosti /procesy a identifikujte požadované opatrenia na zabezpečenie súladu (napríklad systém/dokumenty riadenia a prípadne nástroje IT). - CAB monitoruje dôkazy o požadovaných zmenách a overujte priebežnú implementáciu zmien. - CAB zabezpečí, aby jeho príslušní pracovníci ovplyvnení zmenami boli kompetentní pre revidovanú verziu a proces prechodu. Personál môže okrem iného zahŕňať audítora, kontrolórov správy o audite, osoby s rozhodovacou právomocou v oblasti certifikácie, kontrolóra aplikácií, plánovača. - CAB sa odporúča, aby plánovali a začali s požadovanými činnosťami pri najbližšej príležitosti.

Činnosť	Áno/Nie	Poznámky/záznamy:
Iné	ÁNO	Keďže požiadavky na určenie času auditu sa vo vydaní ISO/IEC 27006-1 z roku 2024 zmenili, je možné, že bude potrebné zrevidovať zmluvu medzi CAB a ich existujúcimi certifikovanými klientmi.

5 SÚVISIACE PREDPISY

ISO/IEC 17021-1: 2015 Posudzovanie zhody. Požiadavky na orgány certifikujúce systémy manažérstva. Časť 1: Požiadavky

ISO/IEC 17021-1: 2015, Posudzovanie zhody – Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva – Časť 1: Požiadavky

ISO/IEC 27001: 2013, Informačné technológie – Bezpečnostné metódy – Systémy manažérstva informačnej bezpečnosti – Požiadavky

ISO/IEC 27006: 2015 Informačné technológie. Bezpečnostné techniky. Požiadavky na orgány zabezpečujúce audit a certifikáciu systémov riadenia bezpečnosti informácií

ISO/IEC 27006: 2015/Dodatok 1:2020, Informačné technológie – Bezpečnostné metódy – Systémy manažérstva informačnej bezpečnosti – Požiadavky na orgány poskytujúce audit a certifikáciu systémov riadenia informačnej bezpečnosti.

ISO/IEC 27001: 2022 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky.

ISO/IEC 27006-1: 2024 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia - Požiadavky na orgány zabezpečujúce audit a certifikáciu systémov riadenia bezpečnosti informácií. Časť 1: Všeobecne

IAF MD 29: 2024 Požiadavky na prechod na ISO/IEC 27001: 2022

Zákon č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody