SNAS SLOVENSKÁ NÁRODNÁ AKREDITAČNÁ SLUŽBA

Politika

PL - 57

POLITIKA A POSTUP SNAS PRI POSUDZOVANÍ CERTIFIKAČNÝCH ORGÁNOV CERTIFIKUJÚCICH SYSTÉMY MANAŽÉRSTVA INFORMAČNEJ BEZPEČNOSTI (ISMS) PODĽA POŽIADAVIEK NORMY ISO/IEC 27001: 2022 V SÚLADE S IAF MD 26: 2023

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

Účinnosť od: 07.07.2023	Vydanie: 1 Aktualizácia: 2	Označenie RD: PL - 57

- **Tento dokument bol vytvorený elektronicky -**

ÚČEL: Tento dokument určuje politiku a postup SNAS pri posudzovaní certifikačných orgánov certifikujúcich systémy manažérstva informačnej bezpečnosti podľa požiadaviek normy ISO/IEC 27001: 2022 v súlade s dokumentom IAF MD 26: 2023, vydanie 2.

Spracoval: **Ing. Alena Trabalková**
Ing. Marcela Kráľová
Dátum spracovania: 22.06.2023

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

Nadobudnutím účinnosti tejto PL -57 končí účinnosť PL - 57 zo dňa 17.03.2023.

Obsah

1 ÚVOD ..... Chyba! Záložka nie je definovaná.

2 SÚVISIACE DOKUMENTY ..... Chyba! Záložka nie je definovaná.

3 NÁZOV KAPITOLY ..... Chyba! Záložka nie je definovaná.

3.1 NÁZOV PODKAPITOLY : ..... Chyba! Záložka nie je definovaná.

3.1.1 Názov kapitoly RD 3 úrovne: ..... **Chyba! Záložka nie je definovaná.**

4 Prílohy ..... **Chyba! Záložka nie je definovaná.**

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 s Dodatkom 1: 2020.

V októbri 2022 bola publikovaná nová verzia normy ISO/IEC 27001: 2022, ktorá nahrádza normu ISO/IEC 27001: 2013.

SNAS, v súlade s požiadavkami prechodu na novú verziu normy ISO/IEC 27001: 2022, zverejnenými 15.02.2023 v dokumente IAF MD 26: 2023, vydanie 2, stanovil prechodové obdobie 36 mesiacov na implementáciu normy ISO/IEC 27001: 2022, **ktoré končí 31.10.2025**.

V rámci tohto času, splnením podmienok uvedených nižšie, musia všetky akreditované CAB plniace požiadavky ISO/IEC 17021-1: 2015 a ISO/IEC 27006: 2015 s Dodatkom 1: 2020 preukázať spôsobilosť vykonávať certifikáciu ISMS v súlade s novou verziou normy ISO/IEC 27001: 2022, čo SNAS preverí počas plánovaných alebo mimoriadnych posudzovaní. V prípade ich plnenia, rozhodne o udelení alebo ponechaní akreditácie na výkon certifikácie ISMS 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 30.04. 2023** posudzovať plnenie požiadaviek ISO/IEC 17021-1: 2015 a ISO/IEC 27006: 2015 s Dodatkom 1: 2020 na výkon certifikácie podľa normy ISO/IEC 27001: 2022. CAB akreditované na výkon certifikácie ISMS môžu požiadať o posúdenie pripravenosti na certifikáciu podľa ISO/IEC 27001: 2022 **od 01.01.2023.**

CAB akreditované na výkon certifikácie ISMS podľa normy ISO/IEC 27001: 2013 musia **najneskôr do 31.03.2023** písomne oznámiť na SNAS, či zapracovali vo svojom systéme manažérstva požiadavky na výkon certifikácie podľa ISO/IEC 27001: 2022 alebo oznámiť, do akého termínu tieto požiadavky zapracujú, avšak tento termín **nesmie prekročiť 30.04.2023**.

SNAS preverí pripravenosť na certifikáciu normy ISO/IEC 27001: 2022 počas plánovaných posudzovaní alebo mimoriadnych posudzovaní. Všetky posudzovania s cieľom preverenia plnenia požiadaviek ISO/IEC 27001: 2022 musia byť vykonané najneskôr **do 30.06.2023.**

CAB akreditované na výkon certifikácie ISMS musia preukázať pripravenosť na výkon

certifikácie podľa ISO/IEC 27001: 2022 **k 31.08.2023** a SNAS **najneskôr do 31.10.2023** rozhodne o udelení akreditácie na výkon certifikácie ISMS podľa normy ISO/IEC 27001: 2022.

Zistenia z posudzovaní budú klasifikované v súlade so systémom zverejneným SNAS a musia byť odstránené v lehote, ktorý je uvedený v zákone č. 505/2009 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.

Poznámka 1: Osvedčenia o akreditácii vydané počas prechodového obdobia (3 roky) budú obsahovať obidve normy, t. j. ISO/IEC 27001: 2013 aj ISO/IEC 27001: 2022. Osvedčenia o akreditácii vydané na certifikáciu ISMS podľa ISO/IEC 27001: 2013 budú po 31.10.2025 zrušené.

Poznámka 2: Certifikačné orgány môžu vykonávať certifikačné a recertifikačné audity v súlade s normou ISO/IEC 27001: 2013 len do 30.04.2024.

3 ZHRNUTIE KĽÚČOVÝCH ZMIEN

3.1 HLAVNÉ ZMENY

V porovnaní s ISO/IEC 27001: 2013, hlavné zmeny v ISO/IEC 27001: 2022 zahŕňajú najmä:

1) Príloha A odkazuje na opatrenia v ISO/IEC 27002: 2022, ktoré obsahujú informácie o názve opatrenia a opatrenie;
2) poznámky k odseku 6.1.3 c) sú revidované redakčne, vrátane odstránenia cieľov opatrení a ako náhrada za „opatrenie“ sa použije „opatrenie informačnej bezpečnosti“;
3) znenie odseku 6.1.3 d) je upravené tak, aby sa odstránila potenciálna nejednoznačnosť;
4) pridanie nového odseku 4.2 c) na stanovenie požiadaviek zainteresovaných strán, ktoré sa riešia prostredníctvom systému manažérstva informačnej bezpečnosti (ISMS);
5) pridanie nového článku 6.3 – Plánovanie zmien, ktorá definuje, že zmeny v ISMS musí organizácia vykonať plánovaným spôsobom;
6) zachovanie konzistentnosti slovesa používaného v súvislosti so zdokumentovanými informáciami, napríklad, použitie „Dokumentované informácie musia byť k dispozícii ako dôkaz XXX“ v článkoch 9.1, 9.2.2, 9.3.3 a 10.2;

7) použitie slovného spojenia „externe zabezpečované procesy, výrobky alebo služby“ je nahradené slovným spojením „outsourcované procesy“ v článku 8.1 a vypustenie výrazu „outsource“;
8) pomenovanie a zmena poradia v článkoch 9.2 – Interné audity a 9.3 – Preskúmanie manažmentom;
9) zmena poradia dvoch článkov v kapitole 10 – Zlepšovanie
10) aktualizáciu vydania súvisiacich dokumentov uvedených v Literatúre, ako sú ISO/IEC 27002 a ISO 31000;
11) niektoré odchýlky v ISO/IEC 27001: 2013 od high-level štruktúry, identický základný text, spoločné pojmy a základné definície MSS (noriem pre systémy manažérstva), sa revidujú v súlade s harmonizovanou štruktúrou MSS, napríklad odsek 6.2 d).

Poznámka 1: Prvé dve položky pochádzajú z ISO/IEC 27001: 2013/DAmd, tretia položka je z ISO/IEC 27001: 2013/COR 2: 2015 a ostatné zmeny vyplývajú z harmonizovanej štruktúry pre MSS.

Poznámka 2: V porovnaní so starým vydaním sa počet opatrení v norme ISO/IEC 27002: 2022 znížil zo 114 opatrení v 14 sekciách na 93 opatrení v 4 sekciách. Pre opatrenia v norme ISO/IEC 27002: 2022 je 11 opatrení nových, 24 opatrení zlúčených s už existujúcimi opatreniami a 58 opatrení aktualizovaných. Reviduje sa štruktúra opatrení, ktorá zavádza "atribút" a "účel" pre každé opatrenie a už nepoužíva "ciel'" pre skupinu opatrení.

Poznámka 3: Norma ISO/IEC 27001: 2013/COR 1: 2014 súvisí s prílohou A a prekrýva sa s normou ISO/IEC 27001: 2013/DAMD 1.

3.2 VPLYV

Vplyv zmien v norme ISO/IEC 27001: 2022 zahŕňa najmä zavedenie novej prílohy A a článku 6.3, pretože:

1) ISO/IEC 27001: 2013/COR 2: 2015 už bola uverejnená a implementovaná;
2) Príloha A je normatívna.,
3) Harmonizovaná štruktúra pre MSS je považovaná za menšiu revíziu pre high-level štruktúru, identický základný text, spoločné pojmy a základné definície MSS, v ktorej sa väčšina zmien považuje za redakčné.

Požiadavky v ISO/IEC 27001: 2022, ktoré používajú referenčný súbor opatrení v prílohe A, sú porovnávacím procesom medzi opatreniami informačnej bezpečnosti určenými organizáciou, opatreniami v prílohe A (6.1.3 c)) a vypracovaným vyhlásením o aplikovateľnosti (6.1.3 d)). Porovnaním potrebných opatrení informačnej bezpečnosti s

opatreniami v prílohe A môže organizácia potvrdiť, že sa neúmyselne nevynechalo žiadne potrebné opatrenie informačnej bezpečnosti z referenčného súboru v prílohe A.

Takéto porovnanie nemusí viesť k zisteniu akéhokoľvek potrebného opatrenia informačnej bezpečnosti, ktorý bol neúmyselne vynechaný. Avšak, aj keď sa zistia neúmyselne vynechané potrebné opatrenia informačnej bezpečnosti, organizácia aktualizuje svoje plány riešenia rizík tak, aby vyhovovali dodatočným potrebným opatreniam informačnej bezpečnosti a implementuje ich.

Ako už bolo naznačené vyššie, vplyv normy ISO/IEC 27001: 2022 na organizácie, ktoré implementovali ISMS, nemusí byť významný.

4 ČASOVÝ HARMONOGRAM

Činnosť	Termín plnenia
AB	
AB bude pripravený na posudzovanie podľa ISO/IEC 27001: 2022 najneskôr do	6 mesiacov od posledného dňa v mesiaci od zverejnenia dokumentu ISO/IEC 27001: 2022 (t. j. 30 apríla 2023)
AB začne vykonávať počiatočné posúdenie podľa normy ISO/IEC 27001: 2022 najneskôr do	6 mesiacov od posledného dňa v mesiaci od zverejnenia dokumentu ISO/IEC 27001: 2022 (t. j. 30 apríla 2023).
AB dokončí prechody všetkých CAB do	12 mesiacov od posledného dňa v mesiaci od zverejnenia dokumentu ISO/IEC 27001: 2022 (t. j. 31 októbra 2023)
CAB	
CAB začne počiatočnú certifikáciu a recertifikáciu podľa normy ISO/IEC 27001: 2022, najneskôr do	18 mesiacov od posledného dňa v mesiaci od zverejnenia dokumentu ISO/IEC 27001: 2022 (t. j. 30 . apríla 2024).
CAB dokončí prechody certifikovaných klientov, do	36 mesiacov od posledného dňa v mesiaci od zverejnenia dokumentu ISO/IEC 27001: 2022 (t. j. 31. októbra 2025).

5 ČINNOSTI PROCESU PRECHODU

5.1 ČINNOSTI AKREDITAČNÉHO ORGÁNU (AB)

Činnosť	Áno/Nie	Poznámky/záznamy:
Opatrenia AB	ÁNO	1) AB musí ustanoviť svoje prechodové činnosti pre normu ISO/IEC 27001: 2022 s ohľadom na požiadavky tohto dokumentu. 2) V prechodových činnostiach sa musí určiť, čo musí urobiť AB a čo musí urobiť CAB. AB môže mať niekoľko samostatných dokumentov na riešenie prechodových činnosti. 3) Prechodové činnosti musia zahŕňať prinajmenšom zváženie nasledujúceho: • zmeny v norme ISO/IEC 27001: 2022 a GAP rozdielovú analýzu; • príslušní pracovníci sú spôsobilí pre normu ISO/IEC 27001: 2022 a proces prechodu; Poznámka: Posudzovacia skupina, ako celok, musí mať znalosti z technológií a z postupov v oblasti informačnej bezpečnosti (pozri IAF MD 13: 2020, 4.2). Ako je známe, ISO/IEC 27002 poskytuje referenčný súbor všeobecných opatrení informačnej bezpečnosti vrátane návodu na implementáciu. • sú identifikované súvisiace procesy a dokumenty AB ovplyvnené zmenou ISO/IEC 27001, ako aj IT systémy pre riadenie akreditačných činností, v prípade potreby; • program posudzovania prechodu; • CAB boli včas informované o programe posudzovania prechodu, ako napríklad o časovom harmonograme a prístupe k posudzovaniu prechodu, a o dôsledkoch neukončenia prechodu v stanovenej lehote.

Činnosť	Áno/Nie	Poznámky/záznamy:
		4) AB sa odporúča, aby pri najbližšej príležitosti naplánovali a začali prijímať požadované opatrenia.
Posúdenie dokumentácie CAB	NIE	
Posúdenie technickej dokumentácie CAB	ÁNO	1) AB vykoná preskúmanie technickej dokumentácie s cieľom potvrdiť, či orgány posudzovania zhody sú alebo nie sú kompetentné na ISO/IEC 27001: 2022. 2) AB musí rozhodnúť o vhodnosti prechodových činnosti CAB a v prípade potreby aj o účinnosti ich vykonávania prostredníctvom preskúmania týchto informácií, ktoré predložili CAB: • GAP rozdielovú analýzu zmien v ISO/IEC 27001: 2022; • prechodové činnosti a dôkazy o ich implementácii; • oprávnenia príslušných pracovníkov; • ostatné relevantné informácie, ktoré AB považuje za potrebné.
Technické posúdenie v sídle CAB (posudzovanie na mieste alebo na diaľku)	V prípade potreby	Ak je AB schopný získať dostatočné dôkazy prostredníctvom preskúmania technickej dokumentácie CAB, potom sa posúdenie v sídle CAB nevyžaduje. Ak AB nie je schopný overiť účinné vykonávanie a súlad s prechodovými činnosťami, je potrebné posúdenie v sídle CAB.
Svedecké posúdenie CAB	NIE	
Je pravdepodobné, že na prechod bude potrebný čas navyše?	ÁNO	Posudzovanie zahŕňa minimálne dodatočný 0,5-dňový deň posudzovania na potvrdenie prechodu CAB, keď sa prechod vykonáva ako samostatné posudzovanie.
Iné	ÁNO	1) AB určí časový harmonogram predloženia žiadosti o prechod orgánom posudzovania zhody v programe posudzovania prechodu.

Činnosť	Áno/Nie	Poznámky/záznamy:
		2) AB prijme rozhodnutie o prechode na základe prechodového posúdenia (í). 3) V prípade potreby AB aktualizuje akreditačné informácie akreditovaného CAB (napr. osvedčenie o akreditácii), ak bola preukázaná ich kompetentnosť na ISO/IEC 27001: 2022. 4) Ak akreditovaný CAB úspešne nedokončí posúdenie prechodu pred príslušným dátumom uvedeným v kapitole 1, dátum skončenia platnosti jeho akreditácie na ISO/IEC 27001: 2013 nesmie byť neskôr než je koniec prechodového obdobia.

5.2 ČINNOSTI ORGÁNU POSUDZOVANIA ZHODY (CAB)

Činnosť	Áno/Nie	Poznámky/záznamy:
Opatrenia CAB	ÁNO	1) CAB stanoví svoje prechodové činnosti pre ISO/IEC 27001: 2022 s prihliadnutím na požiadavky tohto dokumentu a prechodové činnosti príslušného akreditačného orgánu. 2) Prechodovými činnosťami sa rieši, čo má CAB urobiť a čo má urobiť klient. CAB môže mať niekoľko samostatných dokumentov na riešenie prechodových činností. 3) Prechodové činnosti zahŕňajú prinajmenšom zváženie týchto skutočností: • zmeny v norme ISO/IEC 27001 a GAP rozdielovú analýzu; • potreba upraviť súvisiace certifikačné procesy, dokumenty a prípadne IT systémy na riadenie certifikačných činností; • príslušní pracovníci sú kompetentní pre ISO/IEC 27001: 2022 a proces prechodu; • audítorský tím ako celok musí mať znalosti o všetkých opatreniach obsiahnutých v norme ISO/IEC 27001: 2022 a o ich vykonávaní

Činnosť	Áno/Nie	Poznámky/záznamy:
		(pozri normu ISO/IEC 27006: 2015, 7.1.2.1.3 b)) ; • program prechodových auditov; • dochádza k včasnej komunikácii s klientmi o programe prechodu, napríklad o časovom harmonograme, prístupe k prechodovému auditu a o dôsledkoch, ak sa klientovi nepodarí prejsť pred koncom prechodového obdobia. 4) CAB sa odporúča, aby pri najbližšej príležitosti naplánovali a začali prijímať požadované opatrenia.
Prechodový audit	ÁNO	1) CAB môže vykonávať prechodový audit v spojení s dozorovým auditom, recertifikačným auditom alebo prostredníctvom samostatného auditu. 2) Prechodový audit sa nesmie spoliehať len na preskúmanie dokumentov, najmä pokiaľ ide o preskúmanie technologických opatrení. 3) Prechodový audit zahŕňa okrem iného: • GAP rozdielovú analýzu normy ISO/IEC 27001: 2022, ako aj potrebu zmien klientov ISMS; • aktualizáciu vyhlásenia o aplikovateľnosti; • v prípade potreby, aktualizáciu plánu zaobchádzania s rizikom; • implementáciu a účinnosť nových alebo zmenených opatrení, ktoré si vybrali klienti. 4) CAB môže vykonávať prechodový audit na diaľku, ak zabezpečí splnenie cieľov prechodového auditu.
Je pravdepodobné, že na prechod bude potrebný čas navyše ?	ÁNO	1) Audit zahŕňa minimálne 0,5 auditodňa na potvrdenie prechodu certifikovaných klientov, keď sa prechod vykonáva v spojení s recertifikačným auditom. 2) Audit zahŕňa minimálne 1,0 auditodeň na potvrdenie prechodu certifikovaných klientov,

Činnosť	Áno/Nie	Poznámky/záznamy:
		keď sa prechod vykonáva v spojení s dozorným auditom alebo ako samostatný audit.
Iné	ÁNO	1) CAB môže definovať harmonogram predkladania žiadosti o prechod certifikovanými klientmi v programe auditu prechodu. 2) CAB prijme rozhodnutie o prechode na základe výsledku prechodového auditu. 3) CAB aktualizuje certifikačné dokumenty certifikovaného klienta, ak jeho ISMS spĺňa požiadavky normy ISO/IEC 27001: 2022. Poznámka: Keď sa aktualizuje certifikačný dokument, pretože klient úspešne absolvoval iba prechodový audit, vypršanie jeho aktuálneho certifikačného cyklu sa nezmení 4) Platnosť všetkých certifikácií podľa normy ISO/IEC 27001: 2013 uplynie alebo sa odoberie na konci prechodového obdobia.

5.3 INÉ ČINNOSTI

4.3.1 Posúdenie sídla CAB v nadväznosti na rozhodnutie o prechode sa zameria na overenie vykonávania prechodových činnosti pred úplným dokončením prechodových činnosti CAB. Toto hodnotenie sídla musí obsahovať minimálne tieto údaje:

- implementácia revidovaných procesov a postupov CAB;
- odborná spôsobilosť príslušného personálu sa preukáže predtým, ako sa zapojí do certifikačných činností podľa normy ISO/IEC 27001: 2022;
- postup (priebeh) prechodu certifikovaných klientov na ISO/IEC 27001: 2022.

4.3.2 Všetky svedecké posúdenia vybrané po rozhodnutí o prechode musia byť vykonané podľa ISO/IEC 27001: 2022 a zamerané na spôsobilosť CAB vykonávať audit na základe normy ISO/IEC 27001: 2022.

6 SÚVISIACE PREDPISY

ISO/IEC 17021-1: 2015	Posudzovanie zhody. Požiadavky na orgány certifikujúce systémy manažérstva. Časť 1: Požiadavky
ISO/IEC 27001: 2022	Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky.
ISO/IEC 27002: 2022	Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Opatrenia informačnej bezpečnosti
ISO/IEC 27006: 2015	Informačné technológie. Bezpečnostné techniky. Požiadavky na orgány zabezpečujúce audit a certifikáciu systémov riadenia bezpečnosti informácií
IAF MD 26: 2023	Požiadavky na prechod na ISO/IEC 27001: 2022
Zákon č. 53/2023 Z. z.	o akreditácii orgánov posudzovania zhody