Změnový list 09/24 k MPA 50-01-24 verze 2

K aplikaci ČSN EN ISO/IEC 17021-1:2016 Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu – Část 1: Požadavky v akreditačním systému České republiky:

- Implementace ČSN EN ISO 27006-1:2024,
- formálních úprav

s účinností od 01. 01. 2025 takto:

Část „1 Úvod“ se:
a) mění první odstavec, který zní takto:

V tomto vydání MPA je zapracována norma ČSN EN ISO/IEC 27006-1:2024 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Požadavky na orgány provádějící audit a certifikaci systémů managementu informační bezpečnosti - Část 1: Obecně a upřesněn výpočet doby posuzování, pokud požadovaný rozsah akreditace žadatele neobsahuje systém managementu kvality.

b) upřesňuje odrážka sedmá, která zní takto:

- systémů managementu informační bezpečnosti (ISMS),

c) upřesňuje odrážka poslední, která zní takto:

- dokumenty vertikálního charakteru obsahující požadavky a/nebo výklady vztahující se k určitým jednotlivým certifikačním schématům (konkrétním jednotlivým systémům managementu) nebo schématu EMAS. Jedná se např. o požadavkové nebo výkladové dokumenty týkající se akreditace certifikačních orgánů k výkonu certifikace v konkrétních oblastech systému managementu (např. ČSN EN ISO/IEC 27006-1:2024 pro oblast certifikace systému managementu informační bezpečnosti atp.).

Část „10 Přechodná a závěrečná ustanovení“ se mění takto:

Tento MPA 50-01-xx nabývá účinnosti dnem 01. 01. 2025 a ruší předchozí MPA 50-01-24 verze 2 ze dne 27. 10. 2024.

Část „PŘÍLOHA 1 Postup pro stanovení počtu WA“ v části „1) Obecně“, upřesňuje řádek poř. č. 9, který zní takto:

9.	Systémy managementu informační bezpečnosti (ISMS)	1	3	-

Část „PŘÍLOHA 2 Předpokládaný časový rozsah posuzování“ v části „Další oblasti posuzování“, se doplňuje nový odstavec ve „vysvětlivkách“ pod tabulkou pro „časové kapacity“, který zní takto:

Pokud požadovaný rozsah akreditace neobsahuje QMS, bude jako základ pro výpočet doby trvání posuzování zvolen jiný systém z rozsahu akreditace v tomto pořadí EMS, OHSMS , BCMS, CSR, FSMS nebo další podle převažujících aktivit konkrétního certifikačního orgánu.

Část „PŘÍLOHA 4 Posuzování shody v oblasti systémů managementu“ v části „viii ISMS“, se mění takto:

Akreditace pro účely certifikace systémů managementu informační bezpečnosti (ISMS)

akreditace je prováděna podle

ČSN EN ISO/IEC 17021-1:2016 Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu

ve spojení s

ČSN EN ISO/IEC 27006-1:2024 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Požadavky na orgány provádějící audit a certifikaci systémů managementu informační bezpečnosti - Část 1: Obecně

norma určená k posuzování shody (certifikační norma)

ČSN EN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

ČSN EN ISO/IEC 27001:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky

rozsah akreditace / klasifikace činností

V příloze OA se nespecifikuje rozsah kódů uvedených v Příloze 5 tohoto MPA.

doba auditu

Postupy pro určení délky auditu jsou popsány v článku 9.1.4 ČSN EN ISO/IEC 17021-1:2016. Kromě toho se použijí následující požadavky a návody stanoveny v článku 9.1.4 ČSN EN ISO/IEC 27006-1:2024. Certifikační orgán musí ke stanovení doby auditu použít normativní Přílohu C. Další návody a příklady výpočtu doby trvání auditu jsou poskytnuty v informativní Příloze D.

certifikace na více místech

Postupy pro určení délky auditu jsou popsány v článku 9.1.5 ČSN EN ISO/IEC 17021-1:2016. Kromě toho se použijí požadavky a návody stanovené v článku 9.1.5 ČSN EN ISO/IEC 27006-1:2024.

stanovení požadavků na kompetence pracovníků

V článku 7 normy ČSN EN ISO/IEC 27006-1:2024 jsou stanoveny specifické požadavky na kompetence pracovníků certifikačního orgánu pro certifikaci systémů managementu informační bezpečnosti. Dodatečné informace týkající se znalosti a dovednosti pro audit a certifikaci jsou stanoveny v normativní Příloze A této normy. Další hlediska kompetencí jsou uvedeny v informativní Příloze B.

další dokumenty/požadavky

ČSN EN ISO/IEC 27006-1:2024 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Požadavky na orgány provádějící audit a certifikaci systémů managementu informační bezpečnosti - Část 1: Obecně.