Určeno držitelům certifikátů ČSN EN ISO/IEC 27001: 2014 / ISO/IEC 27001:2013

Zlín, 11. dubna 2023
č j.: 300/256/2023
Vyřizuje: D. Shejbal, audit@itczlin.cz

Informace k přechodnému období pro normu ISO/IEC 27001:2022 (podle rezoluce IAF)

Vážená paní, vážený pane,

dovolte mi, abych Vás informoval o vydání technické normy ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky) a o úpravě postupu certifikačního orgánu provádět audity a certifikace podle normy ČSN EN ISO/IEC 27001: 2014 / ISO/IEC 27001:2013.

Dokumentem IAF MD 26:2022 stanovuje 3leté přechodné období od posledního dne v měsíci data vydání mezinárodní normy ISO/IEC 27001:2022, tzn. **přechodné období platí do 31. 10. 2025**.
Od 31. 10. 2025 certifikáty vydané podle ČSN EN ISO/IEC 27001: 2014 / ISO/IEC 27001:2013 nebudou členové IAF uznávat.

Platnost certifikátů vydávaných podle norem ČSN EN ISO/IEC 27001: 2014 / ISO/IEC 27001:2013 je stanovena paralelně – tedy nejdéle do 31. 10. 2025.

Dále je stanovena povinnost pro certifikační orgány zahájit počáteční certifikace a recertifikace podle ISO/IEC 27001:2022 nejpozději **do 30. září 2024**. Vzhledem k této povinnosti od 30. září 2024 již nebude certifikační orgán provádět počáteční certifikace a **recertifikace** podle ČSN EN ISO/IEC 27001: 2014 / ISO/IEC 27001:2013.

Získání akreditace v COSM 3002 předpokládáme do 31.10.2023.

Proč se norma ISO/IEC 27001 mění?
- Přizpůsobují se měnícímu se světu (současné potřeby, technologie, globalizace).
- Odráží potřeby všech uživatelů a zúčastněných stran.

Jaké hlavní změny nová verze normy přináší?
- V článku 6.1.3 jsou provedeny pouze redakční úpravy.
- Příloha A se odkazuje na opatření uvedená v normě ISO/IEC 27002:2022.
- Ve srovnání se starým vydáním se počet opatření v ISO/IEC 27002:2022 snižuje ze 114 opatření ve 14 oblastech na 93 opatření ve 4 oblastech (37 organizačních, 8 personálních, 14 fyzických, 34 technických). U opatření v ISO/IEC 27002:2022 je 11 opatření nových, 24 opatření je sloučeno ze stávajících opatření a 58 opatření je aktualizováno. Kromě toho je revidována struktura opatření, která zavádí "atribut" a "účel" pro každé opatření a již nepoužívá "cíl" pro skupinu opatření.

Jak tedy postupovat?
Následující kroky by Vám mohly pomoci při přechodu na nové vydání normy:
- Seznámit se se zněním aktualizované verze norem ISO/IEC 27001 novými opatřeními a definicemi, jako např. primární aktiva, RTO, RPO atd.,
  (je možné využít nabídku školení CQS absolvovat kurz Manažer a auditor systému ISMS podle normy ISO/IEC 27001:2022 – bližší informace najdete na https://www.cqs.cz/Skoleni/).

- Provést ve vaší firmě analýzu rizik s ohledem na nová opatření a nové rozdělení aktiv. (pro analýzu a hodnocení rizik lze využít normy ISO/IEC 27005:2022).
- Realizovat opatření z analýzy rizik, implementovat je do procesů ISMS.
- Implementovat nová opatření do provozní dokumentace.
- Provést interní audit s ohledem na nová opatření.
- Aktualizovat Prohlášení o aplikovatelnosti (PoA).
- Provést přezkoumání systému managementu

Na co se zaměří certifikační orgán během auditů navíc?

- Analýzu dopadu normy ISO/IEC 27001:2022 a ISO/IEC 27002:2022 na potřebu změn v systému managementu bezpečnosti informací držitele certifikátu ISMS.
- Přezkoumání organizačních, lidských, technických a fyzických opatření navazujících na požadavky ISO/IEC 27002:2022.
- Aktualizaci Prohlášení o aplikovatelnosti (PoA).
- Implementaci a účinnost nových nebo změněných činností a postupů ve Vaší organizaci.

Audity u stávajících zákazníků aneb jaký bude přístup auditorů a COSM 3002 v přechodném období?
Audit zavedených změn (implementace požadavků ISO/IEC 27001:2022) bude COSM 3002 provádět přednostně v rámci řádných dozorových nebo recertifikačních auditů a to **nejpozději do 31. 10. 2025**.
Změna certifikátu v rámci plánovaných dozorových auditů na ISO/IEC 27001:2022 bude prováděna na základě písemné žádosti v rámci dozorového auditu.

Mezinárodní akreditační fórum (IAF) vydalo pro posuzování ISO/IEC 27001:2022 závazný dokument IAF MD 26:2022, který stanovuje požadavky na certifikační orgány a který vyžaduje, aby při auditu (dozorovém či speciálním auditu) přidal certifikační orgán povinně ke standardní době trvání auditu navíc 1 auditoden (tj. 8 hodin posuzování u klienta) a při recertifikačním auditu navíc 0,5 auditodne (tj. 4 hodiny posuzování u klienta) pro ověření nových požadavků normy ISO/IEC 27001:2022.

Od 30. 09. 2024 bude certifikační orgán systémů managementu provádět certifikace (recertifikace) a vydávat certifikáty pouze podle ISO/IEC 27001:2022.

Další informaci k auditům Vám podá vedení střediska certifikace systémů managementu.
Kontakt: qscert@itczlin.cz, tel.: 572 779 982.

S pozdravem

Ing. Dušan Shejbal, Ph.D.
v.r.
zástupce ředitele divize certifikace
Institut pro testování a certifikaci, a. s.