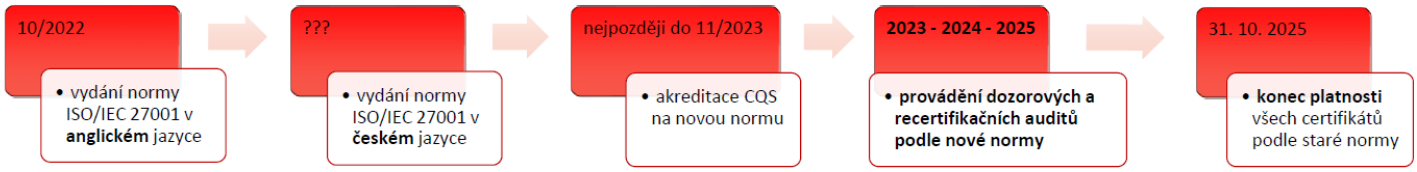
Revize normy systému managementu bezpečnosti informací ISO/IEC 27001:2022

V říjnu 2022 vyšla nová verze normy ISO/IEC 27001:2022



Každá revize norem řady ISO má stanovené přechodové období. Jednotlivé organizace – certifikační orgány a samozřejmě i certifikované organizace – mají určitý čas na implementaci změn. Pro tuto normu bylo stanoveno **tříleté** přechodové období do **31. 10. 2025**. Pro novelu ISO/IEC 27001 je tedy přechodové období následující:

- Již certifikované organizace:
  - Od **01. 11. 2025** se všechny audity budou provádět **pouze** podle nové normy, certifikáty dle ISO/IEC 27001:2013 již po tomto datu nebudou platné. Pro všechny certifikované organizace jsme povinni přidat k auditnímu času **minimálně 1 auditní den na prověření aplikace změn ISO/IEC 27001:2022 v rámci dozorového auditu**

ZMĚNA

- Nově certifikované a recertifikované organizace:
  - Od **01. 05. 2024** se všechny certifikační a recertifikační audity budou provádět **pouze** podle nové normy. Pro všechny certifikované organizace jsme povinni přidat k auditnímu času **minimálně 0,5 auditního dne na prověření aplikace změn ISO/IEC 27001:2022 v rámci recertifikačního auditu**

ZMĚNA

Audity lze podle nové normy provádět již nyní. Český překlad normy – ČSN EN ISO/IEC 27001 nebyl zatím publikován. Audity je možné provádět podle anglického originálu normy zatím neakreditovaně a po získání akreditace od Českého institutu pro akreditaci, o.p.s. Vám certifikáty aktualizujeme s odkazem na akreditaci.

Proč se norma ISO/IEC 27001 mění?

- Přizpůsobují se měnícímu se světu (současné potřeby, technologie, globalizace)
- Odráží potřeby všech uživatelů a zúčastněných stran

Jaké jsou změny v normě ISO/IEC 27001:2022?

ZMĚNA

- V článku 6.1.3 jsou provedeny pouze redakční úpravy, přidán nový bod 4.2.c), přidán nový článek 6.3 a další drobné úpravy jako přečíslování článků v kap. 9 a 10
- 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 článcích na 93 opatření ve 4 doménách. 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:

1. Zakoupit ISO/IEC 27002:2022 a ISO/IEC 27001:2022
2. Seznámit se s novými opatřeními a definicemi, jako např. primární aktiva, RTO, RPO atd., je možné absolvovat kurz CQS Manažer a auditor systému ISMS podle normy ISO/IEC 27001:2022
3. Provést analýzu rizik s ohledem na nová opatření a nové rozdělení aktiv
   (pro analýzu a hodnocení rizik je vhodné vycházet z nové normy ISO/IEC 27005:2022)
4. Realizovat opatření z analýzy rizik, implementovat je do procesů ISMS
5. Implementovat nová opatření do provozní dokumentace
6. Aktualizovat Prohlášení o aplikovatelnosti (PoA)
7. Provést interní audit s ohledem na nová opatření
8. Provést přezkoumání 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 ve Vašem systému managementu bezpečnosti informací
- Přezkoumání organizačních, lidských, technických a fyzických opatření navazujících na ISO/IEC 27002:2022
- Aktualizaci Prohlášení o aplikovatelnosti
- Implementaci a účinnost nových nebo změněných činností a postupů ve Vaší organizaci

Optimistický závěr:

Pro bezproblémový přechod na novou normu jsme pro Vás připravili kurz **Manažer a auditor systému ISMS podle normy ISO/IEC 27001:2022.** Více informací naleznete na našich stránkách **www.cqs.cz** v sekci Školení.
Náš personál a auditoři jsou Vám k dispozici ke sdílení informací týkajících se výkladu nové normy a aplikací změn s tím spojených.

Věříme, že Vám změny pomohou zlepšit nastavené procesy i celý systém managementu ve Vaší organizaci.

Jediná jistota je změna.

15. 03. 2023

Ing. Jana Olšanská
Vedoucí certifikačního orgánu CQS

CQS z.s.
Prosecká 412/74
190 00 Praha 9 – Prosek