PŘEHLED POŽADOVANÝCH ZNALOSTÍ
Auditor BI (bezpečnosti informací)

Všeobecně:

Auditoři systému KIB musí prokazovat všechny znalosti a dovednosti, které jsou požadovány u manažerů systému KIB

Auditoři musí mít důkladné a aktuální znalosti o postupech auditování a musí být schopni aplikovat nezbytné manažerské dovednosti při provádění auditů, jak je doporučováno v ISO 19011.

Musí být schopni provádět audity první, druhou a třetí stranou, při nichž se prokazuje shoda s ČSN ISO/IEC 27001 nebo jinými ekvivalentními normami, které stanovují požadavky na systém ISMS, přičemž podle potřeby berou v úvahu zaměření a požadavky ISO/IEC 17021. Musí být schopni jednat jako auditor v rámci týmu. Vedoucí auditoři musí být schopni jednat jako vedoucí týmu auditorů.

Požadované znalosti k hodnocení způsobilosti jsou ve shodě s požadavky a doporučeními těchto dokumentů:

1. Soubor mezinárodních norem ISO/IEC 27000 v platném znění, zejména ISO/IEC 27001
2. Soubor mezinárodních norem ISO/IEC 14888 v platném znění
3. Norma ČSN EN ISO 19011 v platném znění
4. ČSN EN ISO/IEC 17024 - Posuzování shody - Všeobecné požadavky na orgány pro certifikaci osob
5. ČSN EN ISO/IEC 17021 - Posuzování shody - Požadavky na orgány poskytující služby auditů a certifikace systémů managementu
6. Základní listina práv a svobod
7. 110/2019 Sb. Zákon o zpracování osobních údajů
8. Zákon o obchodních korporacích
9. Zákon o ochraně utajovaných informací
10. Zákon o některých službách informační společnosti
11. Zákon o informačních systémech veřejné správy
12. Autorský zákon
13. Zákon o telekomunikačních službách
14. Zákon č. 264/2025 Sb. Zákon o kybernetické bezpečnosti
    a. Vyhláška č. 334/2025 Sb. Vyhláška o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony

b. Vyhláška č. 408/2025 Sb. Vyhláška o regulovaných službách
c. Vyhláška č. 409/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
d. Vyhláška č. 410/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
e. Vyhláška č. 411/2025 Sb. Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy
f. Vyhláška č. 412/2025 Sb. Vyhláška o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu

15. Zákon č. 40/2009 Sb., trestní zákon
    a. § 180 Neoprávněné nakládání s osobními údaji;
    b. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
16. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
17. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)
18. zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
19. Nařízení Evropského parlamentu a Rady (EU) č. 2014/910 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES – eIDAS;
20. Všechny odkazy na legislativu jsou myšleny v platném aktuálním znění.

Základní požadavky (znalosti a dovednosti)

Úvod

Typy auditů:

- audity systému ISMS/KIB
- audity systému managementu specifické pro jiné odvětví
- audity procesu a produktu
- obchodní audity
- Normy a směrnice pro certifikaci: ISO 27001, ISO 19011 a následné platné revize
- Normy pro akreditaci: řada ISO/IEC 17000, směrnice pro akreditaci
- Základy auditování

- Psychologické aspekty
- Certifikace

1. Okruhy znalostí:

- Význam bezpečnosti informací
- Management bezpečnosti informací
- Organizace managementu informací
- Klasifikace a řízení aktiv
- Personální bezpečnost
- Fyzická bezpečnost a bezpečnost prostředí
- Řízení komunikací a řízení provozu
- Vývoj a údržba systémů
- Řízení kontinuity činností organizace
- Soulad s požadavky
- Sociální hlediska
- Právní a regulační hlediska

1) znalosti řízení rizik bezpečnosti informací na takové úrovní, která auditorům umožní hodnotit použité metody řízení rizik;
2) znalosti bezpečnosti informací (co to je bezpečnost informací) a řízení bezpečnosti informací (jak řídit bezpečnost informací);
3) znalosti umožňující auditorům vyhodnotit výběr opatření, plán zavedení opatření, samotné zavedení opatření, udržování opatření a účinnost zavedených opatření;
4) znalosti pro vyhodnocení použité IT technologie (tj. informovanost o v auditované organizací používaném HW, SW, sítích, antimalware programech…

2. Plánování a příprava programu auditu systému ISMS/KIB

- řízení programu auditu
- role a odpovědnosti auditora, auditovaného a klienta
- záznamy o programu auditu, plány auditu
- vypracování a používání kontrolních seznamů
- kombinované audity systému, společné audity
- přezkoumání a monitorování programu auditu

3. Činnosti procesu auditu

- iniciování auditu
- proveditelnost auditu
- sestavení týmu auditorů
- přípravné jednání

- počáteční přezkoumání dokumentů
- plánování činností při auditu na místě
- zahajovací jednání
- činnosti při auditu na místě
- metody provádění rozhovorů
- komunikování s klientem a auditovaným
- shromažďování důkazů
- dokumentování zjištění z auditu
- neshody
- závěrečné jednání
- nápravná opatření

4. Podávání zpráv

- vypracování zprávy
- obsah zprávy
- schválení a distribuce zprávy
- uchovávání zprávy/dokumentů
- důvěrnost

5. Následná opatření

- opakování auditů
- dozory
- efektivnost následného nápravného opatření

6. Kompetence a hodnocení A-BI

- Osobní chování
- Znalosti a dovednosti
  - Systémů managementu
  - Specifické pro obor a odvětví
  - Všeobecné znalosti a dovednosti vedoucího týmu auditorů
- Hodnocení auditora (kritéria hodnocení, metody hodnocení, provádění hodnocení)
- Udržování a zlepšování kompetencí auditora