Znalosti a dovednosti držitele akreditovaného personálního certifikátu

Auditor BI (bezpečnosti informací)

Všeobecně:

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

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 vedoucí týmu auditorů nebo jako auditor v rámci týmu.

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. Zákon o ochraně 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. Trestní zákon

15. Zákon o kybernetické bezpečnosti
16. Zákon č. 40/2009 Sb., trestní zákon § 180 Neoprávněné nakládání s osobními údaji; § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
17. 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)
18. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (tzv. směrnice NIS).
19. Všechny odkazy na zákony jsou myšleny v platném aktuálním znění.

Základní požadavky (znalosti a dovednosti)

Popis úkolů Auditora BI	**Příslušné znalosti a dovednosti**
a) Vytvářet, implementovat, vyhodnocovat a zlepšovat programy auditů	Být schopen vytvářet, přezkoumávat a zlepšovat auditní programy (podle ISO 19011), zejména: Být schopen definovat vhodně auditní program ve smyslu cílů, rozsahu a zdrojů Být schopen rozpoznat a minimalizovat rizika, překážky a obtíže, vztahující se k auditnímu programu Být schopen provádět auditní program ve smyslu informování zúčastněných o auditním programu, specifikovat cíle, rozsah a kritéria jednotlivých auditů, organizovat provedení jednotlivých auditů – týmy, čas, zdroje); vedení a zaznamenávání auditních programů, jednotlivých auditů a auditního personálu. Být schopen vybrat a používat vhodné metody a nástroje auditu, určit rozsah a cíle auditu (např. vybrat vhodné typy auditu (např. v závislostí na cílech, rozsahu a kritériích - systém, procesy, shoda) Znát proces stanovení a vyhodnocení kompetencí osob, zúčastněných na auditech Znát požadavky na odborné kompetence auditorů (osobní chování, etika, dovednosti) a být schopen je využít při sestavování auditního týmu Být schopen monitorovat auditní program Být schopen přezkoumávat a zlepšovat auditní program
	Interní audity
	Certifikační proces ISMS
	Externí audity
b) Iniciovat, plánovat, provádět a přezkoumávat • udity systémů managementu • rocesní audity	Chápat důležitost auditu pro růst provozní výkonnosti
	Být schopen vysvětlit ostatním osobám prospěšnost auditu
	Rozumět principům auditu, postupům, metodám a technikám auditu a aplikovat je v auditní praxi Být schopen provést audit jednotematického nebo kombinovaného systému
	Být schopen realizovat procesní audity
	Vědět, jak se dělají audity shody (podle potřeby s experty)

Popis úkolů Auditora BI	**Příslušné znalosti a dovednosti**
• udity shody	Být schopen iniciovat, připravit a provést auditní aktivity se zaměřením na cíle a hraniční podmínky organizace (podle kap. 6 ISO 19011), zejména: Chápat roli a úkoly auditora ve všech fázích auditu Být schopen pochopit a klasifikovat úkoly a zodpovědnosti auditovaných osob Být schopen iniciovat audit od prvního kontaktu, určujícího uskutečnitelnost auditu Být schopen připravit audit ve smyslu vytvoření plánu auditu, přidělení rolí jednotlivým členům auditního týmu a přípravy dokumentovaných informací pro audit. K tomu patří např.: • Být schopen zvolit a použít vhodné metody a nástroje auditu s ohledem na rozsah a cíle auditu • Být schopen rozeznat a minimalizovat rizika, překážky a obtíže, týkající se plánování a harmonogramu Být schopen provést auditní aktivity, jako jsou: přidělení rolí a zodpovědností průvodců a pozorovatelů, zahajovací schůzka, komunikace v průběhu auditu, dostupnost a přístup k auditním informacím, přezkoumání dokumentovaných informací, sběr a ověřování informací vytváření zjištění z auditu, stanovení závěrů z auditu a závěrečná schůzka. Mezi jiným k tomu patří: • Být schopen řídit organizování jednotlivých členů týmu podle cílů auditu • Být schopen používat na cíl orientované techniky dotazování ve všech fázích auditu • Rozeznat rizika auditu, překážky a obtíže v průběhu provádění, vyhnout se konfliktům a být schopen je zvládnout v případě, že nastanou Být schopen uzavřít audit a vést následná opatření.
c) Posoudit systémy managementu bezpečnosti informací	Znát a být schopen interpretovat relevantní legislativu, regulativu a normy, týkající se auditovaného systému managementu Být schopen analyzovat a hodnotit charakteristiky a vlastnosti procesů Být schopen vyhodnotit výsledky procesů ve smyslu dosahování cílů a shody Být schopen vyhodnotit během auditu implementaci plánovaných akcí k dosažení cílů na základě strategie a cílů organizace

1	**Obecně.**
	Druhy auditů - audity systému managementu, audity produktu a procesu. Normy a směrnice ISO Normy EN řady 1702x Porovnání norem. Psychologická hlediska. Certifikace.
2	**Plánování a přípravy auditu BI**
3	**Průběh auditu**
4	**Zpracování zprávy**
5	**Následné činnosti**