1. **Příloha** je součástí dokumentu „**Informací pro žadatele o certifikát Certifikačního schématu Systémy managementu organizace**“, kde jsou uvedeny další informace:
   - Celkové certifikační schéma pro **SYSTÉMY MANAGEMENTU ORGANIZACÍ**,
   - popis náplně práce a úkolů manažera systému managementu organizace – obecně,
   - popis náplně práce a úkolů auditora systému managementu – obecně,
   - požadovaná odborná způsobilost pro manažery systému managementu organizace,
   - požadovaná odborná způsobilost pro auditory systému managementu organizace,
   - požadované schopnosti,
   - nezbytné předpoklady
   - pravidla chování manažera a auditora SM.

   Požadavky na proces certifikace:
   - Postup při certifikaci osob,
   - zkušební řád,
   - metody a kritéria týkající se dozoru,
   - kritéria pro pozastavování a odnímání certifikace,
   - kritéria pro změnu rozsahu nebo úrovně certifikace.

2. Přehled požadovaných znalostí Auditora BI (Bezpečnosti informací)

Všeobecně:

Auditoři systému ISMS (systém řízení bezpečnosti informací) 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 ve směrnici 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) Směrnice ČSN EN ISO 19011 v platném znění

(3) ČSN EN ISO/IEC 17024 - Posuzování shody – Všeobecné požadavky na orgány pro certifikaci osob

(4) ČSN EN ISO/IEC 17021 - Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu

(5) ČSN ISO/IEC 27006 v platném znění – Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

(6) ČSN ISO/IEC 27007 – Informační technologie-Bezpečnostní techniky-Směrnice pro audit systémů řízení bezpečnosti informací
(7) Základní listina práv a svobod
(8) Zákon o ochraně osobních údajů
(9) Zákon o obchodních korporacích
(10) Zákon o ochraně utajovaných informací
(11) Zákon o některých službách informační společnosti
(12) Zákon o informačních systémech veřejné správy
(13) Autorský zákon
(14) Zákon o telekomunikačních službách
(15) Trestní zákon
(16) Zákon o kybernetické bezpečnosti
(17) Vyhláška o kybernetické bezpečnosti
(18) Zákon č. 40/2009 Sb., trestní zákon § 180 Neoprávněné nakládání s osobními údaji; § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
(19) 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)
(20) 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).
(21) Všechny odkazy na zákony jsou myšleny v platném aktuálním znění.
(22) Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
(23) 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;

Základní požadavky (znalosti a dovednosti)

1. <u>Úvod</u>

Typy auditů:

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

2. <u>Okruhy znalostí:</u>

- 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. specializace na v auditované organizací používané HW, SW, sítě, antivirové programy,

3. <u>Plánování a příprava programu auditu systému ISMS</u>

- 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

4. Činnosti procesu auditu

- iniciování auditu
- proveditelnost auditu
- sestavení týmu auditorů
- přípravné jednání
- počáteční přezkoumání dokumentů
- plánování činností při auditu na místě
- činnosti při auditu na místě

- metody provádění rozhovorů
- komunikování s klientem a auditovaným
- shromažďování důkazů
- dokumentování zjištění z auditu
- neshody
- závěrečné jednání
- nápravná opatření

5. <u>Podávání zpráv</u>

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

6. <u>Následná opatření</u>

- opakování auditů
- dozory
- efektivnost následného nápravného opatření

7. <u>Kvalifikace auditorů systému managementu</u>

- osobní vlastnosti
- 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

8. Specifické znalosti a dovednosti pro audit v oblasti ISMS (vycházející z normy ISO /IEC 27006, příloha A)

a. Programování a plánování auditu
b. Typy a metodiky auditu
c. Rizika auditu
d. Analýza procesů bezpečnosti informací
e. Neustálé zlepšování
f. Interní audit bezpečnosti informací

9. Znalosti a dovednosti pro audit v oblasti ISMS (vycházející z normy ISO /IEC 27006, příloha A) – porozumění znalosti

a. Duševní vlastnictví
b. Obsah, ochrana a uchování záznamů organizace
c. Ochrana dat a soukromí
d. Regulace kryptografických opatření
e. Elektronický obchod
f. Elektronický a digitální podpis
g. Dohled nad pracovištěm
h. Telekomunikační zachycení a monitorování dat (např.- e-mailu)
i. Zneužití počítače
j. Shromáždění elektronických důkazů
k. Penetrační testování
l. Požadavky specifické pro mezinárodní a národní obory