PŘEHLED POŽADOVANÝCH ZNALOSTÍ
MANAŽER BI

Požadované znalosti k hodnocení způsobilosti jsou ve shodě jednak s požadavky a doporučeními technických norem:

- řady ČSN ISO/IEC 27000 a ISO/IEC 14888

jednak s požadavky právních předpisů:

- Základní listina práv a svobod
- 110/2019 Sb. Zákon o zpracování osobních údajů
- Zákon o obchodních korporacích
- Zákon o ochraně utajovaných informací
- Zákon o některých službách informační společnosti
- Zákon o informačních systémech veřejné správy
- Autorský zákon
- Zákon o telekomunikačních službách
- Trestní zákon
- Zákon č. 264/2025 Sb. Zákon o kybernetické bezpečnosti
    - Vyhláška č. 334/2025 Sb. Vyhláška o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony
    - Vyhláška č. 408/2025 Sb. Vyhláška o regulovaných službách
    - Vyhláška č. 409/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
    - Vyhláška č. 410/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
    - Vyhláška č. 411/2025 Sb. Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy
    - Vyhláška č. 412/2025 Sb. Vyhláška o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu
- Zákon č. 40/2009 Sb., trestní zákon
    - § 180 Neoprávněné nakládání s osobními údaji;
    - § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- 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)
- 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)

Všechny odkazy na zákony jsou myšleny v platném aktuálním znění.

VÝZNAM BEZPEČNOSTI INFORMACÍ

- pro společnost, organizaci, zákazníka, stát, životní prostředí.
- základní pojmy – dostupnost, důvěrnost, integrita
- testování KIB, zlepšování KIB, systémy KIB, penetrační testy, testy obnovy, testy plánů kontinuity.
- Bezpečnostní politika - úloha managementu, cíle bezpečnosti informací.
- Management - úloha manažerů ISMS/KIB, funkce a postavení v organizaci.

ORGANIZACE – OBECNÉ ZÁSADY

- Typy organizací – formální uspořádání, organizační struktury, funkce, delegování funkcí

MANAGEMENT BEZPEČNOSTI INFORMACÍ

- Bezpečnostní politika, strategie, cíle, principy
- Vedení a řízení – systém managementu KIB jako podsystém managementu organizace
- Ověřování bezpečnosti – vnitřní audity, přezkoumání vedením, zákaznické audity, audity třetí stranou, testování

ORGANIZACE MANAGEMENTU INFORMACÍ

- Fórum pro management bezpečnosti informací
- Koordinace bezpečnosti
- Delegování pravomocí
- Schvalovací proces pro prostředky IT, konzultace, spolupráce mezi organizacemi, nezávislá přezkoumání

KLASIFIKACE A ŘÍZENÍ AKTIV

- Evidence aktiv
- Klasifikace informací
- Směrnice pro klasifikaci
- Označování a nakládání s informacemi

PERSONÁLNÍ BEZPEČNOST

- Bezpečnost v popisu práce a při zajišťování lidských zdrojů
- Zahrnutí bezpečnosti do pracovních povinností
- Prověřování zaměstnanců a politika, Podmínky výkonu pracovní činnosti

- Smlouva o ochraně důvěrných informací
- Školení uživatelů, Vzdělávání a školení v oblasti bezpečnosti informací
- Reakce na bezpečnostní incidenty a selhání, Hlášení selhání programového vybavení
- Ponaučení z incidentů, Disciplinární proces

FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

- Zabezpečené oblasti
- Bezpečnost zařízení
- Obecná opatření

ŘÍZENÍ KOMUNIKACÍ A ŘÍZENÍ PROVOZU

- Provozní postupy a odpovědnosti
- Plánování a systém přejímání
- Ochrana proti škodlivým programům
- Vnitřní správa
- Správa sítě
- Bezpečnost při zacházení s médii
- Výměny informací a programů

ŘÍZENÍ PŘÍSTUPU

- Požadavky na řízení přístupu
- Řízení přístupu uživatelů
- Odpovědnosti uživatelů
- Řízení přístupu k síti
- Řízení přístupu k operačnímu systému
- Řízení přístupu k aplikacím
- Monitorování přístupu k systému a jeho použití
- Mobilní výpočetní prostředky a práce na dálku

KRYPTOGRAFIE

- Šifrování, klíče, pravidla

PROVOZ

- Zálohování - prostředky, pravidla
- Řízení změn
- Antimalware
- Logování

ŘÍZENÍ INCIDENTU

- Událost, incident

- Posouzení, eskalace
- Řešení, poučení, prevence, hlášení NÚKIB

VÝVOJ A ÚDRŽBA SYSTÉMŮ

- Bezpečnostní požadavky systémů
- Bezpečnost v aplikačních systémech
- Kryptografická opatření
- Bezpečnost systémových souborů
- Bezpečnost procesů vývoje a podpory

ŘÍZENÍ KONTINUITY ČINNOSTÍ ORGANIZACE

- Hlediska řízení kontinuity činností organizace
- Proces řízení kontinuity činností organizace
- Kontinuita činností organizace a analýza dopadů
- Vytváření a implementace plánů kontinuity
- Systém plánování kontinuity činností organizace
- Testování, udržování a přezkoumání plánů kontinuity

SOULAD S POŽADAVKY

- Soulad s právními normami
- Přezkoumání bezpečnostní politiky a technické shody
- Hlediska auditu systému

SOCIÁLNÍ HLEDISKA

- Manažerské nástroje a dovednosti
- Uspokojování pracovníků - motivace, odměňování, uznávání, řízení lidských zdrojů a hodnocení spokojenosti personálu.
- Komunikace - komunikace, postavení a úloha odborníků, řízení změny, účast na řízení a míra součinnosti, motivační hlediska v organizaci a v jejím managementu, styl/kultura vedení, dobré jméno podniku/organizace.

PRÁVNÍ A REGULAČNÍ HLEDISKA

- Legislativa - národní a mezinárodní legislativa, zákony, bezpečnost, analýza rizik, smluvní záruky, záruky
- Zákon o ochraně osobních údajů
- GDPR, procesy GDPR
- Kybernetická bezpečnost

VÝBĚR BEZPEČNOSTNÍCH OPATŘENÍ

- Posouzení relevance opatření
- Vhodnost a přiměřenost opatření