Vzdelávací program: Audítor kybernetickej bezpečnosti

Profil absolventa

Absolvent vzdelávacieho programu „Audítor kybernetickej bezpečnosti“ je vysoko kvalifikovaný odborník schopný vykonávať komplexné audity kybernetickej bezpečnosti v organizáciách. Disponuje hĺbkovými vedomosťami o procesoch riadenia bezpečnosti, právnych predpisoch, analýze rizík, bezpečnostných mechanizmoch a metodikách auditu. Je schopný posudzovať dôkazy, vypracovávať prehľadné správy a navrhovať opatrenia na zlepšenie bezpečnosti. Absolvent efektívne komunikuje s vedením, tímami a orgánmi verejnej moci, pričom uplatňuje analytické a strategické myslenie pri hodnotení systémov a procesov.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
   - Ovláda procesy a systémy riadenia kybernetickej bezpečnosti, vrátane fyzickej a objektovej bezpečnosti (BL 6).
   - Rozumie zásadám organizácie bezpečnosti, riadenia prístupov, kryptografických mechanizmov a testovania bezpečnosti (BL 6).
   - Pozná právne predpisy a normy (napr. zákon č. 69/2018 Z. z., GDPR, STN EN ISO/IEC 17024) a metodiky ochrany osobných údajov (BL 6).
   - Chápe procesy riadenia rizík, analýzy hrozieb, kontinuity činností a havarijnej obnovy (BL 6).
   - Má znalosti o sieťových technológiách, podnikových architektúrach (napr. TOGAF) a audítorských metodikách (BL 6).
   - Rozumie princípom riadenia projektov, nákladov, ľudských zdrojov a dodávateľských služieb (BL 6).
2. **Zručnosti**:
   - Navrhuje a uplatňuje bezpečnostné stratégie a politiky.
   - Vykonáva analýzu rizík, posudzuje dôkazy a hodnotí bezpečnostné mechanizmy.
   - Vypracováva prehľadné záverečné správy o výsledkoch auditu.
   - Prioritizuje úlohy, efektívne priraďuje zdroje a vedie audítorské tímy.
   - Koordinuje audity a spolupracuje s orgánmi verejnej moci.
   - Implementuje metodiky auditu a posudzuje súlad s právnymi a technickými normami.
3. **Postoje**:
   - Zodpovedný a etický prístup k auditu a ochrane údajov.
   - Objektivita pri posudzovaní dôkazov a navrhovaní odporúčaní.
   - Proaktívne riešenie bezpečnostných nedostatkov a podpora súladu.
   - Schopnosť efektívne komunikovať s rôznymi zainteresovanými stranami.
4. **Špecifické kompetencie**:
   - Schopnosť prijímať rozhodnutia a myslieť v súvislostiach.
   - Analytické myslenie, kreativita a prezentačné zručnosti.
   - Schopnosť viesť tímy, delegovať úlohy a organizovať prácu.

- Poskytovanie spätnej väzby a riadenie audítorských procesov.

Požiadavky na vstup:

- **Vzdelanie**: Úplné stredné všeobecné alebo odborné, vysokoškolské I., II. alebo III. stupňa.
- **Odborná prax**:
  - Minimálne 5–10 rokov praxe v oblasti IT, z toho 3–7 rokov v riadení IT služieb, informačnej bezpečnosti, riadenia rizík, architektúry IT alebo regulácie kybernetickej bezpečnosti.
- **Špecifická kvalifikácia**:
  - Medzinárodný certifikát z auditu informačných systémov alebo certifikát manažéra kybernetickej bezpečnosti (podľa STN EN ISO/IEC 17024).
  - Zoznam vykonaných auditov s overiteľnými referenciami.

Metódy vzdelávania

Vzdelávací program kombinuje teoretické, praktické a audítorské metódy zamerané na rozvoj odborných a riadiacich zručností:

1. **Interaktívne prednášky**:
   - Vysvetlenie audítorských metodík, právnych predpisov (napr. GDPR, zákon č. 69/2018 Z. z.) a štandardov (napr. ISO/IEC 17024).
   - Diskusie o riadení rizík, podnikových architektúrach a bezpečnostných mechanizmoch.
2. **Praktické workshopy**:
   - Simulácie auditu kybernetickej bezpečnosti, vrátane posudzovania dôkazov a analýzy rizík.
   - Nácvik tvorby audítorských správ a odporúčaní na zlepšenie.
   - Cvičenia na hodnotenie bezpečnostných mechanizmov (napr. firewally, kryptografické systémy).
3. **Prípadové štúdie**:
   - Analýza reálnych audítorských scenárov a posudzovanie súladu s normami.
   - Skupinové projekty na hodnotenie bezpečnostných politík a procesov organizácie.
4. **E-learning a samoštúdium**:
   - Prístup k online materiálom, certifikačným prípravám (napr. CISA, CRISC) a metodickým usmerneniam Úradu na ochranu osobných údajov.
   - Interaktívne kvízy na overenie vedomostí o právnych predpisoch a audítorských postupoch.
5. **Simulácie auditu**:
   - Role-playing scenáre, kde účastníci vykonávajú modelový audit IT systémov.
   - Koordinácia audítorského tímu a komunikácia s vedením organizácie.
6. **Mentorované projekty**:
   - Samostatné projekty na vypracovanie audítorskej správy alebo návrhu bezpečnostných opatrení.
   - Mentorovanie zamerané na rozvoj analytických a prezentačných zručností.

Forma vzdelávania

Program je navrhnutý ako kombinovaný, aby vyhovoval odborníkom s náročným pracovným harmonogramom:

1. **Prezenčná forma**:
    - Intenzívne workshopy v školiacich centrách zamerané na praktické audítorské cvičenia a tímovú spoluprácu.
    - Trvanie: 3 dni.
2. **Online forma**:
    - Videokonferenčné školenia cez bezpečné platformy s dôrazom na teoretické prednášky a diskusie.
    - Prístup k e-learningovým platformám s nahratými prednáškami a samoštudijnými materiálmi.
    - Vhodné pre samoštúdium a vzdialený prístup.
3. **Kombinovaná forma**:
    - Kombinácia prezenčných workshopov (napr. na simulácie auditu) a online samoštúdia.
    - Účastníci absolvujú praktické cvičenia na mieste a teoretickú časť online, čo zvyšuje flexibilitu.

Metódy hodnotenia

Hodnotenie je zamerané na overenie teoretických vedomostí, audítorských zručností a schopnosti aplikovať metodiky:

1. **Znalostné testy**:
    - Písomné alebo online testy zamerané na právne predpisy, audítorské metodiky, riadenie rizík a bezpečnostné mechanizmy.
    - Formát: esejové otázky, analýza scenárov, výber z možností.
2. **Praktické audítorské úlohy**:
    - Vykonanie simulovaného auditu IT systému, vrátane posúdenia dôkazov a rizík.
    - Vypracovanie audítorskej správy s odporúčaniami na zlepšenie bezpečnosti.
    - Hodnotí sa presnosť, úplnosť a súlad s normami.
3. **Prípadové štúdie**:
    - Analýza hypotetického alebo reálneho auditu a návrh opatrení na odstránenie nedostatkov.
    - Hodnotí sa schopnosť identifikovať riziká, posúdiť súlad a navrhnúť riešenia.
4. **Prezentácie a ústne skúšanie**:
    - Prezentácia audítorskej správy alebo odporúčaní pred komisiou.
    - Hodnotí sa prezentačná zručnosť, argumentácia a schopnosť obhájiť zistenia.
5. **Simulácie riadenia auditu**:
    - Koordinácia modelového audítorského tímu a komunikácia s vedením.
    - Hodnotí sa schopnosť delegovať úlohy, riadiť procesy a poskytovať spätnú väzbu.

Kritériá úspešnosti:

- Úspešné absolvovanie programu vyžaduje dosiahnutie minimálne 85 % úspešnosti v znalostných testoch, praktických úlohách a simuláciách.

- Účastníci obdržia certifikát o absolvovaní programu po splnení všetkých požiadaviek, ktorý môže slúžiť ako príprava na medzinárodné certifikácie (napr. CISA).

Záver

Vzdelávací program „Audítor kybernetickej bezpečnosti“ pripravuje odborníkov na vykonávanie komplexných auditov kybernetickej bezpečnosti s dôrazom na súlad s právnymi normami a metodikami. Kombinácia teoretických prednášok, praktických simulácií a projektov zaisťuje, že absolventi sú schopní efektívne posudzovať bezpečnostné systémy, navrhovať opatrenia a komunikovať s rôznymi zainteresovanými stranami.