

Špecialista pre riadenie súladu

Rola:	Špecialista pre riadenie súladu	
Vedomosti:	<p>Riadenie bezpečnosti</p> <ol style="list-style-type: none"> 1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti BL5 2) zásady organizácie informačnej a kybernetickej bezpečnosti BL5 3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti BL5 4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí BL4 5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.) BL5 6) zdroje, charakteristiky a použitie informačných aktív organizácie BL5 7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami BL5 8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI) BL5 9) procesy riadenia kontinuity činností a plánovania havarijnej obnovy prevádzky BL4 10) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) BL3 11) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia) BL3 12) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov BL3 13) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti BL3 14) princípy zálohovania a obnovy dát BL6 15) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch BL5 <p>Riadenie hrozieb a rizík</p> <ol style="list-style-type: none"> 1) procesy riadenia rizík, postupy a metodiky analýzy rizík BL4 2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie BL3 	

3) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL3*
4) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletiny)	BL3
5) triedy a vektory útokov	BL3
Aplikácia bezpečnostných opatrení	
1) navrhovanie opatrení na ošetrovanie bezpečnostných rizík	BL3
2) bezpečnostné mechanizmy a spôsoby ich implementácie	BL3
3) bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti	BL3
4) zásady personálnej bezpečnosti	BL3
5) opatrenia týkajúce sa používania, spracovania, uchovávaní a prenosu údajov	BL3
6) zásady a princípy riadenia identít a prístupov	BL3
7) kryptografické bezpečnostné mechanizmy	BL3
Výkon operatívnych bezpečnostných činností	
1) procesy riešenia kybernetických bezpečnostných incidentov	BL5
2) znalosti o štádiách kybernetického útoku (napr. Prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahladenie stôp)	BL4
3) princípy logovania a bezpečnostného monitorovania	BL3
4) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL3
5) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL5
6) zásady riadenia bezpečnosti prostredia cloudu	BL3
Riadenie súladu	
1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť	BL6
2) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na ochranu osobných údajov	BL6
3) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na prevádzku informačných a komunikačných technológií	BL6
4) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostnú politiku	BL6
5) princípy posudzovania kybernetickej bezpečnosti	BL4

	<p>6) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii BL6</p> <p>7) zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín BL5</p> <p>8) štandardy bezpečnosti platobných kariet (PCI) BL6*</p> <p>9) štandardy a procesy riadenia rizík v dodávateľskom reťazci BL5</p>
<p>Zručnosti:</p>	<p>Riadenie bezpečnosti</p> <p>a) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie</p> <p>b) vypracovanie a prezentácia bezpečnostných stratégií a konceptov</p> <p>c) implementácia procesov informačnej a kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov</p> <p>d) zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie informačnej a kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie</p> <p>e) metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie</p> <p>f) riadenie informačnej a kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri zaobstarávaní, projektovaní a vývoji softvéru a systémov</p> <p>g) správa bezpečnosti informačných aktív organizácie</p> <p>Riadenie hrozieb a rizík</p> <p>a) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí</p> <p>b) evidencia a prevencia kybernetických bezpečnostných incidentov</p> <p>Aplikácia bezpečnostných opatrení</p> <p>a) návrhy zmien a integrácie bezpečnostných technológií a riešení</p> <p>b) podpora riadenia bezpečnostnej architektúry</p> <p>c) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie</p> <p>Výkon operatívnych bezpečnostných činností</p>

	<ul style="list-style-type: none"> a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov c) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov <p>Riadenie súladu</p> <ul style="list-style-type: none"> a) pravidelné preskúvanie stavu kybernetickej a informačnej bezpečnosti b) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti c) budovanie bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov d) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní
Špecifické kľúčové kompetencie	<ul style="list-style-type: none"> a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) analytické myslenie d) prezentačná zručnosť e) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí f) schopnosť organizovania a plánovania práce g) strategické a koncepčné myslenie

Požiadavky označené * sú odvetvovo závislé. Pre príslušnú rolu sú posudzované v kontexte kompetencií, potrebných na vykonávanie určitej pracovnej činnosti v konkrétnom odvetví.