Príklad štruktúry otázok na skúšku audítora kybernetickej bezpečnosti

Okruh	Zadanie	Odpoveď 1	OK1	Odpoveď 2	OK2	Odpoveď 3	OK3	Odpoveď 4	OK4
Testovanie bezpečnosti	Nesprávne nastavenie prístupových práv je	Hrozba	Nie	Zraniteľnosť	Áno	Zostatkové riziko	Nie	Akceptovateľné riziko	Nie
Auditné postupy	Počet dní trvania auditu závisí od	Počtu pracovníkov organizácie prevádzkovateľa ZS	Nie	Počtu informačných systémov a pracovníkov zúčastňujúcich sa na ich prevádzke	Áno	Počtu používateľov informačného systému	Nie	Počtu aktív podporujúcich prevádzku informačného systému	Nie
Legislatíva a štandardy	Ktoré z nasledujúcich bezpečnostných opatrení nepatrí medzi minimálne bezpečnostné opatrenia v zmysle § 20 ods. 4 Zákona?	Detekcia kybernetických bezpečnostných incidentov.	Nie	Evidencia kybernetických bezpečnostných incidentov.	Nie	Postupy riešenia a riešenie kybernetických bezpečnostných incidentov.	Nie	Riadenie bezpečnosti sietí a informačných systémov.	Áno
Testovanie bezpečnosti	Vykonanie penetračného testu, pri ktorom organizácia poskytne vykonávateľovi testu bližšie informácie o systéme a prostredí, je akceptovateľné.	Nie, lebo organizácia sa vystavuje zbytočnému riziku.	Nie	Áno, ale len so súhlasom NBÚ.	Nie	Áno, je to štandardný proces pre "white box" test.	Áno	Áno, keďže pri zraniteľnom systéme si to hacker aj tak zistí.	Nie
Riadenie informačnej bezpečnosti	V prípade, že organizácia využíva outsourcing pre plnenie úloh informačnej bezpečnosti, čo z nasledovného by si mala ponechať?	Preukázateľnú zodpovednosť za bezpečnostnú politiku.	Áno	Vytvorenie bezpečnostnej politiky.	Nie	Implementáciu bezpečnostnej politiky.	Nie	Definíciu bezpečnostných postupov a návodov.	Nie
Riadenie hrozieb a rizík	Audítor môže pri výkone auditu bezpečnostnej politiky organizácie zaznamenať rozličné zistenia. Ktoré z nasledovného reprezentuje najvyššie potenciálne riziko?	Politika za posledný rok nebola aktualizovaná.	Nie	Politika neobsahuje históriu zmien.	Nie	Politika bola schválená administrátorom bezpečnosti.	Áno	Organizácia nemá výbor pre bezpečnostnú politiku.	Nie
Bezpečnosť prevádzky IT	Nevýhodou pri použití symetrickej šifry pri zabezpečení komunikácie je	Vysoká výpočtová náročnosť.	Nie	Nutnosť zdieľať tajný kľúč.	Áno	Nízka úroveň bezpečnosti.	Nie	Nutnosť vybudovať dôveryhodnú certifikačnú autoritu.	Nie
Riadenie kontinuity	Aká je definícia kritickej funkcie?	Business funkcia, ktorá je natoľko kritická, že nemôže byť narušená na viac ako niekoľko hodín bez vážnych obchodných dopadov.	Nie	Business funkcia alebo proces, ktorý nemôže byť nefunkčný dlhšie ako stanovenú časovú lehotu bez toho, aby to malo negatívny vplyv na organizáciu.	Áno	Funkcia alebo úloha v organizácii, ktorá je nenahraditeľná.	Nie	Funkcia alebo úloha, ktorú riadi tím krízového riadenia.	Nie
Personálna bezpečnosť	Prečo je pre vedenie organizácie dôležité, aby absolvovalo svoje vlastné školenie o bezpečnosti?	Vzdelávanie o tom, čo robia ich konkurenti.	Nie	Pomáha to posilňovať bezpečnostné iniciatívy a znalosť medzi zamestnancami.	Áno	Identifikujeme, kto môže v prípade potreby prevziať zásadnú úlohu v riadení IT.	Nie	Uistenie, že vedenie rozumie tomu, ako bezpečnostné programy fungujú.	Nie
IT architektúra	V ktorej odpovedi sa nachádzajú iba vrstvy siete podľa OSI modelu?	Aplikačná, Implementačná, Fyzická	Nie	Šifrovacia, Sieťová, Prezentačná	Nie	Relačná, Transportná, Sieťová	Áno	Fyzická, Linková, Komunikačná	Nie

Príklady otázok na skúšku audítora kybernetickej bezpečnosti

Okruh	Zadanie
Auditné postupy	Ak sú všetky nedostatky zistené auditom odstránené do dohodnutého času pred spracovaním záverečnej správy o výsledkoch auditu, audítor postupuje nasledovne
Auditné postupy	Aké sú základné metódy auditu?
Auditné postupy	Aké sú zásady auditu?
Auditné postupy	Audit kybernetickej bezpečnosti sa vykonáva
Auditné postupy	Audit vykonávaný certifikačným orgánom sa volá
Auditné postupy	Počas auditu audítor potrebuje overiť záznamy v log súbore. Aký je správny postup získania tohto súboru?
Auditné postupy	Prečo sa volá interný audit "interný" ?
Auditné postupy	V ktorej fáze auditu sa definuje cieľ auditu?
Auditné postupy	Za stanovenie a zahájenie realizácie nápravných činností, ktoré sú potrebné k odstráneniu nezhody alebo jej príčiny, je zodpovedný
Bezpečnosť OT/SCADA	Postupy riešenia kybernetickej bezpečnosti v rámci priemyselných a riadiacich systémov v porovnaní s bežnými informačnými systémami
Bezpečnosť OT/SCADA	S ohľadom na bežnú architektúru priemyselných a riadiacich systémov je najčastejšie chýbajúcim prvkom
Bezpečnosť OT/SCADA	Základný rozdiel medzi systémami pre dispečerské riadenie a zber dát (SCADA - Supervisory Control and Data Acquisition) a distribuovaným riadiacim systémom (DCS - Distributed Control System) spočíva
Bezpečnosť OT/SCADA	S ohľadom na bežnú architektúru priemyselných a riadiacich systémov je najčastejšie chýbajúcim prvkom
Bezpečnosť prevádzky IT	Ktorý z nasledujúcich protokolov používa nešifrovanú autentifikáciu?
Bezpečnosť prevádzky IT	Ktorá z nasledujúcich vrstiev modelu OSI je zodpovedná za smerovanie a posielanie sieťových paketov?
Bezpečnosť prevádzky IT	Nevýhodou pri použití symetrickej šifry pri zabezpečení komunikácie je
Bezpečnosť prevádzky IT	Ktorý z modelov NIE JE štandardným modelom pre reštrikciu systémového prístupu pre autorizovaných užívateľov?
Bezpečnosť prevádzky IT	Počas kontroly procesu zmenových požiadaviek, ktorá zo situácií je z pohľadu audítora najrizikovejšia?
Bezpečnosť prevádzky IT	Riadenie prístupov osôb k sieti a informačnému systému NEzahŕňa
Bezpečnosť prevádzky IT	Umiestnenie informačného systému verejnej správy má svoje špecifické kritériá. Ktorý z nasledujúcich priestorov je dostatočný pre adekvátne zabezpečenie IS?
Bezpečnosť prevádzky IT	Výraz "pridanie soli" alebo "salting" súvisí s
Bezpečnosť prevádzky IT	Za základné bezpečnostné zraniteľnosti pre aplikácie NEpovažujeme
Bezpečnosť prevádzky IT	Ktoré z nasledujúcich tvrdení NESPRÁVNE popisuje techniku asynchrónneho prenosu (ATM)?
Bezpečnosť prevádzky IT	Ktorú z nasledujúcich možností je potrebnú ako NAJDÔLEŽITEJŠIU vziať do úvahy pri vývoji politiky používania vlastných zariadení (BYOD)?
IT architektúra	Čo je podstatou princípu najnižších privilégií?
IT architektúra	Ktorý výraz nepatrí medzi vrstvy bezpečnostnej architektúry podľa metodiky SABSA?
IT architektúra	Siete a informačné systémy tvoriace hranicu medzi rôznymi bezpečnostnými kategóriami v bezpečnostnom systéme sa zaradia do
IT architektúra	V ktorej odpovedi sa nachádzajú iba vrstvy siete podľa OSI modelu?
Legislatíva a štandardy	Bezpečnostná dokumentácia NEobsahuje
Legislatíva a štandardy	Bezpečnostná stratégia kybernetickej bezpečnosti obsahuje
Legislatíva a štandardy	Do povinnosti prevádzkovateľa základnej služby definovaných vyhláškou NEspadá
Legislatíva a štandardy	Klasifikácia informácií a kategorizácia sietí a informačných systémov má definovanú štruktúru vo vyhláške NBÚ. Čo je potrebné ošetriť, ak má prevádzkovateľ základnej služby vlastné pravidlá klasifikácie?
Legislatíva a štandardy	Ktoré sú minimálne náležitosti žiadosti o vykonanie auditu kybernetickej bezpečnosti

Legislatíva a štandardy	Ktorý dokument NIE je povinnou súčasťou štruktúry bezpečnostných politík?
Legislatíva a štandardy	Spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií sa nazýva
Legislatíva a štandardy	Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako
Personálna bezpečnosť	Ako sa nazýva proces overenia identity?
Personálna bezpečnosť	Aký druh školení o zvyšovaní povedomia o bezpečnosti by sa mal poskytnúť všetkým zamestnancom na pracovisku? Vyberte jednu možnosť.
Personálna bezpečnosť	Keď sa zamestnanec presúva v rámci organizácie, aké je vaše odporúčanie pre zachádzanie s jeho prístupmi?
Personálna bezpečnosť	Ktorá z nasledujúcich možností NIE je všeobecne uznávanou výhodou informovanosti o bezpečnosti, odbornej prípravy a vzdelávania?
Personálna bezpečnosť	Zamestnanci banky, ktorí prichádzajú do styku s citlivými údajmi klientov by mali absolvovať školenie v oblasti informačnej bezpečnosti
Riadenie dodávateľov	Dodávateľ má skúsenosti s podporou účtovných systémov. Ktoré z nasledujúcich tvrdení je správne?
Riadenie dodávateľov	Monitorovanie dodávateľských služieb a dodržiavanie bezpečnostných štandardov dodávateľa je potrebné vykonávať za ktorej z nansledujúcich okolností?
Riadenie dodávateľov	Manažér informačnej bezpečnosti pomáha pri vývoji žiadosti o cenovú ponuku budúcej externe zabezpečovanej služby. Manažér bezpečnosti by sa mal PRIMÁRNE zamerať na definovanie
Riadenie dodávateľov	Organizácia rieši formou outsourcingu činnosti týkajúce sa vývoja aplikácií. Ktoré z nasledujúcich možností poskytuje NAJLEPŠIE uistenie, že zmluvní programátori tretích strán dodržiavajú bezpečnostné zásady organizácie?
Riadenie dodávateľov	V rámci obstarávania a implementácie informačných technológií verejnej správy má byť zmluvne zakotvené, že
Riadenie hrozieb a rizík	Aké sú tri fázy cyklu riadenia rizika?
Riadenie hrozieb a rizík	Čo znamená výraz akceptovateľné riziko?
Riadenie hrozieb a rizík	Spoločnosť má nasadených viacero typov koncových staníc - 40% LINUX, 30% WINDOWS and 30% MAC OS X. Ktorá z nasledujúcich situácií je z pohľadu audítora najrizikovejšia?
Riadenie hrozieb a rizík	Za základné bezpečnostné zraniteľnosti pre aplikácie NIE SÚ považované
Riadenie hrozieb a rizík	Matica na hodnotenie rizika neobsahuje (vyberte jednu možnosť)
Riadenie hrozieb a rizík	Neodstránenie prístupových práv pri ukončení pracovného pomeru je zraniteľnosť, ktorá by mohla byť využitá na (vyberte najpravdepodobnejšiu)
Riadenie hrozieb a rizík	Riadenie aktív NEpozostáva z identifikácie a evidencie
Riadenie hrozieb a rizík	Zavedenie systému školení a vzdelávania je technikou/ stratégiou, ktorou sa
Riadenie hrozieb a rizík	Zorganizujte správne kroky, tak ako idú po sebe, pri hodnotení a riadení rizík.
Riadenie hrozieb a rizík	Zvyšková úroveň rizika je
Riadenie informačnej bezpečnosti	Aká je hlavná úloha bezpečnostného manažéra v organizácií?
Riadenie informačnej bezpečnosti	Aká je úloha administrátora v procese prideľovania prístupových práv?
Riadenie informačnej bezpečnosti	Aké sú typické bezpečnostné mechanizmy?
Riadenie informačnej bezpečnosti	Do ktorej oblasti dokumentácie patrí dokument s názvom Smernica o klasifikácii informácií?
Riadenie informačnej bezpečnosti	Ktorá úroveň bezpečnostnej dokumentácie obsahuje merateľné ukazovatele pre jednotlivé bezpečnostné opatrenia?
Riadenie informačnej bezpečnosti	Pokiaľ je identifikácia a autentifikácia založená na niečom čím človek "je"- fyziologické atribúty alebo behaviorálne atribúty, hovoríme že sa využívajú
Riadenie informačnej bezpečnosti	Politika informačnej bezpečnosti by mala byť
Riadenie informačnej bezpečnosti	Pri odchode zamestnanca z organizácie je účet do informačných systémov zablokovaný
Riadenie informačnej bezpečnosti	Stanovenie, čo je používateľ oprávnený vykonať alebo aké má prístupové oprávnenia nazývame
Riadenie informačnej bezpečnosti	Ktorá z nasledujúcich dynamických interakcií podnikového modelu informačnej bezpečnosti (BMIS) je vzorcom správania, účinkov, predpokladov, postojov a spôsobov práce?
Riadenie informačnej bezpečnosti	Nadnárodná organizácia zavádza rámec riadenia bezpečnosti. Manažér informačnej bezpečnosti sa obáva, že postupy regionálnej bezpečnosti sa líšia. Ktorá z nasledujúcich možností by sa mala vyhodnotiť ako PRVÁ?
Riadenie informačnej bezpečnosti	Ktorá z nasledujúcich možností je najdôležitejším faktorom pri vývoji politiky a postupov v oblasti informačnej bezpečnosti (pre organizáciu)?
Riadenie IT služieb	Aplikačné zmeny pred nasadením do produkčného prostredia
Riadenie IT služieb	Ktorý z modelov nie je štandardným modelom pre reštrikciu systémového prístupu pre autorizovaných užívateľov?
Riadenie IT služieb	Testovacie prostredie by malo obsahovať

Riadenie kontinuity	Ako by sa mali riadiť náklady spojené s plánom kontinuity činnosti?
Riadenie kontinuity	Cieľový bod obnovy (RPO – Recovery Point Objective) vyjadruje
Riadenie kontinuity	Čo je najdôležitejšia časť procesu riadenia kontinuity podnikania?
Riadenie kontinuity	Kedy je kríza zvyčajne vyhlásená za „skončenú“?
Riadenie kontinuity	Kto stanovuje požiadavky na RTO, RPO kritických systémov organizácie?
Riadenie kontinuity	Pán Novák má Recovery Point Objective (RPO) nastavený na 24 hodín. Čo to znamená?
Riadenie kontinuity	Plán kontinuity činnosti (BCP) by mal obsahovať
Riešenie incidentov	Aký je vzťah medzi pojmami kybernetická bezpečnostná udalosť a kybernetický bezpečnostný incident?
Riešenie incidentov	Dopad kybernetického závažného incidentu sa vyhodnocuje na základe
Riešenie incidentov	Ktorá z nasledujúcich činností nie je hlavnou činnosťou vo fáze plánovania a prípravy riadenia bezpečnostných incidentov?
Riešenie incidentov	Kybernetický bezpečnostný incident pri ktorom došlo k prezradeniu osobných údajov cca 200 000 osôb je
Riešenie incidentov	Riešenie kybernetických bezpečnostných incidentov je povinné pre nasledujúcu kategóriu sietí a informačných systémov
Riešenie incidentov	Aký je vzťah medzi pojmami bezpečnostná udalosť a kybernetický bezpečnostný incident?
Strategický manažment	Účastník IT projektu požaduje vykonať zmenu, ktorá by mohla ovplyvniť rozsah a harmonogram projektu. Ktorá z nasledujúcich možností by bola pre projektového manažéra najvhodnejšia v súvislosti so žiadosťou o zmenu?
Strategický manažment	V rámci obstarávania a implementácie informačných technológií verejnej správy má byť zmluvne zakotvené, že
Strategický manažment	Za Bezpečnostnú politiku prevádzkovateľa základnej služby je zodpovedný
Strategický manažment	Čo z uvedeného nepatrí medzi základné atribúty procesu?
Strategický manažment	Ktorá z definícií najlepšie vyjadruje požiadavku na rozsah manažérskych právomocí?

Okruhy skúšobných otázok na skúšku audítora kybernetickej bezpečnosti

a) Auditné postupy
b) Riadenie informačnej bezpečnosti
c) Riadenie IT služieb
d) IT architektúra
e) Riadenie hrozieb a rizík
f) Vývoj systémov (SDLC)
g) Riadenie dodávateľov
h) Bezpečnosť prevádzky IT
i) Riešenie incidentov
j) Bezpečnosť OT/SCADA
k) Personálna bezpečnosť
l) Riadenie kontinuity
m) Strategický manažment
n) Legislatíva a štandardy