Príklad štruktúry a otázok na skúšku manažéra kybernetickej bezpečnosti

Oblasti otázok	Otázka	Odpoveď 1	OK 1?	Odpoveď 2	OK 2?	Odpoveď 3	OK 3?	Odpoveď 4	OK 4?
a) Riadenie kybernetickej a informačnej bezpečnosti	V prípade, že organizácia využíva outsourcing pre plnenie úloh informačnej bezpečnosti, čo z nasledovného by si mala ponechať?	Vytvorenie bezpečnostnej politiky.	Nie	Preukázateľnú zodpovednosť za bezpečnostnú politiku.	Áno	Implementáciu bezpečnostnej politiky.	Nie	Definiciu bezpečnostných postupov a návodov.	Nie
b) Riadenie IT služieb	Testovacie prostredie by nemalo obsahovať	Reálne dáta z produkčného prostredia, ktoré obsahujú aj citlivé a osobné údaje.	Áno	Náhodne vygenerované dáta.	Nie	Reálne dáta z produkčného prostredia.	Nie	Dáta, ktoré sú overené a použité pri predchádzajúcom testovaní.	Nie
c) Riadenie prístupov	Nesprávne nastavenie prístupových práv je	Hrozba	Nie	Zostatkové riziko	Nie	Zraniteľnosť	Áno	Akceptovateľné riziko	Nie
d) IT architektúra	V ktorej odpovedi sa nachádzajú iba vrstvy siete podľa OSI modelu?	Aplikačná, Implementačná, Fyzická	Nie	Šifrovacia, Sieťová, Prezentačná	Nie	Fyzická, Linková, Komunikačná	Nie	Relačná, Transportná, Sieťová	Áno
e) Riadenie aktív, hrozieb a rizík	Novo menovaný manažér informačnej bezpečnosti si urobil mimo iné aj kontrolu dokumentácie v oblasti Bezpečnostnej politiky. Ktoré z nasledovných zistení môže reprezentovať najvyššie potenciálne riziko?	Politika bola schválená administrátorom bezpečnosti.	Áno	Politika neobsahuje históriu zmien.	Nie	Politika za posledný rok nebola aktualizovaná.	Nie	Organizácia nemá výbor pre bezpečnostnú politiku.	Nie
f) Akvizícia, vývoj, implementácia a údržba systémov (SDLC)	V rámci nastavenia procesu zmenových požiadaviek, ktorá zo situácií je z pohľadu manažéra informačnej bezpečnosti najmenej riziková?	Aktuálny proces implementácie zmenových požiadaviek sa neuplatňuje vo vývojovom prostredí.	Nie	Retrospektívne typy zmien sú nasadzované do produkčného prostredia bez predchádzajúcej kontroly alebo schvaľovania.	Nie	Kvôli obmedzeným ľudským zdrojom sú štandardné zmeny implementované bez nezávislého overenia a sú nasadzované do produkčného prostredia bez ďalšieho schválenia.	Nie	Proces implementácie zmenových požiadaviek bol len nedávno aktualizovaný (pred jedným mesiacom).	Áno
g) Riadenie tretích strán a dodávateľských služieb	Vyberte optimálny prístup pre monitorovanie dodávateľských služieb a dodržiavanie bezpečnostných štandardov:	Vykonáva sa príležitostne. A intenzívne len keď dôjde k bezpečnostnému incidentu zo strany dodávateľa.	Nie	Nie je potrebné vykonávať, pokiaľ nie je stanovené zmluvne.	Nie	Pravidelne sa monitoruje, vyhodnocuje a dokumentuje v mesačných reportoch.	Áno	Pravidelne sa monitoruje, vyhodnocuje. Nie je potreba dokumentovať, pokiaľ nie je identifikovaný zásadný problém.	Nie
h) Bezpečnosť prevádzky IT	Vykonanie penetračného testu, pri ktorom organizácia poskytne vykonávateľovi testu bližšie informácie o systéme a prostredí, je akceptovateľné.	Áno, je to štandardný proces pre "white box" test.	Áno	Áno, ale len so súhlasom NBÚ.	Nie	Nie, lebo organizácia sa vystavuje zbytočnému riziku.	Nie	Áno, keďže pri zraniteľnom systéme si to hacker aj tak zistí.	Nie
i) Bezpečnosť počítačových sietí	Nevýhodou pri použití symetrickej šifry pri zabezpečení komunikácie je	Vysoká výpočtová náročnosť.	Nie	Nutnosť vybudovať dôveryhodnú certifikačnú autoritu.	Nie	Nízka úroveň bezpečnosti.	Nie	Nutnosť zdieľať tajný kľúč.	Áno
j) Riešenie incidentov	Ktorá z nasledujúcich činností JE väčšinou riešená ako prvá vo fáze plánovania a prípravy riadenia bezpečnostných incidentov?	Identifikujte rozsah, ciele a priority.	Áno	Definujte úlohy a zodpovednosti všetkých zúčastnených strán.	Nie	Aktualizujte bezpečnostné politiky.	Nie	Školenie a vzdelávanie zamestnancov o konceptoch, postupoch a technických zručnostiach.	Nie
k) Manažment bezpečnostných zraniteľností	Za základné bezpečnostné zraniteľnosti pre aplikácie považujeme	Bezpečnostné chyby v softvéri a/alebo v kóde aplikácie. Používateľské chyby pri prevádzke aplikácie.	Nie	Bezpečnostné chyby v softvéri a/alebo v kóde aplikácie. Chyby v konfiguračných nastaveniach.	Áno	Chyby v konfiguračných nastaveniach (v aplikácii, v systéme na ktorom je databáza, alebo iné). Zastaraný kód z pohľadu inovácii v rámci vývoja aplikácií.	Nie	Nedostatočné bezpečnostné praktiky pri prevádzke aplikácií. Zastaraný kód z pohľadu inovácii v rámci vývoja aplikácií.	Nie
l) Základy bezpečnosti OT/ICS	Čo by bolo pre manažéra kybernetickej bezpečnosti najväčším problémom v ramci architektúry priemyselných a riadiacich systémov?	Chýbajúce určenie zodpovednosti za priemyselne a riadiace systémy na úrovni najvyššieho vedenia.	Nie	Nedostatočné náhradné a záložné systémy v ramci architektúry priemyselných a riadiacich systémov.	Nie	Neexistencia testovacieho prostredia pre priemyselne systemy.	Nie	Nedostatočné oddelenie priemyselných a riadiacich systémov a IT casti siete.	Áno
m) Personálna bezpečnosť	Prečo je pre vedenie organizácie dôležité, aby absolvovalo svoje vlastné školenie o bezpečnosti?	Pomáha to posilňovať bezpečnostné iniciatívy a znalosť medzi zamestnancami.	Áno	Identifikujeme, kto môže v prípade potreby prevziať zásadnú úlohu v riadení IT.	Nie	Vzdelávanie o tom, čo robia ich konkurenti.	Nie	Uistenie, že vedenie rozumie tomu, ako bezpečnostné programy fungujú.	Nie
n) Riadenie kontinuity	Aká je definícia kritickej funkcie?	Biznis funkcia, ktorá je natoľko kritická, že nemôže byť narušená na viac ako niekoľko hodín bez vážnych obchodných dopadov.	Nie	Funkcia alebo úloha v organizácii, ktorá je nenahraditeľná.	Nie	Biznis 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, ktorú riadi tím krízového riadenia.	Nie
o) Strategický manažment	Ktorú z nasledujúcich možností je možno považovať za NAJMENEJ dôležitu pri vývoji politiky používania vlastných zariadení (BYOD) z hľadiska kybernetickej bezpečnosti?	Používateľská privetivost	Áno	Postup pre prístup k sieti	Nie	Postupy diaľkového vymazania	Nie	Obmedzenia sťahovania aplikácií	Nie
p) Legislatíva a štandardy	Ktoré z nasledujúcich bezpečnostných opatrení nepatrí medzi minimálne bezpečnostné opatrenia v zmysle § 20 ods. 4 Zákona?	Detekcia kybernetických bezpečnostných incidentov.	Nie	Riadenie bezpečnosti sietí a informačných systémov.	Áno	Postupy riešenia a riešenie kybernetických bezpečnostných incidentov.	Nie	Evidencia kybernetických bezpečnostných incidentov.	Nie