Információbiztonsági szakmérnök/szakember szakirányú továbbképzés

Az információbiztonság kiépítése
Témakörök záróvizsgára történő felkészüléshez

1. Mutassa be az információbiztonság irányelveit
    a. A bizalmasság elve
    b. A sérthetetlenség elve
    c. A rendelkezésre állás elve
    d. A hitelesség
    e. A szükséges ismeret elve
    f. A szükségesség és arányosság elve
2. Mutassa be a minősített adat kezeléséhez tárolásához szükséges fizikai biztonsági követelményeket, feltételeket, illetve a szükséges elektronikus információbiztonsági követelményeket.
3. Mutassa be a minősített adat kezeléséhez tárolásához szükséges személyi- és adminisztratív biztonsági követelményeket, feltételeket.
4. Mutassa be az információbiztonság menedzselésével kapcsolatos feladatokat.
5. Mutassa be az MSZ ISO/IEC 27001:2014/2023 szabványhoz kapcsolódóan az IBIR kiépítésének menetét.
6. Mutassa be egy Információbiztonsági Szabályzat felépítését, főbb pontjait.
7. Mi a COBIT és mire használható az információbiztonság kialakítása, menedzselése során?
8. Mutassa be a COBIT "kockát", illetve sorolja fel az egyes dimenziók elemeit.
9. Sorolja fel és mutassa be röviden a COBIT 5 Menedzsment folyamatait!

10. Mutassa be a COBIT folyamatképesség modelljét!
11. Sorolja fel és ismertesse röviden a COBIT alapelveket!
12. Hogyan kapcsolódik a COBIT az ISO 27001-hez, illetve a teljes 27000-es szabványcsaládhoz?
13. Mutassa be az informatikai biztonság szabályozásának módjait (logikai, fizikai).
14. Mi a vagyonleltár és mi a jelentősége a szervezet életében?
15. Mi a kockázatmenedzsment jelentősége a szervezetnél, milyen kockázati technikákat/módokat ismer?

IT rendszerek üzemeltetésének logikai, fizikai biztonsági követelményei

Témakörök záróvizsgára történő felkészüléshez

1. Magyarázza el az OSI modell és a TCP IP modell közötti különbségeket. Ismertesse az ARP-t. Sorolja fel milyen IP cím osztályokat ismer, térjen ki a privát és publikus címekre.
2. Microsoft Windows üzemeltetési környezetben melyek a védett módban futó komponensek? A Windows hálózati modellje melyik két csoportba sorolja a számítógépeket?
3. Szűrési módszerük alapján, hogyan csoportosítjuk a tűzfalakat? Mondjon pár példát a host alapú tűzfalakra? Mit jelent az SNMP?
4. Mit jelent a Malware kifejezés? Mi a különbség a Vírus és a Worm között? Melyek a Worm komponensei?
5. Magyarázza meg mi a Ransomware lényege! Melyek a hozzáférési támadások típusai?
6. Mit jelent a Social Engieering, milyen fajtái vannak? Magyarázza meg mi a DOS és a DDOS közötti különbség!
7. Milyen két elv alapján működnek a vírusírtók? Mit értünk karantén alatt?
8. Milyen mentéseket végezhetünk el Microsoft környezetben Windows Server Backup segítségével? Mely elemeket tartalmazza a rendszerállapot mentése? Részletezze az eseménynaplók 3 fajtáját!
9. Microsoft Windows környezetben melyek a hozzáférés-vezérlést segítő Active Directory szolgáltatásai? A hozzáférési engedélyek hozzáférés vezérlési listában mely elemek szerepelnek? Ismertesse az alapvető Fájl és mappa engedélyeket!
10. Melyek az incidensmenedzsment-folyamat lépései?

11. Mik az OT hálózatok jellemzői és mi a különbség az IT hálózatokhoz képest?
12. Mik lehetnek az adatközponti szolgáltatások?
13. Soroljon fel üzemeltetéssel kapcsolatos ajánlásokat, szabályozásokat, minősítéseket!
14. Mik lehetnek az adatközpontok funkcionális felépítése?
15. Milyen típusú sérülékenységvizsgálatokat ismer? Mit értünk az egyes vizsgálatok alatt?
16. Mit tud a fejlesztői környezetekről?
17. Milyen felhasználói hozzáférés típusokat ismer?

IBIR auditálása

Témakörök záróvizsgára történő felkészüléshez

1. Ismertesse az IBIR dokumentumainak hierarchiáját. Térjen ki a dokumentumok elfogadásának, felülvizsgálatának, nyilvánosságra hozatalának gyakorlatára.
2. Ismertessen néhány, információbiztonsági irányítási rendszer kidolgozását támogató nemzetközi szabványt, keretrendszereket, szektor specifikusan!
3. Milyen szabályozásokat ismer Magyarországon az információbiztonsági rendszerek adekvát működtetésének szempontjából?
4. Milyen folyamatokra épül az IBIR auditálása? Térjen ki az audit-riport és a vezetői összefoglaló közti különbségek ismertetésére!
5. Csoportosítsa auditálható és nem auditálható kategóriába az ismert IT auditot / IBIR –t támogató szabványokat, keretrendszereket! Részletesen ismertessen egy tetszőlegesen választottat!
6. Ismertessen néhány ITIL folyamatot, amelyek az ISO 20000 (akár ISO 27001-ben) is implementálásra kerültek!
7. Ismertesse az ISO 2700x szabványcsalád néhány, IBIR szempontjából releváns tagját. (pl. kontrollkövetelmények: ISO 27001, kockázatmenedzsment: ISO27005, audit-kézikönyv ISO 27007, hálózat biztonság: ISO 27033)
8. Ismertesse az (IT) auditok tipikus felépítését! Térjen ki a belső / külső ellenőrzések (auditok) közti hasonlóságokra, különbségekre, illetve az auditbizottság ajánlott összetételére, auditor - elvárásokra, magatartásformákra!
9. Hogyan lehet csoportosítani (akár ISO 27005 szabvány alapján) szerint a különböző fenyegetettségeket? Egy-két példán keresztül szemléltesse, hogy a fenyegetettségek lehetséges okozóinak különböző motivációja révén milyen lehetséges negatív hatásokkal (hardver, szoftver, telephely, szervezett vonatkozásában) lehet számolni a kockázatkezelés során?

10. Az IBIR működtetése szempontjából kiemelt szerepe van a belső információbiztonsági szervezetnek. Ismertessen néhány alapelvet a különböző információbiztonsági szerepek és felelősségek kialakítására, szerepkörök szétválasztásának gyakorlatára. Térjen ki a hatóságokkal, szakmai csoportokkal való kapcsolattartás fontosságára is!
11. A felhasználói felelősségek kiemelt szerepet kapnak az IBIR működtetése szempontjából úgy a saját hitelesítési információk védelme, mint a tiszta asztal, tiszta képernyő elvek betartása, vagy az interneten való tudatos viselkedés terén. Milyen előfeltételei vannak a felhasználói felelősségek megfelelő kialakításának és fenntartásának? Milyen témákat tartana hasznosnak a tudatosítási tréningek során?
12. Az üzemelés biztonsága olyan különböző üzemeltetési eljárásokra és felelősségekre épül, mint pl.: változásfelügyelet, kapacitáskezelés, mentés, rosszindulatú szoftverek elleni védelem. Ismertessen néhány információbiztonsági kontrollt, gyakorlati implementációs eljárást az említett témakörökből!
13. Ismertessen néhány eljárást, kontrollt, best practice-t, amelyek az információbiztonsági incidensek megelőzését, kezelését szolgálják!