Óbudai Egyetem Neumann János Informatikai Kar			Alkalmazott Informatikai Intézet	
Tantárgy neve és kódja: *Intézményi informatikai biztonság NIEIB1FBNE* **Kreditérték*: 6*** *Mérnök Informatikus BSc szak* *Nappali tagozat 2016/17 tanév I. félév*				
Tantárgy oktató(i): Dr. Szenes Katalin				
Előtanulmányi feltételek: (kóddal)	Bevezetés az informatikai ellenőrzésbe I., Számítógép hálózatok biztonsági technológiái			
Heti óraszámok:	Előadás: 2	Tantermi gyak.: 0	Laborgyakorlat: 3	Konzultáció: 0
Számonkérés módja:	Vizsga			

A tananyag

Oktatási cél: A hallgatók eddigi szakirányi informatikai biztonsági és ellenőrzési oktatási eredményeit felhasználva BSc szinten olyan elméleti és gyakorlati alapot adni, amellyel akár az állami, akár a piaci intézményekben képesek lesznek mind junior szintű informatikai biztonsági / ellenőrzési feladatok önálló ellátására, mind a biztonsági, ellenőri szakértők informatikai oldali támogatására. Bemutatjuk, hogyan kell felépíteni, átépíteni, továbbfejleszteni egy vállalat informatikai infrastruktúráját úgy, hogy a vállalat informatikai rendszere, a menedzsment útmutatásai szerinti mértékben, eleget tegyen úgy az olyan, legjobb szakmai gyakorlatnak számító követelményeknek, mint pl. az Informatikai Auditorok és Ellenőrök Nemzetközi Szövetsége (ISACA, Information Systems Audit and Control Association) módszertani anyagai, az ISO/IEC szabványai (különös tekintettel a 27001-es és 27002-es szabványokra), a PCI DSS előírások (Payment Card Industry Data Security Standard), mint Magyarország, és az Európai Únió vonatkozó előírásainak. A gyakorlatokon az informatikai infrastruktúra biztonsági rendszereinek ismeretére és az intézményi informatikai biztonság tervezésének módszereire építve a hallgatók kis munkacsoportokban gyakorlati feladatot oldanak meg és dokumentálnak. Először egy intézményi biztonsági rendszer részletes tervezését és kivitelezését ismerik meg esettanulmány bemutatásával, majd különböző biztonsági elvárásoknak megfelelő biztonsági rendszert terveznek, kiviteleznek, ellenőriznek, és üzemeltetésükhöz utasítást készítenek.

Tematika: A fenti legjobb szakmai gyakorlati, illetve törvényi előírásokban szereplő alapelvek rendszerezése az intézményi kiválóság alappillérei, a szervezet, a szabályozás, és a technika, valamint működés kiválósági kritériumok segítségével. A hazai és EU-s törvényi követelmények, a különféle iparági szabályozások, és az egyéb szabványok, ajánlások és legjobb gyakorlatok. Az alkalmazásfejlesztéssel kapcsolatos biztonsági követelmények az életciklusuk egyes szakaszaiban. A felhő alapú információfeldolgozás problémái. A kiszervezés informatikai biztonsági és ellenőrzési kérdései. A vállalati információs rendszer mai infrastruktúrája biztonsági és ellenőrzési szemszögből, az információs rendszer auditálás szervezeti és irányítási szempontjai. A vállalati vagyon (információ és információs rendszer) védelmi és ellenőrzési vonatkozásai. Esettanulmány bemutatása, elemzése biztonsági szempontból. Vállalati informatikai rendszerek biztonságának tervezése, eszközök konfigurálása, tesztelése. Hálózati topológia kialakítása, aktív elemek kiválasztása, biztonsági feladataik meghatározása, konfigurálása. Hálózati behatolás védelmi, sérülékenységet vizsgáló eszközök, tűzfalak topológiába illesztése, konfigurálása. A szerver és ügyfél operációs rendszerek biztonsági rendszerének installálása és konfigurálása. Dokumentálás, és üzemeltetési terv készítése.

Féléves ütemezés:	
Oktatási hét (konzultáció)	Témakör

1.	EA: A hazai és EU-s törvényi követelmények, a különféle iparági szabályozások, és az egyéb szabványok, ajánlások és legjobb gyakorlatok. LAB: Cisco Site-to-Site VPN - Ipsec.
2.	EA: A féléves feladatok megbeszélése: Az informatikai ellenőrzés tantárgyban elkészített informatikai biztonsági szabályzat továbbfejlesztésének előkészítése az- ISO/IEC 27002 szabvány segítségével. Informatikai audit terv készítése. LAB: Ethernet kapcsolás biztonsága.
3.	EA: Az alkalmazói rendszerekkel kapcsolatos biztonsági követelmények az életciklusuk egyes szakaszaiban. LAB: Hálózati tárolás biztonsága.
4.	EA: Új intézményi adatfeldolgozási lehetőségek és problémáik. LAB: Esettanulmány konfigurálása.
5	EA: Új európai úniós direktívák, rendeletek és következményeik. LAB: Behatolás- és vírusvédelem.
6.	EA: A kiszervezés informatikai biztonsági problémái. LAB: Esettanulmány konfigurálása.
7.	EA: A kiszervezés informatikai biztonsági problémái (folyt.). LAB: Adatvédelem, adatmentés.
8.	EA: A kiszervezés informatikai biztonsági problémái (folyt.). LAB: Esettanulmány konfigurálása.
9.	EA: A kiszervezés informatikai biztonsági problémái (folyt.) LAB: Esettanulmány konfigurálása.
10.	EA: A kiszervezés informatikai biztonsági problémái (folyt.) LAB: Esettanulmány konfigurálása.
11.	EA: Az IBSZ féléves feladat értékelése. Lab: Esettanulmány konfigurálása.
12.	EA: Az audit terv féléves feladat értékelése. Lab: Esettanulmány konfigurálása.
13.	EA: Zárthelyi. LAB: Esettanulmány konfigurálása.
14.	EA: A féléves munka és a zárthelyi értékelése. LAB: Féléves feladat bemutatása, beadása, értékelése.

Félévközi követelmények
Félévközi zárthelyi sikeres megírása, a tervezési és kivitelezési feladatok elvégzése, bemutatása.

Zárthelyi dolgozatok	
Oktatási hét (konzultáció)	Témakör
12	Zárthelyi (előadások anyagából) HA EZ AZ ENYÉM, nyugodtan húzd ki, úgyse értem
14	Féléves feladat HA EZ AZ ENYÉM, nyugodtan húzd ki, úgyse értem
1	Szöveg beírásához kattintson ide.

A *félévzáró érdemjegy* (é) kialakításának módszere
Szöveg beírásához kattintson ide.

2022. 03. 28.

Pótlás módja
Ha a tervezési és kivitelezési feladatot a hallgató nem tudja beadni az utolsó oktatási héten, vagy elégtelen osztályzatot kap rá vagy az elméleti ZH-ra, az aláírás a vizsgaidőszak első 10 munkanapjának egyikén, előre megadott időpontban megszerezhető.
Vizsga módja
Szóbeli vizsga
Vizsgajegy kialakítása
Az elméleti ZH és a szóbeli felelt eredményének átlaga.
Irodalom
Kötelező:
Az előadás prezentációk http://www.isaca.org Reusz, Holtz, Szenes: Adatfeldolgozási és biztonsági események naplózása, Verlag Dashöfer kiadó, Budapest, 2009. szeptembertől, 4.3.1. old. - 4.3.4.4. old. - 32 oldal Szenes, K: A COBIT 4.0 és 4.1 újdonságai, Az Informatikai biztonság kézikönyve, 27. aktualizálás, Verlag Dashöfer kiadó, Budapest, 2007. novembertől, 7.3 1. old. - 7-3 64. old. - 54 oldal Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására, Minőség és Megbízhatóság; nemzeti minőségpolitikai szakfolyóirat, kiadja: az European Organization for Quality (EOQ) Magyar Nemzeti Bizottsága, XLVI. évf. 2012. / 5. sz., 252-257. old.
Ajánlott:
Szenes, K.: Az informatikai erőforrás-kihelyezés auditálási szempontjai, Az Informatikai biztonság kézikönyve, I. rész: 36. aktualizálás, 2010. február, 8.10. 1. old. – 26. old. (26 oldal), II. rész: 39. aktualizálás, 2010. december 8.10. 27. old. – 158. old. (132 oldal) (összesen 158 oldal), Verlag Dashöfer kiadó, Budapest, http://www.isc2.org http://www.sans.org L. McCarthy: IT Security. Risking the Corporation Prentice Hall PTR, NJ, USA, 2002. Vasvári Gy.: Bankbiztonság BME GTK ITT, Budapest, 2003. CISA Review Techical Information Manual, ISACA Information Systems Audit and Control Association, Inc., Rolling Meadows, Illinois, USA, 2010. QAT közreműködő évente a készítésben: Szenes Katalin http://www.securityfocus.com http://www.cisco.com http://www.symantec.com http://www.microsoft.com
Egyéb segédletek:
A Moodle rendszerben megtalálható anyagok (Prezentációk, feladat leírás, egyéb segédletek)