DOKUMENT:	**PRIMER TEST FIZIČNE VARNOSTI OSNUTEK**
Ime revidiranca:	
Ime revizije:	Revizija delovanja informacijskih sistemov po okviru COBIT 4.1[1]
Namen dokumenta:	Dokumentirati ugotovitve pregleda fizične varnosti v organizaciji ABC[2]
Cilj testa:	Pregledati kako kakovostni so mehanizmi organizacije za fizično omejevanje dostopa ter za zaščito pred okoljskimi škodami
Povezave na COBIT procese[3]:	**DS12 Upravljajte fizično okolje** **DS12.1 Izbor prostora in načrt** Opredelite in izberite prostore za opremo IT, ki bodo podpirali tehnološko strategijo, povezano s poslovno strategijo. Pri izboru in pripravi načrta prostora je treba upoštevati tveganje, ki je povezano z naravnimi nesrečami in z nesrečami, ki jih povzroči človek, ter pri tem upoštevati relevantne zakone in predpise, kot so predpisi o zdravju in varnosti na delovnem mestu. **DS12.2 Ukrepi za fizično varnost**

[1] Kljub temu, da je že izdana različica 5 okvira COBIT, se v standardni revizijski mapi zanašamo na v slovenščino prevedeno različico COBIT 4.1. Okvir COBIT 4.1 (Kontrolni cilji za informacijsko in sorodno tehnologijo) pripravlja Inštitut za upravljanje IT (angl. IT Governance Institut ITGI™), ki pripravlja standarde v zvezi z usmerjanjem in nadzorom informacijske tehnologije v podjetjih (različico 5 pripravlja ISACA). Okvir opisuje dobre prakse celotne domene IT in procesnega okvira ter predstavlja aktivnosti na področju IT na obvladljiv in logičen način. COBIT-ove dobre prakse so usmerjene bolj na kontrolo in manj na izvajanje. Namenjene so pomoči pri optimiziranju investicij s komponento IT, pri zagotavljanju storitev IT ter pri presojanju v primerih, ko gredo stvari narobe. Kot okvir dobrih praks izvajanja domene IT jih lahko uporabljamo tudi kot vodilo priporočenega stanja procesov in kontrol na tem področju, pri čemer pa je treba upoštevati uporabnost posameznih dobrih praks v dejanskih organizacijah. Slovenski prevod COBIT 4.1 je na voljo na spletni strani http://www.isaca.si/. Gradivo je avtorsko zaščiteno ter je v pričujoče materiale vključeno izključno v izobraževalne namene.

[2] Delovni zapis je pripravljen ob predpostavki, da organizacija naroča revizijo učinkovitosti delovanja informacijskega sistema ABC po okviru COBIT 4.1. Primer je izbran ker gre za pogost tip pregleda. Dokument mora biti prilagojena zahtevam konkretne revizijske naloge.

[3] Našteti procesi COBIT predstavljajo zgolj predlog. Dejanska povezava s COBIT procesi mora biti posebej prilagojena za vsak posamezen test ter povezana s točnimi cilji testa, vsebino revizijske naloge in informacijskim okolje revidiranca.

	Da zavarujete lokacijo in fizična sredstva, opredelite in vpeljite ukrepe za zagotavljanje fizične varnosti v skladu s poslovnimi zahtevami. Ukrepi za fizično varnost morajo biti sposobni uspešnega preprečevanja, odkrivanja in blaženja tveganj, ki se nanašajo na krajo, temperaturo, požar, dim, vodo, vibracije, teror, vandalizem, izpade energije, kemikalije ali eksplozive. **DS12.3 Fizični dostop** Opredelite in vpeljite postopke za odobritev, omejevanje in preklic dostopa do prostorov, zgradb in območij v skladu s poslovnimi potrebami vključno v primeru sile. Dostop do prostorov, zgradb in območij mora biti upravičen, odobren in zabeležen ter ga je treba spremljati. To mora veljati za vse osebe, ki vstopajo v prostore, vključno z osebjem, začasnimi uslužbenci, strankami, prodajalci, obiskovalci in tretjimi strankami. **DS12.4 Zaščita pred okoljskimi dejavniki** Oblikujte in vpeljite ukrepe za zaščito pred okoljskimi dejavniki. Namestite specializirano opremo in naprave za spremljanje in nadzor okolja. **DS12.5 Upravljanje fizičnih zmogljivosti** Upravljajte zmogljivosti vključno z električno in komunikacijsko opremo v skladu z zakoni in predpisi, tehničnimi in poslovnimi zahtevami, specifikacijami prodajalca ter smernicami glede varovanja zdravja in varnosti.
Opis področja:	Osnovne informacije o tem področju upravljanja IS naj bi se pridobilo že v okviru spoznavanja informacijskega okolja organizacije (glej mapo **1040 Spoznavanje okolja organizacije**) - tu je smiselno informacije ali referencirati ali ponoviti.
Izvedeni postopki:	Opis postopkov za pridobitev revizijskega zagotovila (vključno z navedbo prič, navedbo pregledanih dokumentov, datuma izvedenega postopka in vseh drugih identifikacijskih znakov, ki bi neodvisnemu revizorju omogočali, da postopke ponovi sam)
Ugotovitve:	
Podporna	

dokumentacija:	
Avtor:	Maja Hmelak, Uroš Žust

VERZIJA	DATUM	OSEBA	OPIS
1.0	16.9.2013	MH, UŽ	Prva pripravljena verzija
1.1	21.10.2013	MH, UŽ	Uskladitev dokumentov na nivoju celotne mape
1.2	4.11.2013	MH, UŽ	Izboljšanje skladno s prvimi povratnimi komentarji

Vzorčni primeri testov[4] upravljanja fizične varnosti:

- Pregledamo politike in postopke, povezane s fizično varnostjo v organizaciji.
- Podrobno pregledamo varnostne incidente, povezanih s fizično varnostjo v revidiranem obdobju.
- Pregledamo način varovanja komunikacijskih naprav in komunikacijskih vodov v poslovni stavbi organizacije.
- Pregledamo način varovanja delovnih prostorov organizacije ter način splošnega varovanja informacijskih virov.
- Ogledamo si strežniške sobe, njihove mehanizme fizičnega varovanja in zaščite in njene okolice.
- Pregledamo dnevnik dostopov do strežniške sobe ter izvedemo podrobni pregled dostopov na podlagi izbranega vzorca.
- Pregledamo dnevnik vzdrževanja naprav za zagotavljanje varnosti in zaščito pred okoljskimi vplivi.
- Pregledamo druge ukrepe za zagotavljanje fizične varnosti

[4] Vse vzorčne teste je potrebno prilagoditi dejanskim kontrolnim ciljem, informacijskemu okolju in tveganjem.