DOKUMENT:	**PRIMER TEST RAVNANJA Z ADMINISTRATORSKIMI DOSTOPI OSNUTEK**
Ime revidiranca:	
Ime revizije:	Revizija delovanja informacijskih sistemov po okviru COBIT 4.1[1]
Namen dokumenta:	Dokumentirati področje ravnanja z administratorskimi in drugimi močnimi uporabniškimi imeni[2]
Cilj testa:	Ugotoviti skladnost s COBIT kontrolnimi cilji in morebitne odmike od dobrih praks upravljanja močnih uporabniških imen.
Povezave na COBIT procese[3]:	**DS5 Zagotovite varnost sistemov** **DS5.3 Upravljanje identitete** Zagotovite, da so vsi uporabniki (notranji, zunanji in začasni) in njihove dejavnosti na sistemih IT (poslovne aplikacije, IT okolje, sistemske operacije, razvoj in vzdrževanje) enolično prepoznavni. Preko avtentikacijskih mehanizmov omogočite prepoznavanje identitete uporabnikov. Potrdite, da so pravice uporabnikov glede dostopa do sistemov in podatkov v skladu z opredeljenimi in dokumentiranimi poslovnimi potrebami ter da so

[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.

	zahteve delovnega mesta povezane z identiteto uporabnikov. Poskrbite, da dostopne pravice uporabnika zahteva njegovo nadrejeno vodstvo, da jih odobrijo lastniki sistemov in da jih dodeli oseba, zadolžena za varnost. Identitete uporabnikov ter dostopne pravice vzdržujte centralno. Uporabite stroškovno učinkovite tehnične in postopkovne ukrepe in jih posodabljajte za identifikacijo uporabnikov, avtentikacijo in uveljavitev dostopnih pravic.. **DS5.4 Upravljanje uporabniškega računa** Obravnavajte zahtevo, vzpostavitev, izdajo, začasen odvzem, spremembo in zaprtje uporabniškega računa ter s tem povezanih uporabniških privilegijev s sklopom postopkov za upravljanje uporabniškega računa. Vključite postopek za odobritev, ki določa lastnika podatkov ali sistema za dodeljevanje privilegijev za dostop. Ti postopki morajo veljati za vse uporabnike, vključno z administratorji (privilegirani uporabniki) ter notranjimi in zunanjimi uporabniki, v običajnih razmerah in v primeru sile. Pravice in obveznosti v zvezi z dostopom do sistemov in informacij podjetja morajo biti pogodbeno dogovorjene za vse vrste uporabnikov. Izvajajte redne vodstvene preglede vseh računov in z njimi povezanih privilegijev.
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 z administratorskimi uporabniškimi imeni:

- Dokumentiramo administratorska in druga močna uporabniška imena.
- Dokumentiramo potencialno ločitev dnevniških zapisov za akcije, opravljene pod temi uporabniškimi imeni.
- Dokumentiramo metode alternativnega hranjenja gesel za administrativna in druga močna uporabniška imena.
- Za pregledovano programsko rešitev, operacijski sistem ali sistem za upravljanje zbirk podatkov pridobimo seznam standardnih administratorskih imen in gesel ter potrdimo, da so bila spremenjena. Pri tem si lahko pomagamo z brezplačnimi analitskimi orodji, kot je na primer MBSA[5].

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

[5] Microsoft Baseline Security Analizer; brezplačno Microsoft orodje, ki je na voljo na spletni strani: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=7558