

DOKUMENT:	PRIMER TEST VARNOSTNEGA KOPIRANJA PODATKOV OSNUTEK
Ime revidiranca:	
Ime revizije:	Revizija delovanja informacijskih sistemov po okviru COBIT 4.1 ¹
Namen dokumenta:	Dokumentirati ugotovitve pregleda varnostnega kopiranja ²
Cilj testa:	Pregledati kako kakovostne so nastavitve varnostnih politik za omejevanje dostopa
Povezave na COBIT procese ³ :	<p>DS4 Zagotovite neprekinjenost storitev</p> <p>DS4.9 Varnostno shranjevanje na izločeni lokaciji</p> <p>Na izločeni lokaciji shranite vse kritične varnostne nosilce podatkov, dokumentacijo in druga sredstva IT, ki so potrebna za obnovo IT, in načrte neprekinjenega poslovanja. Vsebinsko varnostne kopije določite s sodelovanjem med lastniki poslovnih procesov in osebjem IT. Upravljanje izločene zmogljivosti za shranjevanje mora ustrezati politiki za klasifikacijo podatkov in praksam podjetja za shranjevanje nosilcev podatkov. Vodstvo IT mora zagotoviti, da se ureditev delovanja izločene lokacije</p>

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, vsebinsko revizijske naloge in informacijskim okolje revidiranca.

Dokument je pripravljen kot pomoč pri izvedbi revizijskega posla. Pred izvedbo vsakega revizijskega posla ga je potrebno prilagoditi zahtevam in posebnostim dogovorjenega posla. Elementi dokumenta niso obvezni in ne predstavljajo obveznega ravnanja strokovnjakov za revizijo IS in dajanje zagotovil.

	<p>redno ocenjuje (vsaj enkrat letno) glede ustreznosti vsebine, okoljskih pogojev in varnosti. Zagotovite združljivost strojne in programske opreme za obnovo arhiviranih podatkov ter redno testirajte in osvežujte arhivirane podatke.</p> <p>DS11 Upravljajte podatke</p> <p>DS11.1 Poslovne zahteve za upravljanje podatkov</p> <p>Potrdite, da so vsi podatki, pričakovani za obdelavo, prejeti ter obdelani v celoti, pravilno in pravočasno ter da se vsi rezultati razdelijo v skladu s poslovnimi zahtevami. Podpirajte potrebe za ponoven zagon in ponovno obdelavo.</p> <p>DS11.2 Dogovori za shranjevanje in hrambo</p> <p>Opredelite in vpeljite postopke za uspešno in učinkovito shranjevanje podatkov, njihovo hrambo in arhiviranje, da izpolnite poslovne cilje, varnostno politiko organizacije in zahteve regulative.</p> <p>DS11.3 Sistem za upravljanje knjižnice nosilcev podatkov</p> <p>Opredelite in vpeljite postopke za vzdrževanje popisa shranjenih in arhiviranih nosilcev podatkov, da zagotovite njihovo uporabnost in celovitost.</p> <p>DS11.4 Odstranjevanje</p> <p>Opredelite in vpeljite postopke za zagotovitev, da so poslovne zahteve za varstvo občutljivih podatkov in programske opreme izpolnjene, kadar se podatki in strojna oprema odstranijo ali prenesejo.</p> <p>DS11.5 Varnostno kopiranje in obnova</p> <p>Opredelite in vpeljite postopke za varnostno kopiranje in obnovo sistemov, aplikacij, podatkov in dokumentacije v skladu s poslovnimi zahtevami in načrtom za neprekinjenost.</p> <p>DS11.6 Varnostne zahteve za upravljanje podatkov</p> <p>Opredelite in vpeljite politike in postopke za prepoznavanje in uporabo varnostnih zahtev, ki veljajo za sprejetje, obdelavo, shranjevanje in ustvarjanje podatkov, tako da se izpolnijo poslovni cilji, varnostna politika organizacije in zahteve regulatorjev.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 testi⁴ varnostnega kopiranja podatkov:

- Pridobimo podatke o metodi, ki jo organizacija uporablja za rezervno kopiranje.
- Pridobimo podatke o uporabniških zahtevah za frekvenco varnostnega kopiranja ter periodo hrambe podatkov (zlasti tistih podatkov, za katere veljajo posebne varnostne zahteve).
- Pregledamo predmet varnostnega kopiranja in urnik varnostnega kopiranja v programski rešitvi za varnostno kopiranje.
- Pregledamo zagotovila o uspešnosti zrcaljenja ali kopiranja podatkov na rezervno lokacijo.

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

- Pregledamo vzorec dnevniških zapisov o uspešnosti izvedenega varnostnega kopiranja podatkov ter raziščemo morebitne napake/zakasnitve.
- Vizualno pregledamo robota (knjižnico) za varnostno kopiranje podatkov.
- Vizualno pregledamo medije za varnostno kopiranje podatkov, njihove oznake in druge fizične značilnosti (skupaj z mediji v sefih in rotacijskim načrtom)
- Pregledamo dokumentacijo o preizkusu ponovnega priklica podatkov.
- Pregledamo metode za varno uničevanje pomnilniških medijev ter na vzorcu preizkusimo, ali je prišlo do pravočasnega odpisa medijev.
- Pregledamo postopke varovanja varnostnih kopij podatkov (fizičnega varovanja medijev).
- Pregledamo zahteve, ki jih ima organizacija za hrambo podatkov skladno z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA)⁵.
- Pregledamo način hrambe podatkov pri zunanjem izvajalcu storitev arhiviranja.

⁵ Uradni list RS, št. 30/2006.