DOKUMENT:	**PREDLOGA SEZNAM STANDARDNIH DOKUMENTOV ZA IZVEDBO OSNOVNIH POSTOPKOV REVIZIJE DELOVANJA IS OSNUTEK**
Ime revidiranca:	
Ime revizije:	Revizija učinkovitosti delovanja informacijskega sistema ABC po okviru COBIT 4.1[1]
Namen dokumenta:	Opredeliti standardne zahteve po dokumentih za revizije delovanja[2]
V vednost:	
Avtor:	Maja Hmelak, Uroš Žust

Verzija	Datum	Oseba	Opis
1.0	16.9.2013	MH, UŽ	Prva pripravljena verzija
1.1	20.10.2013	MH, UŽ	Uskladitev dokumentov na nivoju celotne mape
1.2	4.11.2013	MH, UŽ	Izboljšanje skladno s prvimi povratnimi komentarji

Za uspešen in učinkovit potek revizij informacijskih sistemov je pomembno, da ima organizacija dovolj časa, da se nanjo pripravi ter dovolj informacij, da ve kaj bo strokovnjak za revizijo IS in dajanje zagotovil za opravljanje svojega dela potreboval. V nadaljevanju predstavljamo okviren seznam dokumentov, ki jih

[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.

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

strokovnjak za revizijo IS in dajanje zagotovil potrebuje v prvi fazi revizijske naloge – spoznavanju poslovnega in informacijskega okolja organizacije. Seznam za organizacijo ni obvezujoč – le redke organizacije v Sloveniji imajo vse ali celo večino naštetih dokumentov; naštevamo širok spekter dokumentov, od katerih bodo na voljo nekateri. Informacije o ostalih področjih bo strokovnjak za revizijo IS in dajanje zagotovil r pridobival na druge načine.

- Opis informacijskega sistema: ključnih aplikacij in njihovih funkcionalnosti, baz podatkov, operacijskih sistemov, komponent omrežja (glej tudi **103003 PREDLOGA Seznam aplikacij**);
- Shema računalniškega omrežja;
- Shema pretoka podatkov med aplikacijami;
- Seznam vseh strežnikov ter navedba verzije operacijskega sistema ter baze podatkov,
- Organizacijska shema organizacije in oddelka za informatiko – seznam zaposlenih z njihovimi odgovornostmi
- Ocena operativnih tveganj – tveganj informacijskih tehnologij
- Dokumentacijo s področja upravljanja odnosov z zunanjimi dobavitelji storitev,
- Dokumentacijo s področja upravljanja informacijskih sredstev,
- Dokumentacijo s področja ločevanja vlog v oddelku informatike,
- Poročila notranje ali zunanje revizije za področje IT za zadnjih 12 mesecev,
- Načrt vzdrževanja strojne opreme,
- Dokumenti informacijske varnosti
- Splošna politika informacijske varnosti,
- Varnostne politike, delovne procedure in drugi dokumenti posameznih področij informacijske varnosti na primer:
    - klasifikacije podatkov,
    - zagotavljanje zaupnosti podatkov,
    - dodeljevanje in odvzem uporabniških dostopov in pravic, vključno z zunanjimi dostopi,
    - varovanje opredmetenih informacijskih tehnologij,
    - varno uničevanje elektronskih nosilcev podatkov,

  - varovanje pred zlonamerno programsko kodo,
  - varovanje omrežja,
  - varnost elektronskega poslovanja,
  - zagotavljanja revizijske sledi,
  - upravljanje gesel,
  - postopki »čiste« mize in »čistega« ekrana,
  - kriptografske tehnologije,
  - upravljanje varnostnih incidentov
- Opis delovnega mesta varnostnega inženirja oziroma osebe zadolžene za varnost
- Dokumenti upravljanja informacijskega sistema
- Strategija razvoja informacijske funkcije,
- Seznam razvojnih nalog – pomembnejših sprememb pregledovanega poslovnega leta,
- Politika in procedure uvajanja sprememb,
- Politike in procedure arhiviranja podatkov,
- Politike in procedure nadgrajevanja operacijskih sistemov,
- Politike in procedure neprekinjenega poslovanja in okrevanja po katastrofi,
- Politike in procedure zaščite avtorskih pravic programske opreme,
- Dokumenti za izvedbo testiranj
- Seznam zaposlenih
- Seznam zaposlenih, ki so organizacijo zapustili v obdobju zadnjega leta
- Zapisnik prevoza trakov na oddaljeno lokacijo za obdobje od XX do XY;
- Opis ključnih nadgradenj in novo uvedenih elementov informacijskega sistema;
- Razpored dnevnih sveženjskih obdelav in seznam obdelav v dejanskem času.
- Projektna dokumentacija večjih sprememb v informacijskem okolju, vključno z morebitnimi analizami pripadajočih tveganj, izvedenimi pred uvedbo

Za pridobivanje zagotovil o operativni učinkovitosti kontrol informacijskega sistema ter za pridobivanje zagotovil o ustrezni zasnovi in učinkovitosti aplikativnih kontrol strokovnjak za revizijo IS in dajanje zagotovil potrebuje dodatne dokaze. Te večinoma zbere pri opravljanju samih revizijskih postopkov, navadno z različnimi metodami vzorčenja.