

<b>DOKUMENT:</b>	<b>PRIMER TEST POGODB O NAKUPU/RAZVOJU/VZDRŽEVANJU PROGRAMSKE REŠITVE OSNUTEK</b>
Ime revidiranca:	
Ime revizije:	Revizija delovanja informacijskih sistemov po okviru COBIT 4.1 <sup>1</sup>
Namen dokumenta:	Dokumentirati ugotovitve pregleda pogodb s ključnimi zunanjimi razvijalci in izvajalci vzdrževanja na področju IT organizacije <sup>2</sup>
Cilj testa:	Ugotoviti skladnost s COBIT kontrolnimi cilji in morebitne odmike v pogodbenih dogovorih. V primeru, da organizacija kupuje/vzdržuje nestandardno programsko rešitev, ki je ali razvita zanj ali pomembno prilagojena zanj, mora poskrbeti, da so s pogodbenim dogovorom njeni interesi kar najbolj zaščiteni.
Povezave na COBIT procese <sup>3</sup> :	<b>AI5 Zagotovite vire IT</b> <b>AI5.2 Upravljanje pogodb dobaviteljev</b>  Vzpostavite postopek za sklenitev, spreminjanje in prekinitev pogodb z vsemi dobavitelji. Postopek mora zajemati najmanj pravne, finančne, organizacijske,

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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.

*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.*

	<p>dokumentacijske, zmogljivostne, varnostne, intelektualno-lastninske in prekinitvene odgovornosti in obveznosti (vključno s kazenskimi določbami). Vse pogodbe in spremembe pogodb morajo pregledati pravni svetovalci.</p> <p><b>AI5.4 Nabava virov IT</b></p> <p>Zaščitite in uveljavite interese organizacije v vseh nabavnih pogodbenih sporazumih, vključno z navedbo pogodbenih določil o pravicah in obveznostih vseh strani v pogodbenem smislu glede nabave programske opreme, razvojnih virov, infrastrukture in storitev.</p> <p><b>DS2 Izvajajte in podpirajte</b></p> <p><b>DS2.3 Obvladovanje tveganja dobavitelja</b></p> <p>Prepoznajte in zmanjšajte tveganja, povezana s sposobnostjo dobavitelja za neprekinjeno uspešno izvajanje storitev na varen in učinkovit način. Zagotovite, da so pogodbe v skladu z univerzalnimi poslovnimi standardi glede pravnih in regulativnih zahtev. Obvladovanje tveganja mora nadalje upoštevati klavzule glede varovanja poslovne skrivnosti, pogodbe o hranjenju izvirne programske kode, boniteto dobaviteljev, skladnost z varnostnimi zahtevami, nadomestne dobavitelje, kazni in nagrade itd.</p>
Opis področja:	programskih rešitev naj bi se pridobilo že v okviru spoznavanja informacijskega okolja organizacije (glej mapo <b>1040 Spoznavanje okolja organizacije</b> ).
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 testi<sup>4</sup> področja pogodbenih dogovorov:

- Spoznamo področje pogodbenih dogovorov vključno s postopki za pregled pogodb in njihovo parafiranje pred podpisom.
- Spoznamo področje upravljanja in hrambe fizičnih izvodov pogodb ter pregledamo vzorec z vidika ustrezne hrambe.
- Spoznamo področje oblikovanja pogodbenih zahtev pri javnih naročilih.
- Pregledamo ključne pogodbe za pomembne elemente pogodbenih dogovorov.

## 1. Splošni elementi pogodbe<sup>5</sup>

Element pogodbe	Stanje
Naslov pogodbe	
Podatki o pogodbenih strankah (naziv, naslov, davčna in matična številka, odgovorna oseba)	
Podpisniki (tako da so razvidna njihova imena in funkcije)	
Trajanje pogodbe, začetek in zaključek veljavnosti pogodbe	
Datum in mesto podpisa pogodbe	
Pogodba pregledana s strani pravne službe	
Pogodba podpisana na vsaki strani	
Številčenje vseh strani pogodbe	
Postopki in določitev pristojnega sodišča v primeru spora	
Število izvodov pogodbe	
Cena in način plačila	
Zamudne obresti v primeru zamude plačila	
Sklicevanje na morebitne prejšnje pogodbe	

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

<sup>5</sup> Priložena seznama nista dokončna. Vsaka organizacija potrebuje svoj seznam priporočenih elementov pogodb, iz katerega bo razvidno, kaj so zanjo ključne zahteve.

Obveznost občasnega pregleda pogodbe, če je ta sklenjena za daljše časovno obdobje.	
Podroben opis predmeta pogodbe	
Podroben opis odgovornosti vsake od pogodbenih strani	
Podroben opis pravic in obveznosti vsake izmed pogodbenih strani v primeru prenehanja pogodbe in to na način, ki bo zagotovil kontinuiteto delovanja	
Opis odgovornosti izvajalca in njegovih zaposlenih za varovanje zaupnosti podatkov in varovanje poslovne tajnosti	
Definicija obveznosti izvajalca, da pred vključitvijo tretjih podizvajalcev v opravljanje dogovorjene storitve zaprosi za soglasje naročnika	
Določitev komunikacijskih poti – kanalov med naročnikom in izvajalcem	
Opredelitev možnosti predčasne prekinitve pogodbenega razmerja z zunanjim izvajalcem na zahtevo naročnika	
Določitev odgovorne osebe za pogodbo na strani izvajalca in naročnika	
Opredelitev pravic intelektualne lastnine	
Opredelitev ravnanja v primeru višje sile	
Opredelitev pogodbenih kazni	
Zagotovitev vpogleda v rezultate neodvisnih revizijskih pregledov in / ali pregledov notranje revizije izvajalca	
Opredelitev jasnih meril, po katerih se bo lahko pogodbo ustrezno spremljalo in primernost njenega izvajanja ocenjevalo	

## 2. Elementi dogovorov z zunanjimi izvajalci informacijske podpore

Priporočen element pogodbe	Stanje
Dovoljenje naročniku za neposredni nadzor nad opravljanjem pogodbenih storitev pri izvajalcu	
Opis načina izvajanja neposrednega nadzora nad opravljanjem pogodbenih storitev pri izvajalcu	
Zagotovitev možnosti zahteve naročnika po neodvisni reviziji pri pogodbenem izvajalcu	
Zagotovitev vpogleda v rezultate neodvisnih revizijskih pregledov in/ali pregledov notranje revizije izvajalca	
Izrecna zahteva za skladnost delovanja zunanjega izvajalca z veljavno zakonodajo in drugimi predpisi	
Določitev meril ravni kakovosti storitve	

Določitev postopkov za obveščanje o doseženi ravni kakovosti storitev	
---	--