**PRILOG 1.**

**Datum: …travanj 2019…………………**

**Memorandum o planiranju angažmana**

**Revizijski angažman: ...Revizija IT-a.........................................**

# Svrha i opravdanost angažmana

*Rok za provedbu novog sustava za upravljanje resursima SAP-HR u Ministarstvu gospodarstva jest 1. srpnja 2019. Posljednjih je godina nekoliko manjih i većih IT projekata u našem javnom sektoru završilo neuspjehom ili je proizvelo nekoliko nepredviđenih problema (financijskih, operativnih i organizacijskih). Glavni tajnik Ministarstva želi spriječiti takve neuspjehe u budućnosti. Novi sustav SAP stoga će se uvesti samo ako bude postojala razumna razina sigurnosti da će sustav ispuniti očekivanja te da će potencijalni nedostaci i rizici biti izbjegnuti koliko je god moguće. Glavni tajnik zatražio je od odjela za reviziju dodatna uvjerenja u pogledu tih pitanja, kao i u pogledu upravljanja provedbom samog projekta.*

# Opis aktivnosti subjekta i postupka nad kojim se provodi revizija

## Postupak nad kojim se provodi revizija

*Sustav SAP-HR uvest će se putem privremene organizacije projekta odgovorne za besprijekornu provedbu. Novi sustav SAP-HR integrirat će sljedeće postupke: obračun plaće, administracija zaposlenika, vremenska organizacija, organizacija putovanja, pravno izvještavanje.*

*Projektni tim čine voditelj projekta, zaposlenici odjela IT-a i vanjski savjetnik za SAP. Voditelj informacijskog odjela snosi potpunu odgovornost za projekt. Prema planu projekta, projekt je osmišljen u skladu s načelima upravljanja metode Prince-2 (Projekti u kontroliranim uvjetima 2).*

*Provedba se planira kroz sljedeće faze:*

1. *ocjena trenutačne situacije;*
2. *promjena plana upravljanja (+plan kontinuiteta);*
3. *izvršenje faze testiranja;*
4. *premještaj na novi sustav: pokretanje sustava 1. srpnja.*

*Ključni ciljevi utvrđeni za prijelaz na novi sustav jesu:*

*•• poboljšati usluge koje pruža odjel ljudskih resursa;*

*•• donositi bolje odluke na učinkovitiji način (cilj uprave);*

*•• poboljšati protok informacija među različitim odjelima;*

*•• modernizirati IT platformu za postupke povezane s ljudskim resursima;*

*•• jedinstvena točka pristupa i informacije za podatke o ljudskim resursima;*

*•• uklanjanje zadataka koji se obavljaju ručno, manje pogrešaka;*

*•• bolja integracija i transparentnost postupaka;*

*•• više produktivnosti i učinkovitosti;*

*•• manji operativni troškovi uklanjanjem zastarjelih sustava.*

# Glavni rizici povezani s postupcima nad kojima se provodi revizija

*Tipični rizici u provedbi sličnih sustava (i prijelazu na njih) obično se definiraju s pomoću triju načela ovlaštenih unutarnjih revizora:* ***p****ovjerljivost (rizik od gubitka/odavanja ključnih ili privatnih informacija trećim osobama),* ***i****ntegritet (vjerodostojnost podataka koje pruža sustav) i* ***d****ostupnost (kontinuitet, sigurnosno kopiranje i oporavak itd.). Općenito, trebala bi se uspostaviti dovoljna kombinacija kontrola aplikacije i općih kontrola radi suočavanja s rizicima koji su povezani s tim trima načelima.*

*Drugi se rizici povezuju s pristupom na temelju vrste faze strukture projekta koji bi trebao otvoriti put uspješnoj provedbi novog sustava: rizici u pogledu odgovarajućih aranžmana upravljanja samog projekta IT-a.*

# Cilj(evi) i obuhvat revizijskog angažmana

*Cilj je revizije dati razumno uvjerenje za sljedeća ključna pitanja revizije:*

* *Je li* ***upravljanje*** *projektom osmišljeno i funkcionira li tako da otvara put uspješnom prelasku na SAP-HR i njegovoj provedbi u Ministarstvu gospodarstva?*
* *Je li* ***prikladnost*** *kontrola aplikacije i općih kontrola* ***dovoljna*** *u pogledu povjerljivosti podataka, njihova integriteta i dostupnosti važnih informacija sustava povezanih s ljudskim resursima tijekom faze projekta, faze prijelaza i provedbe projekta?*

## *Izjave o uvjerenju o pravilnom upravljanju projektom, kao i o prikladnosti kontrola povezanih s povjerljivošću, integritetom i dostupnošću na razini aplikacije i općoj razini bit će popraćene preporukama ako bude potrebno i primjenjivo. Mogući nalazi i preporuke.*

*Kriteriji koji se trebaju upotrebljavati u reviziji izdvojit će se iz sljedećih revizijskih referentnih okvira:*

* ***Prince2****: sljedeća načela Prince2 vodeća su za procjenu pravilnog upravljanja projektom: poslovni slučaj (kontinuirana poslovna opravdanost), utvrđene uloge i odgovornosti u skladu sa strukturom Prince2, upravljanje prema fazama (pristup po fazama, uključujući upravljanje rizikom) i usmjerenost na proizvode u skladu s prethodno utvrđenim razinama tolerancije. Ukupni skup normi u pogledu tih načela opisan je u prilogu;*
* ***COBIT5:*** *Kriteriji triju načela ovlaštenih unutarnjih revizora proizlaze iz sljedećih modula Kontrolnih ciljeva za informacijske i srodne tehnologije (COBIT-5): uskladiti/planirati/organizirati (APO), izraditi/dobiti/provesti (BAI), pružiti/održavati/podržavati (DSS) i pratiti/ocijeniti/procijeniti (MEA). Moduli COBIT-5 opisuju kriterije za svaku fazu od planiranja do potpune provedbe sustava IT-a u bilo kojoj vrsti organizacije. Ključni kriteriji po modulu, kao što je raspravljeno s voditeljem informacijskog odjela, vodit će do izjave o uvjerenju o prikladnosti općih kontrola i kontrola aplikacije u svakoj fazi na putu prema provedbi;*
* *Postojeći organizacijski* ***postupci i propisi*** *koji su važni za postupak prijelaza na novi sustav SAP-HR. Ako su ti postupci i propisi u sukobu sa zahtjevima Prince2 i/ili COBIT-5, to će se navesti kao nalaz revizije.*

## Obuhvat

*Revizija neće proširiti svoj obuhvat procjenom ključnih ciljeva utvrđenih za prijelaz na novi sustav.*

# Metodologija revizije

|  |  |  |  |
| --- | --- | --- | --- |
| Cilj revizije / pitanje | Ključni aspekti | Kriteriji | Metodologija  (Instrumenti za reviziju) |
| **Pravilno upravljanje**: je li projekt usklađen s načelima Prince-2 u pogledu dizajna i rada u svakoj fazi projekta? | Poslovni slučaj (PS) | * PS se ažurira u svakoj fazi projekta. * Razlozi za provedbu projekta moraju biti sukladni organizacijskoj strategiji i strategiji programa. * Plan projekta i PS moraju biti usklađeni. * Prednosti treba jasno utvrditi i opravdati. * Treba biti jasno kako ostvariti prednosti. |  |
| Uloge i odgovornosti | * Izvršne uloge i uloge upravljanja projektom jasno su razgraničene. * itd. |  |
| **Dovoljno općih kontrola**: je li ukupno upravljanje ključnim postupcima IT-a dobro kontrolirano/organizirano unutar organizacije? | COBIT/APO12  Upravljanje rizicima | * Provedena je procjena rizika punog opsega u pogledu prijelaza na SAP-HR. * Stavak o riziku u dokumentu o planu/izradi obuhvaća prava pitanja. * itd. |  |
| **Dovoljne kontrole aplikacije**: jesu li kontrole obuhvaćene u novom sustavu koji se treba provesti (u samom sustavu i u kombinaciji s drugim sustavima tijekom faze prijelaza) dovoljne kako bi se izbjegli rizici koji se odnose na tri načela ovlaštenih unutarnjih revizora? | COBIT/DSS04  Upravljanje kontinuitetom | * Postupci sigurnosnog kopiranja i oporavka provode se u programu koji radi za vrijeme prelaska. * Program sadržava automatizirano pružanje usluga u slučaju smetnji. |  |

## Program revizije

*Ova će se revizija provesti kroz dva usporedna niza aktivnosti:*

***Aktivnosti koje se odnose na davanje razumnog uvjerenja o upravljanju projektom:****revizorski tim provest će aktivnosti revizije u stvarnom vremenu koje su vremenski uzastopne fazama projekta nad kojim se provodi revizija. Svaku fazu projekta (četiri faze) mora odobriti revizorski tim prije početka sljedeće faze. Revizorski će tim kontinuirano pratiti i ocjenjivati usklađenost s načelima Prince2. Svi dokumenti sastavljeni tijekom projekta bit će / mogu biti dio revizijskih dokaza. Povremeni razgovori održavat će se s članovima projektnog tima, upravom (voditelj informacijskog odjela) i drugim relevantnim dionicima (npr. odjel za ljudske resurse, odjel za IT).*

***Aktivnosti koje se odnose na davanje razumnog uvjerenja o dostatnosti općih kontrola i kontrola aplikacije:*** *za opće kontrole i kontrole aplikacije primjenjivat će se širok spektar revizijskih tehnika. Npr. različite vrste testova (na razini aplikacije, penetracijsko testiranje, sigurnosno testiranje, testiranje pouzdanosti i testiranje integriteta). Razgovori će se provoditi i s predstavnicima odjela za IT, odjela za ljudske resurse, odjela politika, uprave (uključujući voditelja informacijskog odjela). Načela COBIT5 i popratni kriteriji služe kao referentna točka za formiranje našeg mišljenja.*

*Oba revizorska tima održavat će redovite zajedničke sastanke kako bi informirali jedni druge o najnovijim podacima. Oba skupa aktivnosti smatraju se jednom revizijom.*

**Ključne točke revizije:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Faza projekta 1.  (siječanj 2019.) | Faza projekta 2.  (srpanj 2019.) | Faza projekta 3.  (prosinac 2019.) | Faza projekta 4. (srpanj 2020.) |
| **Revizija projekta:**  400 sati x 2 člana tima: 800 sati | Stvarno vrijeme + prolaz/pad nakon faze + privremeni izvještaj | Stvarno vrijeme + prolaz/pad nakon faze + privremeni izvještaj | Stvarno vrijeme + prolaz/pad nakon faze + privremeni izvještaj | Stvarno vrijeme + prolaz/pad nakon faze + privremeni izvještaj u kombinaciji s izvještajem s izražavanjem uvjerenja o kontrolama |
| **Revizija općih i IT kontrola**  300 sati x 2 člana tima: 600 sati | Preliminarno istraživanje | Nacrt / privremeni izvještaj o kontrolama dizajna u odnosu na plan upravljanja promjenama (APO+BAI) | Nacrt / privremeni izvještaj o kontrolama tijekom faze testiranja  (DSS+MEA) | Nacrt / ukupni izvještaj o kontrolama tijekom prijelaza i provedbe  (DSS+MEA) u kombinaciji s izvještajem s izražavanjem uvjerenja o projektu |

## Resursi

*Revizija će se provesti u skladu s poveljom o reviziji odjela za reviziju Ministarstva financija. S povjerljivim informacijama postupat će se u skladu s odredbama u toj povelji.*

|  |  |  |
| --- | --- | --- |
| **Uloga** | **Naziv** | **Funkcija** |
| Voditelj projekta | Iskusni ocjenjivač/revizor upravljanja resursima poduzeća (ERP-a) |  |
| Jedan revizor učinka | Ovlašten za Prince2 |  |
| Dva ovlaštena revizora za IT | Iskustvo u ocjeni COBIT |  |

# Moguće poteškoće (ako je primjenjivo)

*Rizik revizije jest mogućnost odgode projekta zbog nepredviđenih okolnosti. U tom će se slučaju revizija zamrznuti i kapaciteti upotrijebiti za druge angažmane dok se projekt ne nastavi.*