HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

Na temelju članka 15. točke 7. Zakona o Hrvatskoj agenciji za nadzor financijskih usluga (»Narodne novine« br. 145/05 i 12/12) Upravno vijeće Hrvatske agencije za nadzor financijskih usluga je na sjednici održanoj 7. veljače 2014. godine donijelo

SMJERNICE

ZA PROVEDBU REVIZIJE INFORMACIJSKOG SUSTAVA SUBJEKATA NADZORA OD STRANE REVIZORSKIH DRUŠTAVA

I. UVODNE ODREDBE

1. Ciljevi, namjena i opseg

1.1. Ciljevi

Ovim Smjernicama za provedbu revizije informacijskog sustava subjekata nadzora od strane revizorskih društava (u daljnjem tekstu: Smjernice) Hrvatska agencija za nadzor financijskih usluga (u daljnjem tekstu: Agencija) pruža smjernice za provedbu revizije informacijskog sustava (u daljnjem tekstu: IS) subjekata nadzora od strane revizorskih društava (u daljnjem tekstu: revizori).

Člankom 2. Zakona o Hrvatskoj agenciji za nadzor financijskih usluga („Narodne novine“ br. 140/05 i 12/12) subjekti nadzora (u daljnjem tekstu: subjekti) definirani su kao sve pravne ili fizičke osobe koje se bave pružanjem financijskih usluga, savjetovanjem na financijskom tržištu, prodajom, posredovanjem ili upravljanjem imovinom korisnika financijskih usluga. U djelokrug i nadležnost Agencije pripada nadzor financijskog tržišta, subjekata i financijskih usluga koje pružaju.

Agencija odgovarajućim zakonskim i podzakonskim aktima propisuje provedbu revizije IS određenih skupina subjekata od strane revizora te izradu izvješća o kvaliteti informacijskog sustava za potrebe Agencije (u daljnjem tekstu: izvješće za Agenciju).

Kako bi u konačnici doprinijela kvaliteti revizijskog postupka i izvješća za Agenciju, Agencija ovim Smjernicama želi ostvariti sljedeće ciljeve:

1) pojasniti načela, kriterije i postupke koje Agencija očekuje od revizora pri provedbi revizije IS subjekata te
2) pojasniti minimalna očekivanja Agencije vezana uz sadržaj izvješća za Agenciju izrađenih temeljem provedenog revizijskog postupka.

1.2. Namjena

Ove Smjernice namijenjene su:

1. revizorima koji, sukladno odgovarajućim zakonskim i podzakonskim aktima, provode reviziju IS kao dio revizije financijskih izvještaja subjekta u cilju stjecanja uvjerenja u pouzdanost i cjelovitost revidiranih podataka, temeljem čega izrađuju izvješće za Agenciju,
2. revizorima koji, sukladno odgovarajućim zakonskim i podzakonskim aktima, provode samostalnu reviziju IS subjekata, temeljem čega izrađuju izvješće za Agenciju te
3. subjektima nad čijim IS se provodi neki od revizijskih postupaka opisanih pod točkama 1. i 2.

Odredbe ovih Smjernica nisu primjenjive u slučajevima gdje provedba revizije IS subjekata u bilo kojem obliku, odnosno izrada izvješća za Agenciju, nije predviđena odgovarajućim zakonskim i podzakonskim aktima.

Agencija može odgovarajućim aktima dodatno propisati specifičnosti revizijskog postupka i izvješća za određene skupine subjekata, koje je potrebno uzeti u obzir uz odredbe ovih Smjernica.

1.3. Opseg

Ovim Smjernicama obuhvaćeno je sljedeće:

1) Načela, kriteriji i postupci provedbe revizije informacijskih sustava subjekata nadzora:

    - osnovna načela,
    - pristup temeljen na procjeni rizika,
    - osobe koje provode reviziju informacijskog sustava,
    - obuhvat revizije informacijskog sustava te
    - provedba revizije informacijskog sustava.

2) Minimalna očekivanja vezana uz sadržaj izvješća o kvaliteti informacijskog sustava za potrebe Hrvatske agencije za nadzor financijskih usluga:

    - opća ocjena stanja i adekvatnosti upravljanja informacijskog sustava,
    - osnovni podaci o provedbi revizijskog postupka,
    - opis informacijskog sustava,
    - uočene slabosti, nedostaci i rizici informacijskog sustava te preporuke za njihovo otklanjanje te
    - osvrt na status izvršenja preporuka za otklanjanje uočenih slabosti, nedostataka i rizika danih tijekom revizije provedene u prethodnom razdoblju.

II. NAČELA, KRITERIJI I POSTUPCI PROVEDBE REVIZIJE INFORMACIJSKOG SUSTAVA SUBJEKATA NADZORA

1. Osnovna načela

Revizor bi se u planiranju i provedbi revizijskog postupka te pri izradi izvješća trebao voditi međunarodno prihvaćenim revizijskim načelima**,** s posebnim naglaskom na načelo razmjernosti i načelo materijalnosti.

2. Pristup temeljen na procjeni rizika

Revizor bi trebao koristiti metodologije i postupke za reviziju IS temeljene na procjeni rizika.

Primjena metodologija i postupaka temeljenih na procjeni rizika zahtijeva razumijevanje specifičnosti samog subjekta i poslovnog okruženja u kojem se nalazi.

Stečena saznanja o specifičnostima subjekta i njegovog poslovnog okruženja revizor bi trebao koristiti u fazi planiranja postupka revizije IS, kako bi vlastite resurse efikasno i efektivno usmjerio na rizična područja.

U samom procesu provedbe revizije IS, revizor bi trebao identificirati specifične rizike IS i procijeniti njihovu razinu s obzirom na njihov utjecaj na poslovne procese i ostvarivanje poslovnih ciljeva subjekta, vodeći se načelima razmjernosti i materijalnosti.

Pri određivanju razine identificiranih rizika, revizor bi trebao uzeti u obzir dizajn i operativnu učinkovitost kontrola implementiranih u cilju upravljanja tim rizicima.

3. Osobe koje provode reviziju informacijskog sustava

Osobe uključene u bilo koju fazu revizijskog postupka trebale bi zadovoljavati osnovna revizorska i etička načela, kao što su:

- kompetentnost,
- osobni integritet,
- neovisnost,
- povjerljivost te
- objektivnost.

Kompetencije tih osoba trebale bi sadržavati odgovarajuće vještine, znanja i iskustvo na području provedbe revizije IS.

4. Obuhvat revizije informacijskog sustava

Obuhvat revizije IS trebao bi biti unaprijed planiran temeljem inicijalne procjene rizika IS. Slijedom toga, revizor bi u revizijskom postupku trebao uzeti u obzir relevantne procese upravljanja informacijskim sustavom te materijalne, nematerijalne i ljudske resurse koji se pri tome koriste. Revizor bi pri određivanju obuhvata posebnu pažnju trebao posvetiti onim dijelovima IS koji imaju značajnu ulogu u podršci središnjim poslovnim procesima subjekta.

5. Provedba revizije informacijskog sustava

Revizor bi se u revizijskom postupku trebao voditi međunarodno prihvaćenim metodologijama provedbe revizije IS, revizorskim standardima i etičkim načelima.

Revizor bi trebao provjeriti primjerenost uspostavljenih procesa upravljanja IS i njihovu dokumentiranost. Provjerom bi se trebala utvrditi razina uspostavljenosti procesa i pripadajućih kontrola, njihova operativna učinkovitost u praksi te eventualne slabosti, nedostatke i rizike koji iz njih proizlaze.

Revizor bi trebao analizirati ključne resurse korištene pri upravljanju IS, pri čemu bi posebnu pažnju trebao posvetiti njihovim svojstvima i parametrima te primjerenosti njihove uloge u podršci poslovanju subjekta te ostvarivanju ciljeva IS i poslovnih ciljeva subjekta u cjelini.

Revizor bi trebao uzeti u obzir i interne propise subjekta, kao i odredbe relevantnih zakonskih i podzakonskih akata.

Revizor bi trebao prikupiti i čuvati dovoljnu količinu dokaznog materijala kojima se potkrepljuju zaključci i nalazi kao rezultat revizijskog postupka.

Revizor bi po završetku revizijskog postupka trebao predstaviti zaključke i nalaze odgovornim osobama subjekta te od njih dobiti potvrdu činjenica utvrđenih tijekom postupka i očitovanje o danim nalazima i preporukama.

III. MINIMALNA OČEKIVANJA VEZANA UZ SADRŽAJ IZVJEŠĆA O KVALITETI INFORMACIJSKOG SUSTAVA ZA POTREBE HRVATSKE AGENCIJE ZA NADZOR FINANCIJSKIH USLUGA

1. Opća ocjena stanja i adekvatnosti upravljanja informacijskim sustavom

Revizor bi, temeljem utvrđenih činjenica u revizijskom postupku, u izvješću trebao dati opću ocjenu stanja i adekvatnosti upravljanja IS. Ocjena bi trebala biti opisnog karaktera, uz pojašnjenje činjenica na kojima se temelji.

2. Osnovni podaci o provedbi revizijskog postupka

Revizor bi u izvješću trebao navesti osnovne podatke vezane uz provedbu revizijskog postupka, što uključuje barem:

- korištene metodologije, standarde i okvire u revizijskom postupku,
- vremensko razdoblje u kojem je revizijski postupak proveden,
- lokacije na kojima se revizijski postupak provodio,
- treće strane angažirane od strane revizora u provedbi revizijskog postupka, uz opis njihove uloge u postupku te
- područja upravljanja IS koja su bila predmet revizijskog postupka.

3. Opis informacijskog sustava

Revizor bi u izvješću trebao navesti i ukratko opisati ključne elemente IS subjekta, što uključuje barem:

- ustrojstvo organizacijskih jedinica odgovornih za upravljanje IS i raspodjelu dužnosti unutar njih,
- sustav unutarnjih kontrola vezanih uz IS,
- tehnološku osnovicu IS, kao što su osobna i poslužiteljska računala, mrežni i telekomunikacijski uređaji, operativni sustavi, poslužitelji baza podataka, poslužitelji elektroničke pošte, datotečni poslužitelji i drugo,
- aplikacije koje se koriste kao podrška poslovanju,
- lokacije poslužiteljskih prostorija,
- vanjske pružatelje usluga i njihove uloge u funkcioniranju IS,
- kritične sustave zaštite IS te
- planove očuvanja neprekidnosti poslovanja i planove oporavka IS.

4. Uočene slabosti, nedostaci i rizici informacijskog sustava te preporuke za njihovo otklanjanje

Revizor bi u izvješću trebao navesti uočene slabosti, nedostatke i rizike IS te dati preporuke za njihovo otklanjanje, vodeći pri tome računa o sljedećem:

- Uočene slabosti, nedostatci i rizici te preporuke za njihovo otklanjanje trebali bi biti jasno razdvojeni u tekstu izvješća od ostalih cjelina, kao što su, na primjer, opisi IS, uočene slabosti, nedostatci i rizici, dane preporuke tijekom revizija u prethodnom razdoblju i slično.
- Revizor bi trebao navesti materijalno značajne slabosti, nedostatke i rizike uočene u revizijskom postupku, ocijeniti ih te pojasniti njihov utjecaj na poslovanje subjekta.
- Revizor bi trebao pojasniti temelje iz kojih se izvode ocjene razina uočenih slabosti, nedostataka i rizika.
- Revizor bi pri ocjenjivanju razina uočenih slabosti, nedostataka i rizika trebao voditi računa o načelima razmjernosti i materijalnosti.
- Revizor bi za materijalno značajne slabosti, nedostatke i rizike trebao dati preporuke aktivnosti i rokova za njihovo otklanjanje.
- Revizor bi za dane preporuke trebao pribaviti i dokumentirati očitovanje odgovornih osoba subjekta o prihvaćanju, odnosno neprihvaćanju preporuka uz obrazloženje.

5. *Osvrt na status izvršenja preporuka za otklanjanje uočenih slabosti, nedostataka i rizika danih tijekom revizije provedene u prethodnom razdoblju*

Revizor bi u izvješću trebao navesti osvrt na postupke subjekta s obzirom na preporuke dane tijekom revizije provedene u prethodnom razdoblju, vodeći pri tome računa o sljedećem:

- Revizor bi trebao pojedinačno navesti sve preporuke dane tijekom revizije provedene u prethodnom razdoblju, uz aktualni status provedbe i opis poduzetih aktivnosti u slučaju da su preporuke u potpunosti ili djelomično izvršene.
- Status izvršenja preporuka danih tijekom revizije provedene u prethodnom razdoblju trebalo bi biti jasno razdvojeno u tekstu od ostalih cjelina, kao što su, na primjer, opisi IS, uočene slabosti, nedostatci i rizici, dane preporuke tijekom aktualne revizije i slično.

IV. PRIJELAZNE I ZAVRŠNE ODREDBE

Ove Smjernice se objavljuju na Internetskoj stranici Agencije te stupaju na snagu danom objave.

Klasa: 011-02/14-04/8

Urbroj: 326-15-14-1

Zagreb, 07. veljače 2014.

Predsjednik Upravnog Vijeća

Petar – Pierre Matek