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 21. prosinca 2022. 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: Hanfa) 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 Hanfe pripada nadzor financijskog tržišta, subjekata i financijskih usluga koje pružaju.

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

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

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

1.2. Namjena

Ove Smjernice namijenjene su:

1. revizorima koji, sukladno odgovarajućim zakonskim i podzakonskim aktima te aktima Europske Unije provode reviziju IS kao dio revizije financijskih izvještaja subjekta u cilju stjecanja uvjerenja u pouzdanost i cjelovitost revidiranih podataka, temeljem čega izrađuju izvješće za Hanfu,
2. revizorima koji, sukladno odgovarajućim zakonskim i podzakonskim aktima te aktima Europske Unije provode samostalnu reviziju IS subjekata, temeljem čega izrađuju izvješće za Hanfu 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 Hanfu, nije predviđena odgovarajućim zakonskim i podzakonskim aktima ni aktima Europske Unije.

Hanfa 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 IS subjekata:

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

2) Minimalna očekivanja vezana uz sadržaj izvješća o kvaliteti IS za potrebe Hanfe:

    - opća ocjena stanja i adekvatnosti upravljanja IS,
    - osnovni podaci o provedbi revizijskog postupka,
    - opis IS,
    - opis mjera za upravljanje kibernetičkom i informacijskom sigurnošću IS
    - 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 se u planiranju i provedbi revizijskog postupka te pri izradi izvješća treba voditi međunarodno prihvaćenim revizijskim načelima**,** s posebnim naglaskom na načelo razmjernosti i načelo materijalnosti.

2. Pristup temeljen na procjeni rizika

Revizor treba 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 treba 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 treba 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 treba 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 moraju zadovoljavati osnovna revizorska i etička načela, kao što su:

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

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

4. Obuhvat revizije informacijskog sustava

Obuhvat revizije IS treba biti unaprijed planiran temeljem inicijalne procjene rizika IS. Slijedom toga, revizor u revizijskom postupku treba uzeti u obzir relevantne procese upravljanja IS, organizacijska i tehnička rješenja zaštite IS, usklađenost IS s mjerodavnim propisima te materijalne, nematerijalne i ljudske resurse koji se pri tome koriste. Revizor, pri određivanju obuhvata, posebnu pažnju treba posvetiti onim dijelovima IS koji imaju značajnu ulogu u podršci središnjim poslovnim procesima subjekta.

5. Provedba revizije informacijskog sustava

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

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

Revizor treba analizirati ključne resurse korištene pri upravljanju IS, učinkovitost uspostavljenih organizacijskih i tehničkih mjera zaštite IS od kibernetičkih i drugih prijetnji sigurnosti IS pri čemu posebnu pažnju treba posvetiti njihovim svojstvima i parametrima te primjerenosti njihove uloge u podršci poslovanju subjekta te ostvarivanju ciljeva IS i poslovnih ciljeva subjekta u cjelini.

Revizor treba uzeti u obzir interne propise subjekta, kao i odredbe relevantnih zakonskih i podzakonskih akata te akata Europske Unije.

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

Revizor, po završetku revizijskog postupka, treba 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 HANFE

1. Opća ocjena stanja i adekvatnosti upravljanja informacijskim sustavom

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

2. Osnovni podaci o provedbi revizijskog postupka

Revizor izvješću treba navesti osnovne podatke vezane uz provedbu revizijskog postupka, što uključuje najmanje:

- 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 u izvješću treba navesti i ukratko opisati ključne elemente IS subjekta, što uključuje najmanje:

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

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

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

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

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

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

- Revizor treba 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 treba biti jasno razdvojen u tekstu od ostalih cjelina, kao što su, na primjer, opisi IS, uočene slabosti, nesukladnosti, nedostatci i rizici, dane preporuke tijekom aktualne revizije i slično.

IV.PRIJELAZNE I ZAVRŠNE ODREDBE

Ove Smjernice se objavljuju na internetskoj stranici Hanfe te stupaju na snagu danom objave.

Stupanjem na snagu ovih Smjernica, prestaju važiti Smjernice za provedbu revizije informacijskih sustava subjekata nadzora od strane revizorskih društava od 7. veljače 2014.

KLASA: 011-01/22-07/01
URBROJ: 326-01-25-22-1
Zagreb, 21. prosinca, 2022.

PREDSJEDNIK UPRAVNOG VIJEĆA

dr. sc. Ante Žigman