BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
AGENCIJA ZA BANKARSTVO FEDERACIJE BOSNE I HERCEGOVINE

OČEKIVANJA AGENCIJE ZA BANKARSTVO FBIH VEZANA UZ OBAVLJANJE REVIZIJE INFORMACIONOG SISTEMA U BANKAMA OD STRANE EKSTERNOG REVIZORA

Juli 2012. godine

Sadržaj

1. Uvod

Cilj ovog dokumenta jeste dati pregled očekivanja Agencije za bankarstvo FBiH (u daljem tekstu: Agencija) u vezi obavljanja eksterne revizije informacionih sistema u bankama, u skladu sa obavezama koje proističu iz Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama, Uputstva o licenciranju i Zakona o bankama. U skladu sa navedenim aktima, revizorska društva su dužna sastaviti revizorski izvještaj o obavljenoj reviziji za potrebe Agencije. Revizorski izvještaj, između ostaloga, treba da sadrži informacije o provedenoj reviziji informacionog sistema, ocjenu stanja i adekvatnosti upravljanja tim sistemom, te bi trebalo banci i Agenciji pružiti kvalitetne i potpune informacije o rizicima kojima je taj informacioni sistem izložen.

Dokument se odnosi na banke i eksterna revizorska društva (u daljem tekstu: Revizor), koja obavljaju reviziju informacionih sistema banaka.

Očekivanja Agencije u vezi obavljanja eksterne revizije informacionog sistema u bankama imaju za cilj poboljšanje kvalitete revizije informacionih sistema, te bolje razumijevanje uloga i odgovornosti banaka i Revizora u tom procesu.

Agencija očekuje da provođenje revizije, kao i revizorski izvještaj budu u skladu sa očekivanjima navedenim u nastavku ovog dokumenta. Agencija će u postupku davanja saglasnosti za obavljanje eksterne revizije informacionog sistema, cijeniti kvalitet i postupanja, te usklađenost revizorskog izvještaja sa ovim dokumentom.

2. Revizija informacionog sistema

Pri provođenju revizije informacionog sistema, Revizor bi trebao:

- služiti se metodama i postupcima za reviziju informacionih sistema zasnovanu na procjeni rizika,
- definisati obim i plan revizije, na osnovu procjene rizika, prije početka obavljanja revizije,
- definisati dubinu revizije, ovisno o zatečenom stanju informacionog sistema,
- provjeriti i ocijeniti stanje informacionog sistema i
- provjeriti poštuje li banka važeću zakonsku i podzakonsku regulativu.

Na osnovu provedene revizije informacionog sistema, Revizor će dati ocjenu o adekvatnosti upravljanja informacionim sistemom, te ukazati na značajne rizike kojima je banka izložena.

3. Angažman Revizora

Angažman i procedure odobrenja Revizora informacionog sistema, utvrđene su Odlukom o minimalnim standardima upravljanja informacionim sistemima u bankama, kao i Uputstvom za licenciranje.

Pri provođenju eksterne revizije informacionog sistema, očekuje se da banka i Revizor primjenjuju standarde koji su utvrđeni odredbama Zakona o računovodstvu i reviziji FBiH, u mjeri u kojoj su primjenjive (ugovor, ugovorni odnos, ustupanje poslova, potpisivanje izvještaja, vremenski period angažmana, broj zaposlenika, radna dokumentacija, povjerljivost podataka, sukob interesa i dr.).

Banka je dužna dostaviti izvještaj o provedenoj eksternoj reviziji informacionog sistema, u roku utvrđenom Zakonom o bankama.

Pri obavljanju eksterne revizije informacionog sistema, Revizor treba primjenjivati Međunarodne revizijske standarde, Kodeks profesionalne etike revizora i pravila revizorske struke, te druga pravila i propise koji regulišu ovu oblast.

4. Kompetencije osoba koje obavljaju eksternu reviziju

Osobe koje operativno provode reviziju informacionog sistema trebaju biti profesionalno kompetentne, posjedovati znanja, vještine i iskustva neophodna za obavljanje revizorskih zadataka, koja se stiču

kontinuiranom edukacijom (npr. formalnom edukacijom, te stručnim usavršavanjem i certificiranjem na područjima vezanim uz reviziju informacionih sistema i informacione sisteme), te posjedovati odgovarajuće radno iskustvo, kako bi se osiguralo kvalitetno i stručno obavljanje revizije informacionog sistema.

U svom radu, Revizor treba primjenjivati standarde za reviziju informacionih sistema, kao i druge odgovarajuće profesionalne ili industrijske standarde, kao i regulatorne zahtjeve, koji bi osigurali mogućnost izražavanja profesionalnog mišljenja o informacionom sistemu banke.

Ako uposlenici Revizora ne posjeduju znanja i vještine potrebne za obavljanje revizije informacionog sistema, Revizor može angažovati vanjske saradnike, koji posjeduju adekvatna, tražena znanja. Odgovornost Revizora prema banci i Agenciji, ne može se prenijeti na osobe koje je Revizor angažovao.

Revizor i angažovana treća lica trebaju biti neovisni, što podrazumijeva da u toku angažmana od strane banke ne mogu imati:

- bilo kakav direktan ili indirektan finansijski interes u banci ili kod bilo kog povezanog lica sa bankom i
- bilo kakav drugi odnos koji može kompromitovati njegovu nezavisnu ocjenu (konsultantske usluge, revizija sopstvenog rada, revizija rada za koji su bili prethodno odgovorni i slično).

5. Odgovornost Revizora i banke

U procesu obavljanja revizije informacionog sistema, banka treba da upozna Revizora sa svim sistemima i aplikacijama koje koristi u svojim aktivnostima. Banka je također odgovorna za dostavljanje sve dokumentacije koja se odnosi na njen informacioni sistem, informacija i dokumentacije koje Revizor traži, a koja je vezana za informacioni sistem banke, kao i da omogući Revizoru pristup resursima informacionog sistema putem ovlaštenog osoblja banke.

Revizor je odgovoran da, na bazi obavljenog procesa revizije i prikupljenih revizijskih dokaza, obezbijedi izvještaj koji sadrži objektivno i realno mišljenje, te ocjenu o stanju informacionog sistema i adekvatnosti upravljanja informacionim sistemom.

6. Planiranje revizije informacionog sistema

U cilju osiguranja efikasnog obavljanja revizije informacionog sistema banke, neophodno je da Revizor obavi planiranje procesa revizije. Primjereno planiranje treba da omogući uspostavljanje prioriteta s ciljem da se Revizor fokusira na značajna područja revizije. U tom kontekstu neophodno je definisati vrstu, obim i vremenski okvir revizijskih postupaka, kao i resurse koji su neophodni za obavljanje revizije. Treba imati na umu da je moguće da u toku obavljanja revizije dođe do promjene u obimu i vremenskom rasporedu revizijskih postupaka zbog promjena okolnosti ili neočekivanih ishoda revizijskih postupaka.

Pri planiranju i definisanju plana revizije informacionog sistema banke, Revizor bi trebao uzeti u obzir slijedeće:

- veličinu banke (tržišnu i finansijsku poziciju i slično),
- profil rizičnosti banke te sklonost preuzimanju rizika,
- obim i složenost usluga koje banka pruža,
- organizaciju banke (broj zaposlenika na nivou banke, organizacionu strukturu banke, broj poslovnih jedinica, organizacionu strukturu jedinice za upravljanje informacionim sistemom i njenu veličinu i slično),
- tehnološku složenost informacionog sistema (heterogenost software-skih i hardware-skih resursa, obim i složenost mrežne infrastrukture i slično),
- nivo eksternalizovnih aktivnosti vezanih za informacioni sistem banke (broj vanjskih pružaoca usluga i nivo značajnosti usluga koje isti obavljaju, ovisnost o vanjskim pružaocima usluga i slično),

- razumijevanje kontrolnih funkcija sa aspekta informacionog sistema i internih kontrola u informacionom sistemu i
- usklađenost sa regulatornim zahtjevima.

Određivanje obima revizije informacionog sistema trebalo bi biti planirno prije same revizije na bazi provedene procjene rizika. Prilikom definisanja obima revizije potrebno je rangirati područja po kriteriju njihove rizičnosti, te u skladu s tim posvetiti pažnju onim dijelovima i resursima informacionog sistema koji su neophodni za funkcionisanje kritičnih/vitalnih poslovnih procesa banke.

7. Ugovorni odnos između banke i Revizora

Ugovor između banke i Revizora trebalo bi jasno definisati sve relevantne uslove, prava i obaveze, te odgovornosti ugovornih strana, pri čemu bi minimalno trebalo da sadrži slijedeće odredbe:

- detaljan opis usluga koje su predmet ugovora,
- oblasti koje će biti pokrivene revizijom,
- imena i prezimena lica koja će operativno provesti reviziju informacionog sistema banke, te njihov ukupan angažman na tim poslovima,
- ukoliko Revizor angažuje podizvođača, potrebno je navesti podatke o podizvođaču i/ili fizičkim licima koji učestvuju u obavljanju operativnog dijela revizije,
- metodologije i procedure koje će Revizor koristiti,
- odgovornost banke i Revizora,
- ograničenje odgovornosti i nadoknada štete i
- obavezu zaštite bankovne i poslovne tajne, te povjerljivosti bančinih podataka.

Kao sastavni dio Ugovora, Revizor je dužan obezbijediti izjavu o nepostojanju sukoba interesa između Revizora, odnosno lica koja operativno provode reviziju, i banke.

8. Provođenje revizije informacionog sistema

8.1. Proces revizije informacionog sistema

Revizija informacionog sistema treba najmanje da:

- identifikuje dijelove informacionog sistema koji podržavaju ključne poslovne procese, te područja najvećeg IT rizika, u svrhu fokusiranja aktivnosti revizije,
- utvrdi primjerenost procesa upravljanja informacionim sistemom pregleda djelovanje kontrolnih funkcija (posebno interne revizije informacionog sistema), voditelja/oficira za sigurnost informacionog sistema, odbora za upravljanje informacionim sistemom i slično),
- procijeni adekvatnost operativnih procesa, i uspostavljenog sistema internih kontrola,
- uzme u obzir eksternalizovane usluge i njihovu značajnost i uticaj na poslovanje Banke, te u skladu s tim, razvije plan revizije i efikasni pristup reviziji i
- uzme u obzir nalaze i preporuke ranije obavljenih revizija urađenih od strane revizorskih društava.

Proces revizije informacionog sistema podrazumijeva i utvrđivanje adekvatnosti upravljanja procesima vezanim uz informacione sisteme (upravljanje incidentima i korisničkim zahtjevima, upravljanje dokumentacijom vezanom za informacione sisteme, upravljanje razvojem i promjenama, upravljanje kontrolama pristupa, upravljanje zaštitom od malicioznog koda, upravljanje resursima informacionog sistema, upravljanje rezervnim kopijama, upravljanje kontinuitetom poslovanja sa aspekta informacionog sistema, fizičke mjere zaštite i tehnička opremljenost prostorija u kojima se nalaze kritični/vitalni resursi informacionog sistema i slično). Adekvatno upravljanje navedenim procesima podrazumijeva postojanje

internih akata koji regulišu upravljanje istim. Postojanje internih akata, kao i njihova adekvatnost, ne znači da su i procesi koje isti regulišu adekvatno uspostavljeni. Zbog navedenog, Revizor bi trebao praktično provjeriti nivo implementiranosti navedenih procesa, odnosno njihovu adekvatnost, i dati objektivnu i realnu ocjenu (mišljenje) o istim.

8.2. Procjena stanja informacionog sistema

U cilju formiranja objektivne i realne ocjene (mišljenja) o stanju informacionog sistema i adekvatnosti upravljanja istim, Revizor treba izvršiti analizu arhitekture informacionog sistema, tehnoloških karakteristika i konfiguracija resursa informacionog sistema. Prethodno navedeno podrazumijeva analizu dizajna mrežne infrastrukture, tehnoloških karakteristika i konfiguracija mrežnih komponenti, analizu i konfiguracije serverskih resursa, analizu i konfiguracije baza podataka, analizu sistema za izradu rezervnih kopija i slično). U skladu sa navedenim, Revizor bi trebao identifikovati one resurse informacionog sistema koji su značajni za odvijanje kritičnih/vitalnih procesa banke, kao i one resurse koji su značajni sa aspekta obezbjeđenja adekvatne sigurnosti informacionog sistema.

8.3. Revizorski alati

Pri obavljanju revizije informacionog sistema, moguće je da Revizor koristi odgovarajuće revizorske alate, a u cilju provjere efikasnosti kontrola ugrađenih u informacioni sistem, utvrđivanja kvalitete podataka i slično. Upotreba revizorskih alata, te obim i način njihove primjene treba biti unaprijed dogovoren sa bankom (prije zaključenja ugovornog odnosa o obavljanju revizije informacionog sistema), s obzirom na moguće negativne posljedice primjene tih alata.

9. Izvještaj o provedenoj reviziji informacionog sistema

9.1. Informacije unutar izvještaja

Revizor treba po završetku revizije pripremiti izvještaj koji treba biti sveobuhvatan, tačan, pouzdan, objektivan, zasnovan na činjenicama, precizan i jasan.

U izvještaju treba naznačiti naziv banke i primaoce, obim, ciljeve, period pokrivenosti revizije, te prirodu i period provođenja revizije. Izvještaj treba uključiti nalaze, rizike i preporuke, te ukoliko postoji suzdržanost Revizora, potrebno je navesti kvalifikacije ili ograničenja u obimu koje je Revizor uočio tokom provođenja revizije.

Revizor treba u izvještaju o provedenoj reviziji informacionog sistema obavezno navesti imena i prezimena osoba koje su operativno provele reviziju informacionog sistema banke, te njihov ukupan angažman na tim poslovima.

Izvještaj bi trebao da sadrži minimalno slijedeće:

- Sažetak izvještaja
- Definisanje obima izvještaja i metodologija
    - Metodologija/e za provođenje revizije (za procjenu rizika i reviziju informacionog sistema)
    - Inicijalna procjena rizika za određivanje obima revizije
    - Oblasti informacionog sistema koje su bile predmet testiranja kontrola
    - Osvrt na prethodni izvještaj revizora informacionog sistema (status preporuka)
- Rezultate procjene rizika
    - Pregled informacionog sistema banke (arhitektura sistema)
    - Primjenjeni postupci procjene rizika
    - Ključne komponente informacionog sistema uključene u obim revizije
- Nalaze o kontrolama u informacionom sistemu
    - Oblast informacionog sistema
    - Zapažanja i rizici

- Ocjena rizika
- Preporuke
- Preporučeni rokovi za implementaciju preporuka

- Ocjene nivoa zrelosti po oblastima informacionog sistema

U sažetku izvještaja o provedenoj reviziji informacionog sistema, trebalo bi izdvojiti najznačajnije nalaze sa pripadajućim nivoima rizika i ukupnu ocjenu o stanju i adekvatnosti upravljanja informacionim sistemom.
Ukoliko su predložene aktivnosti za implementaciju preporuka već diskutovane sa Upravom banke, Revizor treba uključiti ta obrazloženja kao odgovor Uprave u konačnom izvještaju.

9.2. Nalazi, rizici i preporuke

U izvještaju o provedenoj reviziji informacionog sistema treba jasno navesti nalaze, rizike i preporuke za svako testirano područje koje je bilo predmetom revizije.

9.2.1. Nalazi

Revizorski nalaz je pismeno objašnjenje nepravilnosti, slabosti, nedostatka, grešaka ili potreba za poboljšanjima i promjenama koje su otkrivene tokom revizije. Nalaz predstavlja konstruktivan kritički komentar o određenoj radnji ili nepoduzetoj aktivnosti, što prema mišljenju Revizora predstavlja prepreku u ostvarivanju željenih ciljeva na efikasan i efektivan način.
Gdje god je to moguće, Revizor bi trebao razmatrati kumulativni uticaj slabosti ili odsustva kontrola koje se odnose na iste poslovne procese ili resurse, a koji utiču na povećanje ukupnog nivoa rizika informacionog sistema. Takve nalaze bi trebalo međusobno povezati i grupisati, te navesti ukupan rizik koji iz njih proizilazi.
Ako Revizor utvrdi da ne postoje nedostaci ili da su utvrđeni nedostaci od takvog značaja da ih ne treba navesti u izvještaju, informaciju o tome da nisu utvrđeni značajni nedostaci je potrebno navesti u izvještaju. Takvi nalazi trebaju biti adekvatno podržani revizorskim dokazima, baš kao i u slučaju konstatovanja slabosti. U situacijama kada Revizor nije prikupio dovoljno revizorskih dokaza kako bi ispitao i ocijenio određenu oblast informacionog sistema, Revizor treba konstatovati tu činjenicu.
U slučaju postojanja izvještaja drugih vanjskih stručnjaka za specijalizirane oblasti informacionog sistema (npr. penetracioni testovi i slično), Revizor se može referencirati na iste, te u tom slučaju treba procijeniti u kojoj mjeri može koristiti i zasnivati svoju reviziju na radu tih stručnjaka.
Revizorski nalazi trebaju ispunjavati slijedeće:

- jasno identifikovati probleme i nedostatke utvrđene tokom revizije informacionog sistema,
- precizno navesti na koji dio informacionog sistema se odnose ti nalazi (software, hardware, poslovni proces i slično),
- navesti standarde i dobre prakse, specifične politike, procedure ili regulativu na koju se nalaz odnosi,
- opisati okolnosti, zatečeno činjenično stanje i/ili primjere koji podržavaju nalaze,
- biti adekvatno obrazloženi, na objektivan način i u potpunosti podržani revizorskim dokazima i
- biti precizni, dovoljno razumljivi i ubjedljivi.

9.2.2. Rizici

Revizor treba identifikovati i navesti rizike koji proizilaze iz utvrđenih nalaza, te ih obrazložiti na način da banka može na adekvatan način procijeniti mogući uticaj utvrđenih nedostataka na poslovanje banke. Revizor treba navesti uzroke postojeće situacije, kako bi se uočeni nedostaci dovoljno pojasnili. Opis i nivo rizika kojima je izložen informacioni sistem trebali bi jasno upućivati na moguće negativne posljedice na informacioni sistem, te općenito na poslovanje banke. Posljedice najčešće odražavaju potencijalni finansijski gubitak, neusaglašenost, narušavanje kontinuiteta poslovanja, ugroženu sigurnost i slično. Revizor bi trebao objasniti značenja nivoa rizika koje koristi u izvještaju.

9.2.3. Preporuke

Svaki nalaz koji utvrđuje nedostatak, trebao bi da rezultira sa jednom ili više preporuka. Osnovne smjernice za pisanje preporuka su slijedeće:

- preporuka treba da bude stručna i konstruktivna, a sa ciljem poboljšanja upravljanja rizicima,
- preporuka treba biti usmjerena na nadležne osobe ili organizacione jedinice koje su odgovorne ili ovlaštene da preduzmu korektivnu aktivnost,
- ne preporučivati aktivnosti koje su već poduzete; umjesto toga, izvijestiti da su korektivne aktivnosti poduzete,
- ne preporučivati specifična organizaciona i/ili tehnološka rješenja,
- preporuka treba logično da slijedi iz onoga što je predstavljeno u nalazu; ne treba uvoditi nove informacije koje nisu predstavljene u okviru prezentiranog činjeničnog stanja, te izbjegavati davanje općenitih preporuka i
- predložiti rokove za implementaciju preporuka koje se smatraju primjerenim.

Kroz preporuke Revizor treba predložiti kako smanjiti rizike postojeće situacije. Gdje god je to moguće, slični nalazi bi trebali biti grupisani, tako da se naglasi implementacija određene preporuke.

9.3. Ocjena Revizora

Revizor treba dati sveukupnu ocjenu o stanju i adekvatnosti upravljanja informacionim sistemom, te treba upozoriti na značajne rizike kojima je banka izložena. Sveukupna ocjena se daje u sažetku izvještaja.

Ocjena Revizora treba biti opisna i može imati jednu od slijedećih vrijednosti:

- potpuno zadovoljavajuće,
- zadovoljavajuće,
- djelimično zadovoljavajuće,
- nezadovoljavajuće i
- u potpunosti nezadovoljavajuće.

Prilikom davanja ocjene, Revizor je dužan uzeti u obzir i usklađenost poslovanja banke sa Zakonom o bankama, podzakonskim aktima koji se odnose na informacioni sistem (Odluka o minimalnim standardima upravljanja informacionim sistemima u bankama i Odluka o minimalnim standardima upravljanja eksternalizacijom), kao i drugom relevantnom zakonskom regulativom (npr. Zakon o zaštiti ličnih podataka i slično). Prilikom obrazlaganja ocjene, Revizor je dužan navesti činjenice koje su najviše uticale na donošenje ocjene o stanju informacionog sistema i adekvatnosti upravljanja informacionim sistemom.

Za svaku oblast informacionog sistema koja je bila predmet revizije, Revizor treba dati pojedinačnu opisnu ocjenu u skladu sa propisanom metodologijom (npr. ocjene zrelosti u sklopu COBIT metodologije).

10. Uloga banke

10.1. Očitovanje banke o nalazima

Nadležni organi banke trebaju razmatrati izvještaj o provedenoj reviziji informacionog sistema, te se očitovati na iznesene činjenice, komentarisati preporuke i rizike koje je identifikovao Revizor, zatim usaglasiti predložene rokove, kao i odgovornosti za implementaciju navedenih preporuka.

10.2. Upravljanje rizicima

Po zaprimanju konačnog izvještaja revizora, banka treba razmatrati utvrđene nalaze, te procijeniti na koji način se navedeni rizici uklapaju u njen profil rizičnosti. S ciljem poboljšanja upravljanja rizicima, banka

treba procijeniti potrebu provođenja daljih aktivnosti ili prihvatiti navedene rizike. Ukoliko banka procijeni da postoji potreba za provođenjem daljih aktivnosti, potrebno je odrediti koje su to aktivnosti (mjere) koje se trebaju provesti, te definisati rokove i lica odgovorna za provođenje tih aktivnosti, kao i pratiti njihovo izvršenje.

Broj: 03-02-2117/2012

Sarajevo, 13.07.2012. godine

DIREKTOR

Zlatko Barš