SMJERNICE

ZA EKSTERNE REVIZORE ZA OBAVLJANJE REVIZIJE INFORMACIONOG SISTEMA U BANCI

Sarajevo, januar / siječanj 2018. godine

Na osnovu člana 5. stav (1) tačka h) i 23. stav (1) Zakona o Agenciji za bankarstvo Federacije Bosne i Hercegovine („Službene novine Federacije BiH“, broj: 75/17) i člana 16. stav (1) tačka k) Statuta Agenciji za bankarstvo Federacije Bosne i Hercegovine („Službene novine Federacije BiH“, broj: 3/18), direktor Agencije za bankarstvo Federacije Bosne i Hercegovine dana 30.01.2018. godine donosi

SMJERNICE
ZA EKSTERNE REVIZORE ZA OBAVLJANJE REVIZIJE INFORMACIONOG SISTEMA U BANCI

Član 1.
Opće odredbe

(1) Ovim Smjernicama za eksterne revizore za obavljanje revizije informacionog sistema (u daljem tekstu: Smjernice) se daju detaljnije upute u vezi obavljanja eksterne revizije informacionog sistema u bankama, u skladu sa obavezama koje proističu iz Zakona o bankama („Službene novine Federacije BiH“, broj: 27/17), Odluke o upravljanju informacionim sistemom u banci („Službene novine Federacije BiH“, broj: 81/17), Odluke o upravljanju eksternalizacijom u banci („Službene novine Federacije BiH“, broj: 81/17), Odluke o eksternoj reviziji i sadržaju revizije u banci („Službene novine Federacije BiH“, broj: 81/17), Odluke o uslovima i postupku za izdavanje, odbijanje izdavanja i ukidanje saglasnosti za obavljanje bankarskih aktivnosti („Službene novine Federacije BiH“, broj: 90/17), te u skladu sa dobrim praksama.

(2) U skladu sa Zakonom o bankama (u daljem tekstu: Zakon) i podzakonskim aktima navedenim u stavu (1) ovog člana, društva za reviziju (u daljem tekstu: Revizor) su dužna sastaviti izvještaj o obavljenoj reviziji informacionog sistema za potrebe Agencije za bankarstvo Federacije Bosne i Hercegovine (u daljem tekstu: Agencija). Revizorski izvještaj, između ostalog, 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.

(3) Ove Smjernice se odnose na banke i Revizore koji 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.

(4) Agencija očekuje da provođenje revizije, kao i revizorski izvještaj budu u skladu sa Smjernicama 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.

Član 2.
Sastanci predstavnika društva za reviziju i predstavnika Agencije

(1) Predstavnici Agencije i Revizora održavaju sastanke po ukazanoj potrebi, a minimalno jednom godišnje.

(2) Predmet sastanaka su pregledi i analize izvještaja eksterne revizije informacionog sistema za prethodnu godinu, kao i definisanje ciljeva za reviziju informacionog sistema za narednu godinu.

(3) Revizori su obavezni unaprijediti svoje izvještaje u skladu sa preporukama Agencije i pregledati, između ostalog, oblasti informacionog sistema koje Agencija definiše kao kritične za predmetnu godinu.

Član 3.
Revizija informacionog sistema

(1) Revizor daje zasebnu ocjenu o stanju informacionog sistema banke i adekvatnosti upravljanja informacionim sistemom banke, pri čemu je dužan:
   a) služiti se metodama i postupcima za reviziju informacionih sistema temeljenim na procjeni rizika,
   b) definisati obim revizije informacionog sistema na osnovu procjene rizika prije početka obavljanja revizije informacionog sistema,
   c) definisati dubinu revizije informacionog sistema ovisno o zatečenom stanju informacionog sistema,
   d) provjeriti pridržava li se banka podzakonskih akata donesenih na osnovu Zakona, a koji se odnose na informacione sisteme.

(2) Na osnovu revizije informacionog sistema Revizor je dužan ukazati na značajne rizike kojima je banka izložena.

Član 4.
Angažman Revizora

(1) Angažman i procedure odobrenja Revizora informacionog sistema, utvrđene su Odlukom o upravljanju informacionim sistemom u banci, Odlukom o eksternoj reviziji i sadržaju revizije u banci i Odlukom o uslovima i postupku za izdavanje, odbijanje izdavanja i ukidanje saglasnosti za obavljanje bankarskih aktivnosti.

(2) Uslovi i kriteriji koje mora da ispunjava Revizor da bi mogao vršiti reviziju informacionog sistema banke su definisani članom 2. stav (2) Odluke o eksternoj reviziji i sadržaju revizije u banci.

(3) Pri provođenju eksterne revizije informacionog sistema, očekuje se da banka i Revizor primjenjuju standarde koji su utvrđeni odredbama Zakona o računovodstvu i reviziji Federaciji Bosne i Hercegovine, 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 drugo).

(4) Skupština banke, uz prethodnu saglasnost Agencije, imenuje Revizora najkasnije do 30.09. tekuće godine, koje će obaviti reviziju informacionog sistema za tu godinu. Agencija daje prethodnu saglasnost za imenovanje Revizora za obavljanje revizije informacionog sistema na osnovu zahtjeva za izdavanje odobrenja za imenovanje Revizora upućenog od strane banke. Ukoliko dođe do izmjene podataka na osnovu kojih je Revizor dobio saglasnost Agencije, dužno je odmah obavijestiti Agenciju o izmjeni istih.

(5) Izvještaj o obavljenoj reviziji informacionog sistema sa stanjem na dan 31.12. prethodne godine je poseban izvještaj, kojeg je banka dužna dostaviti Agenciji najkasnije do 31.05. tekuće godine. Banka je obavezna Agenciji dostaviti originalan primjerak izvještaja na jednom od jezika koji su u službenoj upotrebi u Federaciji Bosne i Hercegovine.

(6) 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.

Član 5.
Kompetencije osoba koje obavljaju reviziju

(1) 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. Ključni članovi tima koji će

obavljati operativni dio revizije trebaju imati najmanje po dvije godine radnog iskustva, na poslovima eksterne revizije informacionih sistema u bankama.

(2) U svom radu, Revizor treba primjenjivati standarde za reviziju informacionih sistema, zatim druge odgovarajuće profesionalne ili industrijske standarde, kao i regulatorne zahtjeve, koji bi osigurali mogućnost davanja ocjene o stanju informacionog sistema i adekvatnosti upravljanja informacionim sistemom.

(3) 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.

(4) Revizor i angažovana treća lica trebaju biti neovisni, što podrazumijeva da u toku angažmana od strane banke ne mogu imati:
   a) bilo kakav direktan ili indirektan finansijski interes u banci ili kod bilo kog povezanog lica sa bankom i
   b) 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).

Član 6.
Odgovornost Revizora i banke

(1) 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 kompletne 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.

(2) Revizor je odgovoran da, na bazi obavljenog procesa revizije i prikupljenih revizijskih dokaza, obezbijedi izvještaj koji sadrži objektivnu ocjenu o stanju informacionog sistema i adekvatnosti upravljanja informacionim sistemom.

(3) Ukoliko Revizor za vrijeme trajanja angažmana uoči nedostatke, slabosti ili nepravilnosti koje predstavljaju izrazito visoki rizik i koje su istovremeno kritične za sigurnost informacionog sistema Banke, dužan je odmah obavijestiti Agenciju.

Član 7.
Planiranje revizije informacionog sistema

(1) 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.

(2) Pri planiranju i definisanju plana revizije informacionog sistema banke, Revizor bi kao minimum, trebao uzeti u obzir slijedeće:
   a) veličinu banke (tržišnu i finansijsku poziciju i slično),
   b) profil rizičnosti banke, te sklonost preuzimanju rizika,
   c) obim i složenost usluga koje banka pruža,
   d) 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),
   e) tehnološku složenost informacionog sistema (heterogenost software-skih i hardware-skih resursa, obim i složenost mrežne infrastrukture i slično),

f) 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),
g) razumijevanje kontrolnih funkcija sa aspekta informacionog sistema i internih kontrola u informacionom sistemu,
h) aktuelne trendove vezane uz tehnološki napredak (npr.: cyber prijetnje i slično),
i) vremenski period testiranja funkcionalnosti rezervnog informatičkog centra i prisustvo istom,
j) usklađenost sa regulatornim zahtjevima i drugo.

(3) Određivanje obima revizije informacionog sistema trebalo bi biti planirano 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.

Član 8.
Ugovorni odnos između banke i Revizora

(1) Ugovor između banke i Revizora trebao bi jasno definisati sve relevantne uslove, prava i obaveze, te odgovornosti ugovornih strana, pri čemu bi minimalno trebalo da sadrži sljedeće odredbe:
a) detaljan opis usluga koje su predmet ugovora,
b) oblasti koje će biti pokrivene revizijom,
c) imena i prezimena lica koja će operativno provesti reviziju informacionog sistema banke, te njihov ukupan angažman na tim poslovima,
d) ukoliko Revizor angažuje podizvođača, potrebno je navesti podatke o podizvođaču i/ili fizičkim licima koji učestvuju u obavljanju operativnog dijela revizije,
e) metodologije i procedure koje će Revizor koristiti,
f) odgovornost banke i Revizora,
g) ograničenje odgovornosti i nadoknada štete i
h) obavezu zaštite bankovne i poslovne tajne, te povjerljivosti bančinih podataka.

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

Član 9.
Provođenje revizije informacionog sistema

(1) Revizija informacionog sistema treba, kao minimum, da:
a) identifikuje dijelove informacionog sistema koji podržavaju ključne poslovne procese, te područja najvećeg IT rizika, u svrhu fokusiranja aktivnosti revizije,
b) utvrdi primjerenost procesa upravljanja informacionim sistemom, te pregleda djelovanje kontrolnih funkcija (posebno interne revizije informacionog sistema, voditelja/oficira za sigurnost informacionog sistema, odbora za upravljanje informacionim sistemom i slično),
c) procjeni adekvatnost operativnih procesa i uspostavljenog sistema internih kontrola,
d) 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
e) uzme u obzir nalaze i preporuke ranije obavljenih revizija provedenih od strane revizorskih društava za reviziju informacionog sistema.

(2) 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

planom oporavka informacionog sistema, sigurnost informacionog sistema, fizičke mjere zaštite i tehnička opremljenost prostorija u kojima se nalaze kritični/vitalni resursi informacionog sistema, upravljanje operativnim i sistemskim zapisima, cyber sigurnost, upravljanje eksternalizovanim aktivnostima i sl.).

(3) Adekvatno upravljanje procesima iz stava (2) ovog člana 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, te dati objektivnu i realnu ocjenu o istim.

Član 10.
Procjena stanja informacionog sistema

(1) U cilju formiranja objektivne i realne ocjene o stanju informacionog sistema i adekvatnosti upravljanja istim, Revizor treba izvršiti analizu arhitekture informacionog sistema, tehnoloških karakteristika i konfiguracija resursa informacionog sistema.

(2) Navedeno u stavu (1) ovog člana 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.

Član 11.
Upotreba Revizorskih alata

(1) 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.

(2) 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.

Član 12.
Izvještaj o provedenoj reviziji informacionog sistema

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

(2) 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.

(3) 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.

(4) Izvještaj bi trebao da sadrži minimalno slijedeće:
   a) Sažetak izvještaja,
   b) Definisanje obima izvještaja i metodologija:
      1) metodologija/e za provođenje revizije (za procjenu rizika i reviziju informacionog sistema),
      2) inicijalna procjena rizika za određivanje obima revizije,
      3) oblasti informacionog sistema koje su bile predmet testiranja kontrola,
      4) osvrt na prethodni izvještaj revizora informacionog sistema (status preporuka).
   c) Rezultate procjene rizika:

1) pregled informacionog sistema banke (arhitektura sistema),
2) primjenjeni postupci procjene rizika,
3) ključne komponente informacionog sistema uključene u obim revizije.

d) Nalaze o kontrolama u informacionom sistemu:
1) oblast informacionog sistema,
2) zapažanja i rizici,
3) ocjena rizika,
4) preporuke,
5) preporučeni rokovi za implementaciju preporuka.

e) Usklađenost poslovanja banke sa pojedinačnim članovima Odluke o upravljanju informacionim sistemom u banci i Odluke o upravljanju eksternalizacijom u banci,

f) Ocjene nivoa zrelosti po oblastima informacionog sistema.

(5) U sažetku izvještaja o provedenoj reviziji informacionog sistema, trebalo bi izdvojiti najznačajnije nalaze sa pripadajućim nivoima rizika i ukupnu ocjenu o stanju informacionog sistema i adekvatnosti upravljanja informacionim sistemom.

(6) Ukoliko su predložene aktivnosti za implementaciju preporuka već diskutovane sa upravom banke, Revizor treba uključiti ta obrazloženja kao odgovor uprave u konačnom izvještaju.

Član 13.
Nalazi, rizici i preporuke

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

(2) 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.

(3) 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.

(4) 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.

(5) U slučaju postojanja izvještaja drugih vanjskih stručnjaka za specijalizirane oblasti informacionog sistema (npr. penetracioni testovi, izvještaj o reviziji eksternalizovanih aktivnosti kod pružaoca usluga 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.

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

Član 14.

(1) 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.
(2) 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.
(3) 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.

Član 15.

(1) Svaki nalaz koji utvrđuje nedostatak, trebao bi da rezultira sa jednom ili više preporuka. Osnovne smjernice za pisanje preporuka su:
   a) preporuka treba da bude stručna i konstruktivna, a sa ciljem poboljšanja upravljanja rizicima,
   b) preporuka treba biti usmjerena na nadležne osobe ili organizacione jedinice koje su odgovorne ili ovlaštene da preduzmu korektivnu aktivnost,
   c) ne preporučivati aktivnosti koje su već poduzete; umjesto toga, izvijestiti da su korektivne aktivnosti poduzete,
   d) ne preporučivati specifična organizaciona i/ili tehnološka rješenja,
   e) 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
   f) predložiti rokove za implementaciju preporuka koje se smatraju primjerenim.
(2) 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.

Član 16.
Ocjena Revizora

(1) Revizor treba dati sveukupnu ocjenu o stanju informacionog sistema i adekvatnosti upravljanja informacionim sistemom, te treba upozoriti na značajne rizike kojima je banka izložena. Sveukupna ocjena se daje u sažetku izvještaja.
(2) Ocjena Revizora treba biti opisna i može imati jednu od sljedećih vrijednosti:
   a) potpuno zadovoljavajuće,
   b) zadovoljavajuće,
   c) nezadovoljavajuće i
   d) u potpunosti nezadovoljavajuće.
(3) Prilikom davanja ocjene, Revizor je dužan uzeti u obzir i usklađenost poslovanja banke sa Zakonom, podzakonskim aktima koji se odnose na informacioni sistem (Odluka o upravljanju informacionim sistemom u banci i Odluka o upravljanju eksternalizacijom u banci), 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.
(4) 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).
(5) Agencija može od Revizora tražiti dodatne informacije u vezi sa obavljenom revizijom.

(6) Agencija može odbiti ocjenu ako utvrdi da ocjena nije data u skladu sa Zakonom, podzakonskim aktima donesenim na osnovu njega, zakonom kojim se uređuje revizija i pravilima revizorske struke ili ako obavljenom supervizijom poslovanja banke ili na drugi način utvrdi da ocjena nije zasnovana na istinitim i objektivnim činjenicama. U ovom slučaju Agencija može:
   a) zahtijevati od revizora da svoju ocjenu ispravi, odnosno dopuni ili
   b) odbiti ocjenu i zahtijevati od banke da ocjenu daju ovlašteni revizori drugog revizora, a na trošak banke.

(7) Agencija će rješenjem o odbijanju izvještaja o obavljenoj reviziji odnosno rješenjem o odbijanju ocjene utvrditi rok za dostavu novog izvještaja, odnosno nove ocjene revizora.

Član 17.
Uloga Banke

(1) 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.

(2) 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.

(3) 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.

Član 18.
Prijelazne i završne odredbe

Stupanjem na snagu ovih Smjernica, prestaju da važe Očekivanja Agencije za bankarstvo FBiH vezana za obavljanje revizije informacionog sistema u bankama od strane eksternog revizora, broj: 03-02-2117/2012 od 13.07.2012. godine.

Član 19.

Ove Smjernice stupaju na snagu danom donošenja i objavljuje se na službenoj web stranici Agencije.

Broj: 01-262/18
Sarajevo, 30.01.2018. godine

DIREKTOR

Jasmin Mahmuzić s.r.