Sarajevo, 23.05.2012. godine

POJAŠNJENJA I TUMAČENJA AGENCIJE ZA BANKARSTVO FBIH

ODGOVORI NA UPITE BANAKA U VEZI ODLUKE O MINIMALNIM STANDARDIMA UPRAVLJANJA INFORMACIONIM SISTEMIMA U BANKAMA I ODLUKE O MINIMALNIM STANDARDIMA UPRAVLJANJA EKSTERNALIZACIJOM

I. Odgovori na upite banaka u vezi Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama

Pitanje banke: Eksterna revizija informacionog sistema

Član 13 Odluke o minimalnim standardima za upravljanje informacionim sistemima zahtjeva od banaka da imenuju nezavisnog eksternog revizora za reviziju informacionog sistema. Vezano uz ovaj član molili bismo pojašnjenje vezano za obim revizije koji je banka obavezna tražiti od eksternog revizora.

Pojašnjenje Agencije:

Prilikom revizije informacionog sistema, eksterni revizor je dužan uraditi procjenu rizika informacionog sistema, te u skladu sa procjenom rizika razviti plan revizije i obaviti samu reviziju informacionog sistema. Agencija će uskoro objaviti detaljnija uputstva odnosno smjernice koje se odnose na izvještaje i eksternu reviziju informacionih sistema u bankama.

Obim revizije informacionog sistema, osim oblasti koje će biti definisane na osnovu predložene procjene rizika, trebaju obavezno obuhvatiti i reviziju djelovanja kontrolnih funkcija u oblasti informacionog sistema (npr. interne IT revizije, oficira za sigurnost i sl), te ostale oblasti pokrivene Odlukom o minimalnim standardima upravljanja informacionim sistemima u bankama.

Eksterna revizija Banke dužna je uzeti u obzir eksternalizovane usluge i njihovu značajnost i uticaj na poslovanje Banke, te u skladu s tim, razviti plan revizije i efikasni pristup reviziji.

Pitanje banke: Odgovorno lice za sigurnost informacionog sistema

U procesu smo implementacije Odluke o minimalnim standardima za upravljanje informacionim sistemom, te vas molimo za pojašnjenja i odgovore na neka pitanja vezana za član 10. Odgovorno lice za sigurnost informacionog sistema. U Odluci stoji da funkcija sigurnosti infromacionog sistema treba biti nezavisna od funkcije organizacijske jedinice za upravljanje informacionim sistemom.

1. Da li to znači da ovu funkciju ne može obavljati zaposlenik IT Odjela?
2. Da li su i male banke dužne izdvajati ovu funkciju odmah na početku, što može biti preskupo?

3. Ukoliko se funkcija mora izdvojiti, koje još poslove može obavljati ova osoba, da ne bi došlo do sukobljavanja dužnosti, a kako bi ispunila radnu normu (opis i obim poslova ove funkcije ne ispunjava 8 sati dnevnog rada)?
4. Ukoliko se funkcija izdvaja iz IT Odjela kome ona pripada i da li je odgovorna direktno Upravi Banke?

Pojašnjenje Agencije:

1. U skladu sa članom 10 navedene Odluke, funkcija sigurnosti informacionog sistema treba biti nezavisna od funkcije organizacijske jedinice za upravljanje informacionim sistemom i samim tim navedena osoba ne može biti uposlenik IT Odjela.
2. Sve banke su dužne uspostaviti funkciju odgovornog lica za sigurnost informacionog sistema u roku 12 mjeseci od dana stupanja na snagu navedene Odluke.
3. Prije svega, prilikom popunjavanja ove radne pozicije, Banka treba voditi računa da se radi o odgovornoj funkciji za koju su potrebna specifična znanja i razumijevanja o informacionom sistemu. Banka treba sama procijeniti koji su to dodatni poslovi koje bi mogla dodijeliti osobi odgovornoj za sigurnost informacionog sistema, vodeći računa o nespojivosti poslova i neovisnosti od organizacijske jedinice za upravljanje informacionim sistemom. Naprimjer, dodatni poslovi mogu biti poslovi vezani za upravljanje rizicima, upravljanje kontinuitetom poslovanja Banke, opšti poslovi i sl.
4. Kao što je naglašeno u odgovoru za pitanje 1, navedena funkcija treba biti odvojena od IT Odjela. Banka treba sama definisati organizacionu poziciju ove funkcije. Član 11 Odluke nalaže da lice odgovorno za sigurnost redovno izvještava Upravu Banke.

II. Odgovori na upite banaka u vezi Odluke o minimalnim standardima upravljanja eksternalizacijom

Pitanje banke: Eksternalizacija kod članice grupacije

Odluka o minimalnim standardima za upravljanje eksternalizacijom daje mogućnost da se neke od aktivnosti koje banke mogu obavljati mogu prebaciti na kompanije članice grupacije. U tom smislu, molili bismo za pojašnjenje da li se usluge koje za banku obavljaju kompanije članice grupacije posmatraju kao i ostale eksternalizovane usluge ili drugačije. Ako se kompanije članice grupacije posmatraju drugačije u odnosu na ostale vanjske dobavljače, molili bi za pojašnjenje koji je tretman takvih dobavljača.

Pojašnjenje Agencije:

Članom 2. navedene Odluke definišu se mogući pružaoci usluga (članica grupe banke, pravno lice ili fizičko lice). Cijela odluka se odnosi na sve navedene pružaoce usluga, pa tako i na članice grupe banke.

Pitanje banke: Razlike u tretiranju postojeće i buduće eksternalizacije

Odluka o minimalnim standardima za upravljanje eksternalizacijom definiše niz aktivnosti koje je neophodno provesti za svaku eksternalizovanu aktivnost od momenta procjene rizika eksternalizacije, preko odabira vanjskog dobavljača i ugovaranja same eksternalizacije, pa sve do potencijalnog raskida ugovora. Imajući u vidu činjenicu da je banka svoje ugovore o eksternalizaciji zaključila prije donošenja Odluke, molimo za pojašnjenje da li postoji razlika u obimu aktivnosti koje je banka obavezna provesti vezano za usluge koje su ranije bile eksternalizovane i one koje tek treba ili se planira da se eksternalizuju.

Pojašnjenje Agencije:

Agencija prihvata postojeće stanje eksternalizovanih aktivnosti, te se pravi razlika u odnosu na obim aktivnosti koje je potrebno sprovesti za postojeće i za buduće aktivnosti. Odluka se u potpunosti treba primjeniti na buduće eksternalizovane aktivnosti. Za aktivnosti koje su eksternalizovane prije donošenja ove odluke, potrebno je uraditi slijedeće:

- u skladu sa članom 24, Banka je dužna da procijeni sve materijalno značajne aktivnosti i da o tome obavijesti Agenciju u roku od 6 mjeseci od dana stupanja na snagu Odluke,
- Ugovore o eksternalizaciji materijalno značajnih aktivnosti, potrebno je uskladiti sa odredbama Odluke u roku od 12 mjeseci od dana stupanja na snagu Odluke,
- Dokumente koji se navode u članu 18 nije potrebno dostavljati Agenciji, ali je Banka dužna da se uskladi sa članom 18 u mjeri u kojoj je to primjenjivo, što će se procijenjivati u kontroli i
- Banka je dužna kontinuirano upravljati rizicima svih eksternalizovanih aktivnosti.

Pitanje banke: Eksternalizacija IT ili svih usluga

Član 7 Odluke o minimalnim standardima za upravljanje eksternalizacijom definiše obavezu banke da prijavi eksternalizovane usluge. Vezano za ovu temu molili bismo za pojašnjenje, da li se pod eksternalizovanim uslugama u ovom članu podrazumijevaju samo IT povezane usluge ili je regulator mislio na širi obim eksternalizovanih usluga koje banka može i/ili eksternalizuje.

Pojašnjenje Agencije:

Odluka o minimalnim standardima upravljanja eksternalizacijom se odnosi na sve usluge koje je banka eksternalizovala, a koje se definišu pod eksternalizacijom (vidjeti izuzetak u članu 1 stav (2)). Definicija eksternalizacije je data u članu 2.
U navedenoj Odluci, članom 24 stav (1) na koji ste vjerovatno mislili (naveli ste član 7 u Vašem dopisu) je propisana obaveza Banke da sve materijalno značajne aktivnosti, koje su eksternalizovane prije stupanja na snagu ove Odluke procijeni i da o tome obavijesti Agenciju. Dakle, obavijest je potrebno poslati za sve materijalno značajne aktivnosti, a ne samo za materijalno značajne IT aktivnosti.

Pitanje banke: Odluka o eksternalizaciji

U slučaju da reviziju informacionih sistema vrši članica iste grupacije (član 3 tačka 5 Odluke o eksternalizaciji), takva aktivnost čak i ako se ocijeni kao „materijalno značajna“ dozvoljena je po samoj odluci (član 7, tačka (2) 1).

1. Da li je u ovom slučaju neophodna Odluka Nadzornog odbora o eksternalizaciji (član 17 Odluke) i sva dokumentacija iz člana 18?
2. Ako se ovakva aktivnost ne ocjeni materijalno značajnom, onda odluku ne donosi Nadzorni odbor i Agenciji se dostavlja samo obavijest bez propisane dokumentacije.
3. Koji je rok za donošenje internih akata iz člana 12 i 13 Odluke s obzirom da Odlukom nije predviđen, a ista je stupila na snagu 8 dana nakon objavljivanja?

Pojašnjenje Agencije:

1. Ukoliko Banka namjerava eksternalizovati aktivnost interne revizije, a koja se odnosi na reviziju informacionog sistema (član 3 stav (5) Odluke o minimalnim standardima upravljanja eksternalizacijom) neophodna je odluka Nadzornog Odbora o istom.
2. Obzirom da obavljanje interne revizije potpada pod materijalno značajne aktivnosti neophodno je obavijestiti Agenciju o eksternalizaciji interne revizije, a koja se odnosi na reviziju informacionih sistema (član 3 stav (5) Odluke o minimalnim standardima upravljanja

eksternalizacijom), te dostaviti dokumentaciju propisanu članom 18 Odluke o minimalnim standardima upravljanja eksternalizacijom.

3. Član 12 i 13 Odluke o minimalnim standardima upravljanja eksternalizacijom stupaju na snagu osmog dana od dana objavljivanja gore navedene Odluke u „Službenim novinama Federacije BiH“. Agencija će imati razumijevanje da se Banka u primjerenom roku uskladi sa regulativom i cijeniće sve poduzete aktivnosti koje je Banka poduzela u cilju usklađivanja sa istom.

Pitanje banke: Eksternalizacija usluga razvijanja i održavanja korisničkih rješenja

U postupku usklađivanja poslovanja banke sa odredbama Odluke o minimalnim standardima upravljanja eksternalizacijom, vezano za definisanje aktivnosti na koje se primjenjuju odredbe predmetne Odluke, za pojedine aktivnosti postoji nedoumica da li se na njih u slučaju eksternalizacije primjenjuju odredbe ove Odluke ili ne.

Konkretno se radi o slijedećim aktivnostima:

- Usluge razvijanja i održavanja aplikativnih korisničkih rješenja.

Pojašnjenje Agencije:

Članom 7 Odluke o minimalnim standardima upravljanja eksternalizacijom je navedeno da su materijalno značajne aktivnosti one aktivnosti za koje se na osnovu procjene uticaja eksternalizacije utvrdi da su od takvog značaja da bilo kakva slabost ili greška u pružanju tih aktivnosti može imati značajan uticaj na mogućnost banke da zadovolji regulatorne zahtjeve i/ili nastavi svoje poslovanje i da može imati značajan uticaj na upravljanje rizicima. S tim u vezi, Agencija će, između ostalog, smatrati materijalno značajnom eksternalizaciju usluge razvijanja i održavanja ključne bankarske aplikacije, odnosno onih aplikacija koje joj omogućavaju obavljanje djelatnosti pružanja bankovnih ili finansijskih usluga za koje je banka dobila bankarsku dozvolu i ovlaštenje od Agencije. Kako za ključnu bankarsku aplikaciju, tako i za sve ostale aplikacije i/ili module, banka je dužna sama procijeniti materijalnu značajnost i uticaj eksternalizacije u skladu sa članom 6 Odluke o minimalnim standardima upravljanja eksternalizacijom, kao i prateće rizike, ovisnost o vanjskom pružaocu usluga i mogućnost nastavka poslovanja, te u skladu s tim donijeti odluku o eksternalizaciji.

Pitanje banke: Eksternalizacija usluga odvjetničkih ureda za vođenje sudskih postupaka za naplatu potraživanja banke

U postupku usklađivanja poslovanja banke sa odredbama Odluke o minimalnim standardima upravljanja eksternalizacijom, vezano za definisanje aktivnosti na koje se primjenjuju odredbe predmetne Odluke, za pojedine aktivnosti postoji nedoumica da li se na njih u slučaju eksternalizacije primjenjuju odredbe ove Odluke ili ne. Konkretno se radi o aktivnostima angažmana odvjetničkih ureda za vođenje sudskih postupaka za naplatu potraživanja banke.

Pojašnjenje Agencije:

Angažman odvjetničkih ureda za vođenje sudskih postupaka za naplatu potraživanja banke, iako nisu precizno definisane razlike između eksternalizovanih aktivnosti i zastupničkih poslova, bi po svojoj suštini više spadali u zastupničke poslove i po tom osnovu na njih se ne primjenjuje Odluka o minimalnim standardima upravljanja eksternalizacijom. S tim u vezi, postavlja se pitanje da li banka pravne poslove obavlja sama i u kolikoj mjeri, odnosno da li kompletnu aktivnost ili njen veći dio povjerava vanjskom pružaocu usluga, u ovom slučaju odvjetničkom uredu, što bi se smatralo eksternalizovanom aktivnošću. Međutim, pošto ne znamo o kakvom se konkretnom angažmanu sa odvjetničkim uredom radi, banka je dužna sama procijeniti da li se radi o uobičajenom angažmanu koji bi po tom osnovu spadao u zastupničke poslove ili iz samog ugovora proizilaze i neki drugi elementi, koji mogu predstavljati aktivnosti eksternalizacije (npr. prodaja kolaterala i dr.).