

Na osnovu čl. 75., 77. i 78. Zakona o bankama ("Službene novine Federacije BiH", broj 27/17), čl. 5. stav (1) tačka h) i 19. stav (1) tačka c) Zakona o Agenciji za bankarstvo Federacije Bosne i Hercegovine ("Službene novine Federacije BiH", broj 75/17) i člana 12. stav (1) tačka d) Statuta Agencije za bankarstvo Federacije Bosne i Hercegovine ("Službene novine Federacije BiH", broj 3/18), Upravni odbor Agencije za bankarstvo Federacije Bosne i Hercegovine, na sjednici održanoj 13.09.2022. godine donosi

ODLUKU O UPRAVLJANJU EKSTERNALIZACIJOM U BANCIMA

Član 1.

Predmet

- (1) Odlukom o upravljanju eksternalizacijom u banci propisuju se uslovi koje je banka dužna da osigura u postupku provođenja i upravljanja eksternalizacijom i rizicima koji mogu proisteći iz eksternalizacije, kao i usluge koje ne mogu biti predmetom eksternalizacije, pojam materijalno značajnih aktivnosti, uslovi za eksternalizaciju, te sadržaj dokumentacije uz obavijest i rokove za dostavu obavijesti o eksternalizaciji materijalno značajnih aktivnosti.
- (2) Ova odluka primjenjuje se na banke sa sjedištem u Federaciji Bosne i Hercegovine (u daljem tekstu: FBiH) kojima je Agencija za bankarstvo Federacije Bosne i Hercegovine (u daljem tekstu: Agencija) izdala dozvolu za rad.
- (3) Banka je dužna primjenjivati odluku na pojedinačnoj i konsolidovanoj osnovi.
- (4) Na pitanja vezana za upravljanje eksternalizacijom i rizicima koji mogu proisteći iz eksternalizacije koja nisu regulisana ovom odlukom, a regulisana su drugim propisima, primjenjivati će se odredbe tog propisa.

Član 2.

Pojmovi - Definicije

- (1) Pojedini pojmovi koji se koriste u ovoj odluci imaju sljedeće značenje:
 - a) **Eksternalizacija** (eng. outsourcing) je ugovorno povjeravanje obavljanja određenih aktivnosti od strane banke pružaocima usluga, a koje bi banka inače obavljala sama.
 - b) **Aktivnosti koje bi banka inače obavljala sama** su aktivnosti koje banci omogućavaju obavljanje djelatnosti pružanja bankarskih i finansijskih usluga, uključujući i aktivnosti kojima se podržava obavljanje tih djelatnosti.
 - c) **Rizik eksternalizacije** uključuje sve rizike koji nastaju kada banka ugovorno povjerava pružaocima usluga obavljanje aktivnosti koje bi inače sama obavljala.
 - d) **Pružalac usluga** je treća strana koja obavlja određenu eksternalizovanu aktivnost djelimično ili u cjelini na osnovu ugovora zaključenog sa bankom, a može biti:
 - 1) članica bankarske grupe,
 - 2) pravno lice koje je prema propisima države u kojoj je osnovano, odnosno u kojoj ima sjedište ovlašteno za obavljanje djelatnosti koje je predmet eksternalizacije ili
 - 3) fizičko lice koje je prema propisima države u kojoj ima prebivalište ovlašteno za obavljanje djelatnosti koje je predmet eksternalizacije.
 - e) **Podesternalizacija** je situacija u kojoj pružalac usluga, u okviru određenog ugovora o eksternalizaciji, eksternalizovanu uslugu ili neki njen dio povjerava nekom drugom pružaocu usluga, koji se u tom slučaju označava kao podizvođač pružaoca usluge (u daljem tekstu: podizvođač).
 - f) **Usluge računarstva u oblaku** (eng. cloud services) su usluge u kojima se na zahtjev omogućava široko rasprostranjen, pogodan mrežni pristup zajedničkom skupu prilagodljivih resursa informacionog sistema (npr. mreže, serveri, uređaji za skladištenje

podataka, aplikacije i usluge), a koji se mogu trenutno pribaviti i otpustiti uz minimalnu upravljačku aktivnost ili prisutnost pružaoca usluge. Razlikuju se tri tipa usluga računarstva u oblaku (infrastruktura kao usluga – IaaS, platforma kao usluga – PaaS i software kao usluga – SaaS) i četiri modela računarstva u oblaku (javni, privatni, zajednički i hibridni).

- g) **Javni oblak** (eng. public cloud) jeste računarska infrastruktura kojoj može pristupiti šira javnost.
 - h) **Privatni oblak** (eng. private cloud) jeste računarska infrastruktura kojoj može pristupiti samo jedan subjekt.
 - i) **Zajednički oblak** (eng. community cloud) jeste računarska infrastruktura raspoloživa samo određenom broju subjekata.
 - j) **Hibridni oblak** (eng. hybrid cloud) jeste računarska infrastruktura koja je sastavljena od dvije ili više različitih računarskih infrastruktura u oblaku (npr. javni i privatni).
 - k) **Penetracioni test** (eng. penetration testing) predstavlja specijaliziranu vrstu procjene koja se provodi na informacionom sistemu ili njegovim pojedinim dijelovima, a sa ciljem identifikacije i validacije ranjivosti koje bi napadači mogli iskoristiti.
 - l) **Organi banke** u smislu ove odluke su: „nadzorni odbor“ i „uprava banke“.
 - m) **Sporazum o nivou usluga** (eng. Service Level Agreement SLA) predstavlja formalni ugovor kojim se definiše nivo kvaliteta usluge koju banka očekuje od pružaoca usluge.
- (2) Pojmovi koji se koriste u ovoj odluci, a nisu definisani u istoj, imaju značenje kao u Zakonu o bankama i drugim podzakonskim aktima Agencije u kojima su definisani.

Član 3.

Aktivnosti koje ne predstavljaju eksternalizaciju

U smislu ove odluke, eksternalizacijom se ne smatraju:

- a) aktivnosti koje po zakonu obavlja pružalac usluga (npr. eksterna revizija),
- b) usluge globalnih servisa za međubankarsku/finansijsku komunikaciju (npr. SWIFT) u slučaju kada se ključni resursi informacionog sistema potrebni za pružanje navedene usluge nalaze unutar banke i koji podliježu nadzoru relevantnih tijela,
- c) usluge pružanja informacija o tržištu (npr. podaci koje pružaju društva Bloomberg, Moody's, Standard & Poor's, Fitch, Reuters),
- d) usluge globalne mrežne infrastrukture (Visa, MasterCard i sl.),
- e) usluge korespondentnog bankarstva,
- f) sistemi poravnanja i usluge namirenja između klirinških kuća, središnjih drugih ugovornih strana, te institucija za namirenje i njihovih članica,
- g) zakup i nabavka robe,
- h) druge aktivnosti koje banka inače ne obavlja sama (npr. arhitektonske usluge, usluge čišćenja, usluge održavanja objekata, usluge sigurnosti imovine i lica, usluge osiguranja imovine i lica, usluge fizičke, tehničke zaštite i transporta novca, servisno održavanje službenih automobila, ugostiteljske usluge, automati za prodaju, uredski poslovi, putničke usluge, poštanske usluge, recepcionarske usluge, komunalne usluge, pružanje pravnih mišljenja i pružanje ostalih savjetodavnih mišljenja na ad-hoc osnovi različitim funkcijama banke za teme i oblasti rada koje banka ne obavlja ili za koje, zbog male učestalosti potrebe za istim, nije racionalno osiguranje stalnih internih kapaciteta unutar banke (npr. savjetodavno-konsultantska mišljenja konsultantskih kuća i/ili drugih članica bankarske grupe i sl.) i zastupanje na sudu i pred upravnim tijelima, usluge oglašavanja i ispitivanja tržišta, zdravstvene usluge, telefonske usluge, pribavljanje dobara (npr. plastičnih kartica, čitača kartica, uredskog pribora, osobnih računara, namještaja i dr.), izvršenje radova, nabavku robe i usluga, usluge vezane uz upotrebu telekomunikacijske infrastrukture i slično).

Član 4.

Uslovi za eksternalizaciju

- (1) Banka smije eksternalizovati aktivnosti koje joj omogućavaju obavljanje djelatnosti pružanja bankarskih i finansijskih usluga, uključujući i aktivnosti kojima se podržava obavljanje tih djelatnosti, pod uslovima utvrđenim Zakonom, ako eksternalizacija ne narušava:
 - a) obavljanje redovnog poslovanja banke, odnosno pružanje usluga korisnicima u skladu sa važećim zakonskim i drugim propisima, te dobrom bankarskom praksom,
 - b) upravljanje i nadzor nad poslovanjem i aktivnostima banke, uključujući i nad aktivnostima koje su eksternalizovane,
 - c) efikasno upravljanje rizicima banke, uključujući rizike informacione i komunikacijske tehnologije (u daljem tekstu: IKT) i rizike finansijske tehnologije (FinTech),
 - d) sistem internih kontrola i kontrolne funkcije banke,
 - e) obavljanje nadzora od strane Agencije nad eksternalizovanim aktivnostima na lokacijama na kojima će se pružati eksternalizovane usluge, pohranjivati i obrađivati podaci,
 - f) mogućnost provedbe izlazne strategije za eksternalizovane aktivnosti, koja uključuje jednu od sljedećih mjera u odgovarajućem primjerenom roku: prenos aktivnosti na drugog pružaoca usluge, ponovnu integraciju procesa i aktivnosti u banku ili prestanak poslovne aktivnosti.
- (2) Banka ne smije eksternalizovati djelatnost pružanja bankarskih i finansijskih usluga za koje je dobila dozvolu za rad i ovlaštenje od strane Agencije u skladu sa važećim propisima, osim u slučajevima koji su propisani drugim zakonima i propisima i ovom odlukom.
- (3) Banka ugovorima o eksternalizaciji ne smije delegirati ili prenijeti prava i obaveze organa banke koje su definisane Zakonom.
- (4) Banka ostaje potpuno odgovorna i zadužena za osiguravanje usklađenosti sa svim svojim zakonskim i regulatornim obavezama, uključujući sposobnost nadziranja eksternalizovanih aktivnosti.
- (5) Banka ne smije eksternalizovati kontrolne funkcije banke koje su definisane Zakonom, osim aktivnosti podrške kontrolnim funkcijama, na način na koji je to definisano unutar bankarske grupe i u čl. 5. i 6. ove odluke.
- (6) Odgovornost banke prema trećim licima ni u kojem slučaju se ne smije prenositi na pružaoce usluga.

Član 5.

Primjena unutar bankarske grupe

- (1) U slučaju eksternalizacije aktivnosti na nivou bankarske grupe ili podgrupe, bez obzira da li je pružalac usluga član bankarske grupe ili ne, organi banke zadržavaju punu odgovornost za efikasnu primjenu ove odluke i usklađivanje navedene eksternalizacije sa svim zakonskim i regulatornim zahtjevima.
- (2) U svrhu primjene stava (1) ovog člana, banka koja je članica bankarske grupe ili podgrupe, dužna je osigurati da su sistemi, postupci i mehanizmi upravljanja eksternalizacijom dosljedno primijenjeni, pravilno integrisani i primjereni za efikasnu primjenu regulatornih zahtjeva iz ove odluke na svim relevantnim nivoima.
- (3) U slučaju eksternalizacije aktivnosti podrške kontrolnim funkcijama u okviru iste bankarske grupe odnosno podgrupe, a u skladu sa članom 4. stav (5) ove odluke, banka treba osigurati, za potrebe praćenja provođenja i revizije ugovora o eksternalizaciji, uspješno provođenje tih aktivnosti, uključujući i putem odgovarajućih izvještaja.
- (4) U slučaju eksternalizacije materijalno značajne aktivnosti banke na nivou bankarske grupe odnosno podgrupe čiji je banka član, a pri čemu je operativno praćenje eksternalizacije centralizirano:
 - a) banka je dužna osigurati mogućnost nezavisnog provođenja praćenja pružaoca usluga i odgovarajući nadzor, uključujući primanje izvještaja o praćenju eksternalizacije, barem

- jednom godišnje odnosno na zahtjev, sa sažetkom procjene rizika i praćenja izvršavanja, kao i sažetak relevantnih revizorskih izvještaja, a u slučaju zahtjeva, potpuni revizorski izvještaj, (osiguravajući pri tome da procjena rizika i nadzor eksternalizovanih aktivnosti obuhvataju elemente definisane članom 16. i 26. ove Odluke),
- b) banka treba osigurati da organi banke budu pravovremeno obaviješteni o relevantnim planiranim promjenama u pogledu pružanja eksternalizovane usluge, te o mogućem uticaju tih promjena na materijalno značajne aktivnosti banke koje su predmet eksternalizacije, uključujući sažetak analize rizika, među ostalim pravnih rizika, usklađenost s regulatornim zahtjevima i nivoom usluge, a kako bi se mogao procijeniti uticaj tih promjena,
 - c) u slučaju da se na nivou bankarske grupe ili podgrupe provodi centralna procjena rizika prije eksternalizacije, banka treba imati sažetak procjene i uvjeriti se da procjena uzima u obzir specifičnu strukturu i rizike banke, kao i da je procjena rizika u skladu sa članom 15. i 16. ove Odluke,
 - d) u slučaju oslanjanja na izlazni plan koji je uspostavljen na nivou bankarske grupe ili podgrupe, banka treba imati sažetak plana i uvjeriti se da se plan može uspješno provesti,
 - e) banka treba navedenu eksternalizaciju voditi u okviru registra informacija o eksternalizovanim aktivnostima banke, a koji je definisan članom 14. ove odluke.
- (5) U slučaju eksternalizacije aktivnosti na nivou bankarske grupe ili podgrupe čiji je banka član, Agencija zadržava mogućnost obavljanja nadzora eksternalizovanih aktivnosti, u skladu sa zaključenim sporazumom o saradnji i razmjeni informacija između Agencije i nadležnih tijela odgovornih za nadzor pružaoca usluga, banke/bankarske grupe u matičnoj zemlji.

Član 6.

Materijalno značajne aktivnosti

Materijalno značajne aktivnosti su:

- a) aktivnosti od takvog značaja da bilo kakva slabost ili greška u obavljanju tih aktivnosti može imati značajan uticaj na mogućnost banke da zadovolji zakonske i regulatorne zahtjeve i/ili nastavi svoje poslovanje, odnosno pružanje bankarskih/finansijskih usluga,
- b) aktivnosti koje mogu imati značajan uticaj na upravljanje rizicima, sistem internih kontrola i finansijski rezultat banke,
- c) aktivnosti koje omogućavaju banci obavljanje osnovnih poslovnih linija i ključnih funkcija, u skladu sa propisima Agencije koji se odnose na restrukturiranje banaka i sadržaj plana oporavka banke,
- d) sve aktivnosti vezane za podršku kontrolnim funkcijama, u skladu sa članom 4. stav (5) ove odluke,
- e) sve bankarske i finansijske aktivnosti u mjeri za koju bi bilo potrebno odobrenje za rad Agencije.

Član 7.

Procjena materijalne značajnosti

- (1) Prilikom procjene da li je aktivnost koja se eksternalizuje materijalno značajna, banka je dužna, pored procjene rizika iz člana 16. ove odluke, uzeti u obzir i sljedeće:
- a) da li je eksternalizacija direktno povezana sa pružanjem bankarskih odnosno finansijskih usluga i obavljanjem poslova za koje je banka dobila dozvolu za rad,
 - b) mogući uticaj bilo kakvog prekida eksternalizovane aktivnosti ili nemogućnost pružaoca usluga da kontinuirano i na adekvatan način vrši eksternalizovane aktivnosti na:
 - 1) kratkoročnu i dugoročnu finansijsku otpornost i održivost, uključujući, ako je primjenjivo, njenu imovinu, kapital, troškove, izvore finansiranja, likvidnost, dobit i gubitak,
 - 2) kontinuitet poslovanja banke i operativnu otpornost,

- 3) operativni rizik, uključujući rizik nesavjesnog poslovanja (eng. conduct risk), rizik IKT-a, te pravni rizik,
 - 4) reputacijski rizik,
 - 5) plan oporavka i restrukturiranja, mogućnost restrukturiranja i kontinuitet poslovanja banke u situaciji rane intervencije, oporavka ili restrukturiranja,
- c) mogući uticaj eksternalizacije na sposobnost banke da:
 - 1) identifikuje i prati sve rizike te upravlja njima,
 - 2) ispunjava sve zahtjeve propisane zakonskim propisima i podzakonskim aktima i
 - 3) provodi reviziju eksternalizovanih aktivnosti,
 - d) mogući uticaj na usluge koje banka pruža klijentima,
 - e) sve eksternalizacije, ukupnu izloženost banke prema istom pružaocu usluga i mogući kumulativni efekat eksternalizacije koja se odnose na isto područje poslovanja,
 - f) veličinu i složenost područja poslovanja obuhvaćenog eksternalizacijom,
 - g) mogućnost prilagođavanja predloženog ugovora o eksternalizaciji odnosno povećanje eksternalizovane aktivnosti bez izmjene ili dopune osnovnog ugovora,
 - h) mogućnost prenosa, ugovorno i u praksi, eksternalizacije na drugog pružaoca usluga ako je to potrebno ili poželjno, uključujući procijenjene rizike, prepreke za osiguranje kontinuiteta poslovanja, troškove i vremenski okvir u kojem to treba učiniti („zamjenjivost”),
 - i) okolnosti koje mogu dovesti do toga da aktivnost koja inicijalno nije procijenjena kao materijalno značajna naknadno postane materijalno značajna,
 - j) mogućnost vraćanja eksternalizovane aktivnosti unutar banke, ako je to potrebno ili poželjno,
 - k) zaštitu podataka i mogući uticaj povrede povjerljivosti ili propusta u osiguranju dostupnosti i integriteta podataka na banku i njene klijente.
- (2) Agencija može zahtijevati od banke da aktivnosti koje banka nije ocijenila materijalno značajnim ocijeni kao takve, ako utvrdi da ispunjavaju neki od kriterija navedenih u članu 6. ove odluke i stavu (1) ovog člana.
 - (3) Banka smije eksternalizovati materijalno značajne aktivnosti pružiocima usluga definisanim u članu 2. stav (1) tačka d) alineja 1) i 2) ove odluke.

Član 8.

Uspostava sistema za upravljanje rizikom eksternalizacije

- (1) Banka je dužna da, kao dio sveobuhvatnog okvira i mehanizama interne kontrole i sistema upravljanja rizicima, uspostavi efikasno upravljanje rizikom eksternalizacije.
- (2) Ispunjenje zahtjeva iz stava (1) ovog člana omogućava banci donošenje adekvatnih odluka o preuzimanju rizika eksternalizacije i osigurava provođenje adekvatnih mjera za upravljanje rizikom eksternalizacije, uključujući rizike povezane sa kibernetičkim napadima koji se smatraju sigurnosnim aspektom rizika IKT-a.

Član 9.

Sistem za upravljanje rizikom eksternalizacije

- (1) Banka je dužna, uzimajući u obzir princip proporcionalnosti, identifikovati, procijeniti i pratiti sve rizike koji proizilaze iz ugovora sa trećim stranama, kojima jesu ili bi mogle biti izložene, bez obzira da li ugovor predstavlja eksternalizaciju ili ne, te upravljati tim rizicima. Rizike koje proizilaze iz ugovora sa trećim stranama, uključujući i IKT i kibernetičke rizike, treba procijeniti u skladu sa članom 16. ove odluke.
- (2) Upravljanje rizicima koji proizilaze iz ugovora sa trećim stranama treba biti sastavni dio internog sistema upravljanja rizicima banke, u skladu sa propisima Agencije koji regulišu oblast upravljanja rizicima u bankama, kao i propisima vezanim za zaštitu ličnih podataka klijenta banke.

- (3) Banka je dužna uspostaviti efikasan sistem upravljanja eksternalizacijom i rizikom eksternalizacije, srazmjeran profilu rizičnosti, vrsti i poslovnom modelu, veličini i složenosti poslova banke, kao i složenosti eksternalizovanih aktivnosti i rizika koji proizilaze iz eksternalizacije.
- (4) Eksternalizacija aktivnosti ne smije smanjiti zahtjeve u pogledu adekvatnosti članova organa banke, kao i nositelja ključnih funkcija. Banka je dužna osigurati da članovi organa banke imaju vještine i sposobnosti koje osiguravaju adekvatno upravljanje i nadzor nad eksternalizovanim aktivnostima, te da eksternalizovane aktivnosti budu na adekvatan način obuhvaćene sistemom internih kontrola banke.
- (5) Banka je dužna:
 - a) uspostaviti odgovarajuću podjelu nadležnosti, te jasno dodijeliti odgovornosti za dokumentovanje, upravljanje i kontrolu ugovora o eksternalizaciji,
 - b) osigurati dovoljne ljudske resurse s potrebnim vještinama kako bi osigurala adekvatno upravljanje i nadziranje ugovora o eksternalizaciji, kao i ostale potrebne resurse za usklađenost sa svim pravnim i regulatornim zahtjevima, te za dokumentovanje i praćenje svih ugovora o eksternalizaciji,
 - c) uspostaviti posebnu odgovornu funkciju odnosno organizacijsku odgovornost za eksternalizaciju (pri čemu to može biti posebno tijelo/odbor ili određeni član višeg rukovodstva), koja direktno odgovara upravi banke, te je zadužena za upravljanje rizicima povezanim sa eksternalizacijom, pri čemu kod malih i manje složenih banaka odgovornost za eksternalizaciju se može dodijeliti i članu uprave,
 - d) u okviru uspostavljenog okvira (sistema) interne kontrole i kontrolnih funkcija banke osigurati nadziranje eksternalizacije, kao i s njom povezane dokumentacije,
 - e) za svaku pojedinu eksternalizaciju, imenovati osobu zaduženu za operativno praćenje svake pojedinačne eksternalizovane aktivnosti (vlasnika eksternalizacije).
- (6) Banka je dužna u svakom trenutku održavati adekvatan nivo poslovanja, te minimalno:
 - a) u svakom trenutku ispunjavati sve uslove odobrenja za rad, uključujući efikasnost organa banke na izvršavanju dužnosti i odgovornosti propisanih čl. 10. i 11. ove odluke,
 - b) zadržati odgovarajuću organizacijsku strukturu sa jasno definisanim, preglednim i usklađenim odgovornostima unutar banke, te usklađenu sa zakonskim i podzakonskim zahtjevima,
 - c) ako se eksternalizuju aktivnosti podrške kontrolnim funkcijama, u skladu sa članom 4. stav (5) ove odluke, ili u slučaju eksternalizacije određene aktivnosti u okviru bankarske grupe čiji je banka član, izvršavati odgovarajući nadzor i moći upravljati rizicima koji proizilaze iz eksternalizacije,
 - d) raspolagati sa dovoljnim resursima i kapacitetima za osiguravanje usklađenosti sa tačkama a) do c) ovog stava.

Član 10.

Dužnosti i odgovornosti nadzornog odbora banke

Nadzorni odbor dužan je, kao minimum, da:

- a) uspostavi, nadzire i unapređuje sistem upravljanja eksternalizacijom i rizikom eksternalizacije, te svih drugih rizika povezanih sa eksternalizacijom,
- b) usvoji adekvatne strategije, odnosno politiku za upravljanje eksternalizacijom, osigura uslove za njihovo provođenje, te nadzire njihovo provođenje i periodično ih revidira, a uzimajući u obzir poslovni model banke i sklonost ka preuzimanju rizika,
- c) nadzire provođenje identifikacije, procijene i upravljanja potencijalnim sukobom interesa vezanim uz ugovore sa trećim stranama i poduzima odgovarajuće mjere za eliminisanje sukoba interesa,

- d) propiše sadržaj i periodičnost izvještavanja nadzornog odbora i drugih relevantnih odbora, tijela ili lica u vezi sa eksternalizovanim aktivnostima i rizicima, a najmanje na godišnjem nivou,
- e) donese odluku o svakoj pojedinačnoj materijalno značajnoj eksternalizaciji,
- f) uspostavi, održava i unapređuje efikasan sistem internih kontrola u banci i osigurava da uprava banke osigura uslove za njihovo provođenje, odnosno da kontrolne funkcije banke kontinuirano prate i provjeravaju da li se eksternalizacija obavlja u skladu sa zakonom, ovom odlukom, drugim propisima, strategijom, politikama, procedurama i drugim internim aktima banke.

Član 11.

Dužnosti i odgovornosti uprave banke

Uprava banke dužna je, kao minimum, da:

- a) priprema i nadzornom odboru predlaže strategije, odnosno politiku za upravljanje eksternalizacijom, koje je potrebno najmanje jednom godišnje analizirati i prilagoditi promjenama ekonomskih i tržišnih uslova,
- b) donosi ostale interne akte u vezi sa eksternalizacijom,
- c) uspostavi i osigura primjenu adekvatnih metoda i procedura za identifikaciju, mjerenje, odnosno procjenu, praćenje, analizu i kontrolu rizika eksternalizacije, te svih drugih rizika povezanih sa eksternalizacijom,
- d) osigura praćenje ekonomskih i tržišnih uslova radi predviđanja mogućih promjena, uključujući finansijsko stanje pružaoca usluga,
- e) osigura provođenje efikasnog sistema interne kontrole,
- f) osigura povjerljivost u smislu zaštite podataka i drugih informacija putem ugovora,
- g) osigura uslove za identifikaciju i uslove za procjenu potencijalnog sukoba interesa vezanih uz ugovore sa trećim stranama,
- h) osigura nesmetan tok relevantnih informacija sa pružaocem usluga,
- i) pravovremeno osigura nesmetano provođenje eksternalizovanih aktivnosti koje su materijalno značajne (npr. kada se ta aktivnost prenosi na drugog pružaoca usluga, kada banka preuzima navedenu aktivnost od pružaoca usluge i slično),
- j) uspostavi i implementira odgovarajući sistem izvještavanja o eksternalizovanim aktivnostima.

Član 12.

Politike i procedure upravljanja eksternalizacijom

- (1) Banka je dužna usvojiti, provoditi i redovno ažurirati politiku upravljanja eksternalizacijom.
- (2) Politika upravljanja eksternalizacijom treba da obuhvati sve faze životnog ciklusa ugovora o eksternalizaciji i definiše načela, odgovornosti i postupke povezane sa eksternalizacijom, te treba da obuhvati najmanje sljedeće:
 - a) jasno definisane nadležnosti i odgovornosti u pogledu donošenja odluka o eksternalizaciji i njihovim izmjenama, upravljanja eksternalizacijom i rizikom eksternalizacije unutar banke,
 - b) uključenost poslovnih linija, kontrolnih funkcija i drugih odgovornih lica u pogledu ugovora o eksternalizaciji,
 - c) procedure i postupke koji se provode prije sklapanja ugovora sa pružaocem usluga, uključujući:
 - 1) definisanje poslovnih zahtjeva u pogledu ugovora o eksternalizaciji,
 - 2) postupke za utvrđivanje ispunjavanja uslova za eksternalizaciju propisanih članom 4. ove odluke,
 - 3) postupke za utvrđivanje ispunjavanja uslova za primjenu unutar bankarske grupe propisanih čl. 5. ove odluke, u slučajevima gdje je primjenjivo,

- 4) kriterije i postupke za utvrđivanje materijalno značajnih aktivnosti, uključujući kriterije propisane čl. 6. i 7. ove odluke,
 - 5) način utvrđivanja, procjene i upravljanja rizicima koji proizilaze iz eksternalizacije, a minimalno uključujući aktivnosti propisane čl. 15. i 16. ove odluke,
 - 6) način provođenja dubinske analize potencijalnih pružaoca usluga, a minimalno uključujući aktivnosti propisane članom 17. ove odluke,
 - 7) postupke za utvrđivanje i procjenu potencijalnih sukoba interesa, upravljanje tim sukobima i njihovo smanjenje, u skladu sa propisima kojima je regulisan sistem internog upravljanja u banci i članom 13. ove odluke,
 - 8) način planiranja kontinuiteta poslovanja, a kako je propisano članom 22. ove odluke,
 - 9) definisanje načina i kriterija za izbor pružaoca usluga,
 - 10) postupak odobravanja novih ugovora o eksternalizaciji,
- d) način provođenja, praćenja i upravljanja ugovorima o eksternalizaciji, uključujući:
- 1) kontinuiranu procjenu rada pružaoca usluga, u skladu sa članom 26. ove odluke,
 - 2) postupke obavještanja o promjenama i postupanja banke u slučaju promjene ugovora o eksternalizaciji ili okolnostima u vezi sa pružaocem usluga (npr. finansijsko stanje, organizaciona ili vlasnička struktura, odnosi sa podizvođačima i drugo),
 - 3) nezavisnu provjeru usklađenosti sa zakonskim i regulatornim propisima i internim aktima banke od strane funkcije praćenja usklađenosti poslovanja,
 - 4) postupke obnavljanja ugovora,
- e) način dokumentovanja i vođenja registra informacija o eksternalizovanim aktivnostima, uzimajući u obzir zahtjeve člana 14. ove odluke,
- f) način definisanja izlaznih strategija i postupaka za otkaz ili raskid ugovora, uključujući zahtjev za dokumentovani izlazni plan, a uzimajući u obzir zahtjeve definisane članom 23. ove odluke,
- g) način obavljanja nadzora aktivnosti koje su predmet ugovora, odnosno obaveze i odgovornosti nadležnog organizacionog dijela, osiguravajući adekvatan nivo znanja i iskustva zaposlenih koji obavljaju nadzor i upravljanje eksternalizacijom,
- h) način i periodičnost izvještavanja organa banke o aktivnostima i rizicima eksternalizacije,
- i) sisteme izvještavanja i praćenja koji se provode od sklapanja do zaključenja ugovora o eksternalizaciji, uključujući pripremu poslovnog slučaja za eksternalizaciju, sklapanje ugovora o eksternalizaciji, provedbu ugovora do njegovog isteka, planove postupanja u kriznim situacijama i izlazne strategije.
- (3) Banka, u okviru politike upravljanja eksternalizacijom, treba napraviti razliku između eksternalizacije:
- a) materijalno značajnih aktivnosti i drugih eksternalizacija,
 - b) unutar grupe i eksternalizacija izvan grupe,
 - c) pružaocima usluga koji su pod nadzorom relevantnog nadležnog tijela i onima koji nisu,
 - d) pružaocima usluga u BiH i eksternalizacija pružaocima usluga u drugim zemljama.
- (4) Banka treba osigurati da politika upravljanja eksternalizacijom obuhvata utvrđivanje sljedećih mogućih uticaja eksternalizacije, te uzimanje istih u obzir u postupku donošenja odluke:
- a) profil rizičnosti,
 - b) mogućnost nadziranja pružaoca usluge i upravljanje rizicima,
 - c) uticaj rizika eksternalizacije, uključujući operativni, pravni, IKT, reputacijski, koncentracijski i druge rizike,
 - d) mjere za održavanje kontinuiteta poslovanja,
 - e) obavljanje poslovnih aktivnosti banke.
- (5) Politikom upravljanja eksternalizacijom potrebno je definisati:

- a) odgovornost banke za sve eksternalizovane aktivnosti i odluke o upravljanju koje proizilaze iz njih, jasno navodeći da eksternalizacija ne oslobađa banku od regulatornih obaveza i ugovorenih obaveza prema klijentu,
- b) aktivnosti koje treba preduzeti kako bi se osiguralo da eksternalizacija ni na koji način ne ometa efikasan posredni ili neposredni nadzor banke od strane Agencije, provođenje mjera za koje je Agencije ovlaštena, niti je u suprotnosti sa nadzornim ograničenjima u pogledu aktivnosti koje su eksternalizovane,
- c) unutargrupnu eksternalizaciju (odnosno usluge koje pruža pravni subjekt unutar bankarske grupe) i uzeti u obzir sve posebne okolnosti eksternalizacije na nivou bankarske grupe i odluke o upravljanju koje proizilaze iz njih, jasno navodeći da eksternalizacija ne oslobađa banku od regulatornih obaveza i obaveza prema klijentu,
- d) obavezu provjere uspostave odgovarajućih etičkih standarda i kodeksa ponašanja pri odabiru pružaoca usluga materijalno značajnih aktivnosti.

Član 13.

Sukob interesa

U skladu sa propisima kojima je regulisan sistem internog upravljanja u banci, banka je dužna identifikovati, procijeniti i upravljati sukobima interesa u pogledu ugovora o eksternalizaciji, uključujući:

- a) ako banka utvrdi da iz eksternalizacije proizilaze materijalni sukobi interesa, uključujući između subjekata unutar bankarske grupe, banka je dužna poduzeti odgovarajuće mjere za upravljanje tim sukobima interesa,
- b) ako eksternalizovanu aktivnost obavlja pružalac usluga koji je dio bankarske grupe ili je u vlasništvu grupe ili banke, ili lice u posebnom odnosu sa bankom, uslove (uključujući finansijske uslove) za eksternalizovane usluge treba utvrđivati po tržišnim uslovima,
- c) u slučaju eksternalizacije iz tačke b) ovog člana, pri određivanju cijena usluga mogu se uzeti u obzir sinergije koje proizilaze iz pružanja istih ili sličnih usluga za nekoliko subjekata unutar bankarske grupe, pod uslovom da pružalac usluga ostane samostalno održiv, bez obzira na likvidaciju odnosno tečaj bilo kojeg drugog subjekta bankarske grupe.

Član 14.

Registar informacija o eksternalizovanim aktivnostima

- (1) Banka je dužna dokumentovati na adekvatan način sve postojeće ugovore o eksternalizaciji, razlikujući pri tome ugovore o eksternalizaciji materijalno značajnih aktivnosti i druge ugovore o eksternalizaciji. U slučaju prestanka ugovora, banka je dužna, u skladu sa drugim relevantnim zakonima, čuvati dokumentaciju o završenim ugovorima o eksternalizaciji, kao i prateću dokumentaciju.
- (2) Banka je dužna da vodi ažuran registar informacija o eksternalizovanim aktivnostima svih ugovora o eksternalizaciji, a koji treba da sadrži najmanje sljedeće podatke i informacije:
 - a) broj, naziv i datum potpisivanja ugovora,
 - b) datum početka korištenja usluge, trajanje ugovora, datum završetka, kao i ugovoreni otkazni rok,
 - c) procjenu troškova eksternalizacije na godišnjem nivou,
 - d) predmet eksternalizacije, opis eksternalizovanih aktivnosti, podatke koji se eksternalizuju i informaciju o tome da li se vrši prenos ličnih podataka i njihova obrada,
 - e) kategoriju koju dodjeljuje banka, a koja odražava prirodu eksternalizovane aktivnosti u tački d) ovog stava (npr. IT informacione tehnologije (sistem), naziv poslovne aktivnosti i slično),
 - f) naziv i sjedište pružaoca usluge,
 - g) zemlju ili zemlje gdje će se usluga vršiti, lokaciju čuvanja i/ili obrade podataka,

- h) oznaku materijalne značajnosti i kratak opis razloga zašto se aktivnost smatra odnosno ne smatra materijalno značajnom,
 - i) ime osobe zadužene za operativno praćenje eksternalizacije i naziv funkcije odnosno organizacionog dijela banke odgovornog za eksternalizaciju,
 - j) ključno osoblje pružaoca usluge zaduženo za pružanje usluga banci,
 - k) u slučaju eksternalizacije pružaocu usluga računarstva u oblaku, tip usluge, model upotrebe, vrstu podataka i lokaciju čuvanja podataka,
 - l) datum posljednje procjene materijalne značajnosti eksternalizovane aktivnosti.
- (3) U slučaju eksternalizacije materijalno značajnih aktivnosti, registar informacija o eksternalizovanim aktivnostima, pored podataka/informacija iz stava (2) ovog člana, treba da sadrži i sljedeće podatke/informacije:
- a) spisak svih banaka ili društava unutar iste bankarske grupe koji koriste te eksternalizovane usluge, ukoliko je primjenjivo,
 - b) podatak da li je pružalac usluga ili podizvođač dio bankarske grupe ili je u vlasništvu neke od članica bankarske grupe,
 - c) mjerodavno pravo ugovora o eksternalizaciji,
 - d) datum posljednje procjene rizika vezane uz datu eksternalizaciju i pregled glavnih zaključaka,
 - e) datum posljednje i sljedeće planirane revizije pružaoca usluga, ako je primjenjivo,
 - f) nazive svih podizvođača kojima je eksternalizovano obavljanje dijelova materijalno značajnih aktivnosti, uključujući zemlju u kojoj je registrovan podizvođač, u kojoj će se pružati usluga, i ako je primjenjivo, lokaciju na kojoj će se skladištiti podaci,
 - g) rezultat procjene zamjenjivosti pružaoca usluga (jednostavno, teško, nemoguće), te mogućnost integracije eksternalizovane materijalno značajne aktivnosti u banku i uticaj prekida u obavljanju materijalno značajne aktivnosti,
 - h) identifikaciju alternativnih pružaoca usluga u skladu sa tačkom g) ovog stava,
 - i) podatak o tome da li je eksternalizovana materijalno značajna aktivnost vezana/podržava poslovne aktivnosti koje su vremenski kritične.

Član 15.

Analiza prije eksternalizacije

- (1) Prije donošenja svake odluke o eksternalizaciji banka je dužna:
- a) utvrditi da li planirani ugovor odnosno namjeravani poslovni odnos sa pružaocem usluga odgovara definiciji eksternalizacije. U okviru te procjene banka treba uzeti u obzir izvršava li pružalac usluga aktivnost (ili neki njen dio) koja mu se eksternalizuje redovno ili kontinuirano i da li ta aktivnost (ili neki njen dio) predstavlja aktivnost koju bi banka obavljala sama. Ako planirani ugovor sa pružaocem usluga obuhvata više aktivnosti, banka je u svojoj procjeni dužna razmotriti sve aspekte ugovora,
 - b) procijeniti da li su ispunjeni uslovi za eksternalizaciju iz člana 4. ove odluke,
 - c) procijeniti jesu li ispunjeni uslovi za eksternalizaciju unutar bankarske grupe iz čl. 5. ove odluke, ako je primjenjivo,
 - d) procijeniti složenost eksternalizovanih usluga i njihovu materijalnu značajnost u skladu sa čl. 6. i 7. ove odluke,
 - e) identifikovati i procijeniti sve relevantne rizike koji proizilaze iz eksternalizacije, a u skladu sa članom 16. ove odluke,
 - f) provesti odgovarajuću analizu potencijalnih pružatelja usluga, a u slučaju materijalno značajnih aktivnosti provesti dubinsku analizu (potencijalnih) pružaoca usluga, u skladu sa članom 17. ove odluke,
 - g) utvrditi da li propisi države ili država u kojima pružalac usluga posluje, omogućavaju Agenciji obavljanje direktnog nadzora onog dijela poslovanja pružaoca usluga koji ima

- ili bi mogao imati veze sa eksternalizacijom, te mogućnost direktnog nadzora same eksternalizacije koja je predmet ugovora, a u svrhu postizanja ciljeva supervizije,
- h) identifikovati i procijeniti sukobe interesa koji bi mogli proizaći iz eksternalizacije, te preduzeti odgovarajuće mjere za upravljanje tim sukobima interesa, u skladu sa propisima kojima je regulisan sistem internog upravljanja u banci i članom 13. ove odluke.
- (2) Odluka o eksternalizaciji treba biti usklađena sa poslovnom strategijom i ciljevima banke i sadržati obrazloženje koje obuhvata detaljan opis aktivnosti koje se namjeravaju eksternalizovati i razloge donošenja odluke o eksternalizaciji.
- (3) U slučaju nabavke resursa informacionog sistema, banka treba, prije donošenja odluke o kupovini, razmotriti načine održavanja istog. U slučaju da se održavanje neće provoditi od strane banke, kao i da predmetno održavanje predstavlja materijalno značajnu eksternalizovanu aktivnost, banka je dužna, prije same kupovine navedenog resursa, prijaviti predmetnu eksternalizaciju Agenciji i postupiti u skladu sa odredbama ove odluke.

Član 16.

Procjena rizika koji proizilaze iz ugovora o eksternalizaciji

Banka je dužna, prije donošenja odluke o eksternalizaciji, kao i tokom praćenja rada pružaoca usluge, identifikovati i procijeniti sve rizike koji proizilaze iz eksternalizacije, a najmanje:

- a) identifikovati i razvrstati relevantne aktivnosti i povezane podatke i sisteme s obzirom na njihovu osjetljivost i potrebne mjere zaštite,
- b) provesti detaljnu analizu aktivnosti i povezanih podataka i sistema koje obuhvata eksternalizacija, te razmotriti moguće rizike: operativni, pravni, reputacijski, IKT rizik i rizik usklađenosti, kao i ograničenja u pogledu nadzora povezanih sa zemljama u kojima se pružaju ili bi se mogle pružati eksternalizovane usluge i u kojima su pohranjeni ili će se vjerovatno pohraniti podaci,
- c) pregledati politike upravljanja rizicima i, ako je primjenjivo, kontrole informacionog sistema, kao i kontrolno okruženje kod pružaoca usluga, a kako bi osigurala da oni zadovoljavaju interne ciljeve upravljanja rizicima banke i prihvatljive nivoe rizika,
- d) u okviru procjene operativnog rizika, za materijalno značajne eksternalizovane aktivnosti, treba uključivati, prema potrebi, scenarije mogućih događaja povezanih sa rizikom, uključujući događaje sa velikim gubicima. U okviru analize scenarija, banka treba procijeniti mogući uticaj prekida pružanja usluga ili neadekvatnog pružanja usluga, uključujući rizike koji proizilaze iz neuspješnih ili neadekvatnih procesa, sistema, ljudi ili eksternih događaja. Banka je dužna, uzimajući u obzir princip proporcionalnosti, dokumentovati navedene izvršene analize i njihove rezultate, te procjene u kojoj mjeri bi eksternalizacija povećala odnosno smanjila operativni rizik. Navedena analiza bi trebala da uključuje upotrebu internih i eksternih podataka o gubicima, ako su dostupni,
- e) razmotriti uticaj lokacije pružaoca usluga (u BiH ili izvan BiH), moguća ograničenja u pogledu nadzora povezanih sa zemljama u kojima će se pružati eksternalizovane usluge i pohranjivati i obrađivati podaci,
- f) razmotriti političku stabilnost i sigurnosno stanje predmetnih država, uključujući relevantni regulatorni okvir, kao i odredbe zakonskih propisa o stečaju koje bi se primjenjivale u slučaju propasti pružaoca usluga, te sva ograničenja do kojih bi došlo s obzirom na hitan oporavak podataka banke,
- g) definisati adekvatan nivo zaštite povjerljivosti podataka, kontinuiteta eksternalizovanih aktivnosti kod pružaoca usluga, te integriteta i sljedivosti (mogućnosti praćenja) podataka i sistema u kontekstu planirane eksternalizacije. Banka treba razmotriti i konkretne mjere koje se odnose na podatke koji se procesiraju/obrađuju, prenose i pohranjuju, kao što je upotreba tehnologija enkripcije, u kombinaciji sa adekvatnom arhitekturom upravljanja ključevima. U okviru procjene kontinuiteta poslovanja pružaoca usluge, banka je dužna

- procijeniti usklađenost kontinuiteta poslovanja pružaoca usluga u vezi usluga koje će se eksternalizirati te usaglašenost sa kontinuitetom poslovanja banke,
- h) procijeniti očekivane koristi i troškove predložene eksternalizacije, uzimajući u obzir i rizike koji se mogu smanjiti ili kojima se može bolje upravljati u odnosu na rizike koji mogu proistći iz predloženog ugovora, a uzimajući u obzir najmanje:
- 1) rizik koncentracije koji proizilazi iz eksternalizacije značajnom pružaocu usluga kojeg nije jednostavno zamijeniti i većeg broja ugovora o eksternalizaciji sklopljenih sa istim pružaocem usluga ili povezanim pružaocima usluga,
 - 2) ukupne rizike koji proizilaze iz eksternalizovanih aktivnosti banke, kao i ukupne rizike na konsolidiranoj osnovi,
 - 3) rizik koji može proizaći iz potrebe pružanja finansijske podrške pružaocu usluga koji se suočava sa poteškoćama ili zbog potrebe preuzimanja njegovih poslovnih djelatnosti,
 - 4) mjere koje provodi banka sa ciljem upravljanja rizicima i njegovog smanjivanja,
- i) uzeti u obzir činjenicu da li je pružalac usluga matično društvo ili podređeno društvo banke odnosno bankarske grupe ili grupe društava kojoj banka pripada, da li je uključen u računovodstvenu konsolidaciju banke ili bankarske grupe ili grupe društava kojoj banka pripada i, ako jeste, u kojoj ga mjeri ta banka/bankarska grupa kontroliše ili može uticati na njegove radnje, u skladu sa članom 5. ove odluke,
- j) ako ugovor o eksternalizaciji materijalno značajne aktivnosti uključuje mogućnost da pružalac usluga angažuje podizvođača, banka je dužna da uzme u obzir sve povezane rizike, uključujući dodatne rizike koji mogu nastati ako je lokacija podizvođača u zemlji različitoj od one u kojoj je pružalac usluga, kao i rizike smanjenja efikasne sposobnosti nadziranja eksternalizovane aktivnosti od strane banke ili nadzora Agencije u slučaju dugih i složenih lanaca podizvođača.

Član 17.

Dubinska analiza pružaoca usluge

- (1) Prije zaključenja ugovora o eksternalizaciji aktivnosti, banka je dužna, u okviru svojih postupaka odabira i procjene, utvrditi primjerenost pružaoca usluga, odnosno utvrditi da pružalac usluga ima poslovni ugled, odgovarajuće i dovoljne sposobnosti, stručnost, kapacitete, resurse (npr. ljudske, IKT, finansijske resurse), te da je registrovan odnosno ima dozvolu nadležnog tijela za obavljanje predmetne eksternalizovane aktivnosti.
- (2) U slučaju eksternalizacije materijalno značajnih aktivnosti, banka treba provesti dubinsku analizu pružaoca usluga koja treba da uključuje, između ostaloga, i sljedeće:
 - a) analizu poslovnog modela potencijalnog pružaoca usluga, prirodu, veličinu, složenost, finansijsko stanje i vlasničku strukturu odnosno strukturu grupe,
 - b) dugoročne odnose sa pružaocima usluga koji su već procijenjeni i pružaju usluge banci,
 - c) analizu stručnosti ključnog osoblja pružaoca usluga koji će biti odgovorni za pružanje eksternalizovane usluge banci,
 - d) da li je pružalac usluga pod nadzorom nadležnih tijela.
- (3) Ako eksternalizacija uključuje obradu ličnih ili povjerljivih podataka, banka se treba uvjeriti da pružalac usluga provodi odgovarajuće tehničke i organizacione mjere potrebne za zaštitu podataka.
- (4) Banka treba preduzeti odgovarajuće korake kako bi utvrdila da li pružaoci usluga postupaju u skladu sa njenim korporativnim vrijednostima i kodeksom ponašanja. Naročito, kad je riječ o pružaocima usluga u drugim zemljama i, ako je primjenjivo, njihovim podizvođačima, banka se treba uvjeriti da pružalac usluga posluje na etički i društveno odgovoran način.

Član 18.

Dokumentovanost

Banka je dužna na odgovarajući način dokumentovati procjene izvršene u skladu sa čl. 4., 5., 6., 7., 15., 16. i 17. ove odluke, kao i rezultate kontinuiranog praćenja (npr. rad pružaoca usluga, usklađenost s ugovorenim nivoima usluge, ugovornim obavezama, regulatornim zahtjevima, analize revizorskih izvještaja, ažuriranja procjene rizika i slično).

Član 19.

Ugovorni odnos banke i pružaoca usluga

- (1) Pri sklapanju ugovora sa pružaocem usluga banka je dužna voditi računa o tome da ugovorne odredbe prema svom obimu i sadržaju budu odgovarajuće, odnosno srazmjerne rizicima eksternalizacije, te obimu i složenosti eksternalizovanih aktivnosti.
- (2) Banka je dužna sa pružaocem usluga sklopiti ugovor u pisanom obliku, kojim će jasno definisati svi relevantni pojmovi, uslove, prava, obaveze i odgovornosti ugovornih strana.
- (3) Ugovor o eksternalizaciji aktivnosti koje nisu materijalno značajne treba, kao minimum, da sadrži sljedeće:
 - a) jasan i detaljan opis usluga koje su predmet ugovora,
 - b) mjesto, vrijeme i način ispunjavanja ugovornih obaveza,
 - c) datum početka i datum završetka, odnosno trajanje ugovora, te otkazne rokove za pružaoca usluga i za banku,
 - d) opis očekivanog kvaliteta i nivoa usluga,
 - e) finansijske obaveze ugovornih strana,
 - f) način nadzora obavljanja aktivnosti koje su predmet ugovora od strane banke na kontinuiranoj osnovi, te obavezu izvještavanja banke od strane pružaoca usluga,
 - g) obavezu pružaoca usluga da omogući Agenciji, banci, ovlaštenom revizoru banke i trećim stranama koje imenuje Agencija i banka, obavljanje neograničenog prava nadzora i revizije na lokaciji pružanja usluga, te pravovremen, neograničen i nesmetan pristup dokumentaciji, relevantnim poslovnim prostorima (sjedište, informatičkim centrima i dr.), uključujući pristup svim relevantnim uređajima, sistemima, mrežama, informacijama i podacima, koji se koriste za pružanje eksternalizovane aktivnosti, odnosno koji se mogu dovesti u vezi sa pružanjem eksternalizovanih aktivnosti, kao i svim povezanim finansijskim informacijama, odgovornim licima i eksternim revizorima pružaoca usluge,
 - h) obavezu pružaoca usluga da saraduje sa Agencijom, uključujući i drugim osobama koje ona imenuje,
 - i) obavezu pružaoca usluga da neće trećim licima otkriti ili objaviti posjetu od strane Agencije,
 - j) obavezu čuvanja bankovne i poslovne tajne, te obavezu čuvanja i način zaštite povjerljivih podataka, a u skladu sa propisima,
 - k) odredbe u pogledu pravovremenog otklanjanja sigurnosnih rizika i drugih nedostataka identifikovanih u pružanju usluge (na zahtjev banke ili po nalogu Agencije),
 - l) obavezu pružaoca usluga da prije zaključenja ugovora sa podizvođačem zatraži prethodnu pisanu saglasnost banke, te da osigura da je ugovor pružaoca usluga sa podizvođačem usaglašen sa stavkama ugovora banke i pružaoca usluga,
 - m) obavezu pružaoca usluga da pravovremeno obavijesti banku o svim činjenicama i promjenama okolnosti koje značajno utiču, ili bi mogle značajno uticati, na sposobnost pružaoca usluga da efikasno izvršava eksternalizovanu aktivnost u skladu sa dogovorenim nivoom usluge i u skladu sa primjenjivim zakonima i regulatornim zahtjevima, uključujući i izvještavanje o fluktuaciji ključnog osoblja pružaoca usluga,

- n) detaljan opis uslova za raskid i/ili otkaz ugovora, uključujući pravo banke da raskine, odnosno otkáže ugovor sa pružaocem usluga (na zahtjev banke ili po nalogu Agencije), u skladu sa članom 21. ove odluke,
 - o) detaljan opis prava i obaveza ugovornih strana u slučaju prijevremenog prestanka ugovora radi obezbjeđenja kontinuiteta pružanja usluga,
 - p) izbor mjerodavnog prava,
 - q) način rješavanja sporova.
- (4) Ugovor o eksternalizaciji materijalno značajnih aktivnosti, pored tačaka iz stava (3) ovog člana, treba da sadrži i sljedeće:
- a) opis očekivanog kvaliteta i nivoa usluga, a što treba uključivati precizne kvantitativne i kvalitativne ciljeve uspješnosti za eksternalizovanu aktivnost, kako bi se omogućilo adekvatno i pravovremeno praćenje te time i poduzimanje odgovarajućih korektivnih mjera ako se ne postigne dogovoreni nivo usluge,
 - b) lokaciju gdje će se aktivnost izvršavati, uključujući obradu podataka i eventualno skladištenje podataka i uslove koji se moraju ispuniti, te zahtjev o obavještanju banke ukoliko pružalac usluge ima namjeru da promjeni lokaciju obavljanja aktivnosti,
 - c) odredbe o mogućnosti angažovanja podizvođača, kao i uslove pod kojima je dozvoljena podeksternalizacija, a u skladu sa članom 20. ove odluke,
 - d) zahtjeve u pogledu uvođenja i testiranja planova poslovanja u kriznim situacijama,
 - e) potrebu da pružalac usluga poduzme obavezne mjere osiguranja od određenih rizika, te prema potrebi, nivo pokrivanja osiguranja koje se traži,
 - f) odredbe u pogledu pristupa podacima, dostupnosti, integriteta, privatnosti i sigurnosti relevantnih podataka, a kako je navedeno u članu 24. ove odluke,
 - g) detaljan opis prava i obaveza ugovornih strana u slučaju pokretanja postupka restrukturiranja banke, posebno uzevši u obzir ovlaštenja Agencije iz Zakona, uključujući i nemogućnost jednostranog raskida ugovora od strane pružaoca eksternalizirane usluge zbog pokretanja postupka restrukturiranja nad bankom, pod uslovom da se obaveze plaćanja i isporuke i dalje izvršavaju,
 - h) ključno osoblje pružaoca usluge koje je zaduženo za pružanje usluga banci,
 - i) odredbe kojima se osigurava pravo pristupa i raspolaganja bančnim podacima, a koji su u posjedu pružaoca usluga, u slučaju stečaja, restrukturiranja ili prekida poslovnih aktivnosti pružaoca usluga,
 - j) obavezu pružaoca usluga da treba biti pravovremeno usaglašen sa regulatornim zahtjevima i industrijskim standardima, gdje je to primjenjivo.

Član 20.

Angažovanje podizvođača

- (1) U ugovoru sa pružaocem usluga, banka je dužna definisati mogućnost angažovanja podizvođača, a u skladu sa članom 19. stav (4) tačka c) ove Odluke.
- (2) U slučaju da je dozvoljena podeksternalizacija materijalno značajne aktivnosti, banka je dužna utvrditi da li je dio aktivnosti koji se namjerava podeksternalizirati sam po sebi materijalno značajan (odnosno značajan dio materijalno značajne eksternalizacije) te, ako jeste, upisati ga u registar informacija o eksternalizovanim aktivnostima propisan članom 14. ove odluke.
- (3) Ako se radi o podeksternalizaciji koja je ocijenjena materijalno značajnim dijelom eksternalizacije, u skladu sa stavom (2) ovog člana, banka je dužna da, u okviru ugovora sa pružaocem usluga, definiše sljedeće:
 - a) sve vrste aktivnosti koje su isključene iz podeksternalizacije,
 - b) uslove koje je potrebno ispuniti u slučaju podeksternalizacije,
 - c) obavezu pružaoca usluga da nadzire usluge koje je podugovorio kako bi se osiguralo kontinuirano ispunjavanje svih ugovornih obaveza između pružaoca usluga i banke,

- d) obavezu pružaoca usluga da u pisanom obliku i u skladu sa ugovorenim rokovima obavijesti banku o svakom planiranom angažovanju ili izmjeni podizvođača ili značajnim promjenama u vršenju podeksternalizovane usluge, posebno ukoliko one mogu uticati na sposobnost pružaoca usluga da ispuní svoje obaveze iz ugovora o eksternalizaciji; navedeno obavještenje treba najmanje da sadrži detaljan opis aktivnosti koje će biti prenesene na podizvođača, kao i mjesto, vrijeme i način obavljanja dijela podeksternalizovane aktivnosti, uključujući lokaciju, gdje će se aktivnosti izvršavati, lokaciju obrade podataka i eventualnog skladištenja podataka,
 - e) obavezu pružaoca usluga da prije podeksternalizacije podataka pribavi posebno ili opšte pisano odobrenje od banke,
 - f) odredbu kojom se zahtijeva izričito odobrenje banke za angažovanje podizvođača, planiranu izmjenú podizvođača ili značajnu promjenu,
 - g) mogućnost banke da raskine ugovor u slučaju da prenos usluga na podizvođača povećava rizike kojima je banka izložena samom eksternalizacijom ili ako pružalac usluga izvrši angažovanje, odnosno izmjenú podizvođača bez pisane saglasnosti banke.
- (4) Banka može dozvoliti podeksternalizaciju samo pod sljedećim uslovima:
- a) da pružalac usluga osigura da je ugovor pružaoca usluga sa podizvođačem usaglašen sa ugovornim odredbama banke i pružaoca usluga,
 - b) da pružalac usluga osigura da podizvođač ispunjava sve zahtjeve definisane ugovorom, ovom odlukom, drugim zakonskim i podzakonskim propisima,
 - c) da podizvođač osigura prava pristupa i nadzora banci i Agenciji, kao što je osigurao pružalac usluga.
- (5) Banka je dužna osigurati da pružalac usluga na odgovarajući način nadzire podizvođača usluga, u skladu s politikom koju definiše banka. Ako bi namjeravana podeksternalizacija mogla značajno negativno uticati na ugovor o eksternalizaciji materijalno značajne aktivnosti ili bi dovela do materijalno značajnog povećanja rizika, uključujući ako se ne bi ispunili uslovi iz stava (4) ovog člana, banka treba ostvariti svoje pravo na otkaz ugovora.

Član 21.

Pravo na otkaz

- (1) Ugovor o eksternalizaciji mora da sadrži ugovornu odredbu koja omogućava banci otkazivanje ugovora u skladu sa mjerodavnim pravom, a uključujući i sljedeće situacije:
- a) ako pružalac usluga krši ugovoreno pravo, propise ili ugovorne odredbe, uključujući dogovoreni nivo usluge,
 - b) ako se utvrde realizovani rizici, nastali gubici, odnosno prepreke koje bi mogle izmijeniti način obavljanja eksternalizovane aktivnosti,
 - c) ako postoje materijalno značajne promjene koje utiču na eksternalizaciju ili pružaoca usluga (promjena podizvođača za obavljanje aktivnosti koje je procjenjuju kao materijalno značajne bez prethodne saglasnosti banke, a u skladu sa članom 20. odluke, povećana fluktuacija osoblja, značajno smanjenje broja zaposlenih, promjena fizičke lokacije obavljanja usluge, negativni publicitet za koji banka procijeni da utiče značajno na reputaciju banke, istek licenci za koje je zadužen podizvođač i sl.),
 - d) ako postoje slabosti u pogledu upravljanja povjerljivim, ličnim ili na drugi način osjetljivim podacima ili informacijama ili u pogledu njihove sigurnosti,
 - e) ako ugovor nije u skladu sa ovom odlukom,
 - f) ako Agencija izda takav nalog (npr. u slučaju da Agencija zbog eksternalizacije više nije u mogućnosti efikasno obavljati nadzor nad bankom).
- (2) Ugovorom o eksternalizaciji treba definisati postupak prenosa eksternalizacije na drugog pružaoca usluga ili vraćanja aktivnosti unutar banke. U tu svrhu pisanim ugovorom o eksternalizaciji treba:

- a) jasno utvrditi obaveze postojećeg pružaoca usluga u slučaju prenosa eksternalizovane aktivnosti na drugog pružaoca usluga ili vraćanja aktivnosti unutar banke, uključujući obaveze u pogledu postupanja sa podacima,
- b) utvrditi odgovarajući otkazni rok kako bi se smanjio rizik prekida obavljanja eksternalizovane aktivnosti,
- c) utvrditi obavezu pružaoca usluga da pruži podršku banci prilikom prenosa aktivnosti, na odgovarajući način, u slučaju raskida i/ili otkaza ugovora o eksternalizaciji.

Član 22.

Planovi kontinuiteta poslovanja

- (1) Banka je dužna uspostaviti, održavati i redovno testirati odgovarajuće planove kontinuiteta poslovanja u pogledu eksternalizovanih materijalno značajnih aktivnosti, uzimajući u obzir i planove kontinuiteta poslovanja pružaoca usluga (uključujući i podizvođače), njihovu usaglašenost sa planovima kontinuiteta poslovanja banke, te se uvjeriti u njihovu izvodivost.
- (2) U okviru redovnog testiranja kontinuiteta poslovanja iz stava (1) ovog člana, banka je dužna uključiti i scenario vezan za nemogućnost pružaoca usluga (uključujući i podizvođača usluga) da na adekvatan način vrši eksternalizovane materijalno značajne aktivnosti.
- (3) Planovi kontinuiteta poslovanja treba da uzmu u obzir i mogućnost stečaja ili likvidacije pružaoca usluga ili uticaj relevantnih rizika na poslovanje pružaoca usluge (uključujući i podizvođača usluge), npr. politički rizici u državi pružaoca usluga.

Član 23.

Izlazna strategija

- (1) Banka je dužna za svaku eksternalizovanu aktivnost, donijeti izlaznu strategiju i postupke, koji su u skladu sa politikom upravljanja eksternalizacijom i planovima kontinuiteta poslovanja banke, a uzimajući u obzir najmanje sljedeće mogućnosti:
 - a) otkaz ugovora o eksternalizaciji,
 - b) stečaj ili likvidaciju pružaoca usluga
 - c) narušavanje kvaliteta obavljanja eksternalizovanih aktivnosti, potencijalnih poslovnih poremećaja prouzrokovanih neodgovarajućim ili neuspješnim obavljanjem eksternalizovanih aktivnosti,
 - d) nastanak ili povećanje materijalno značajnih rizika koji ugrožavaju adekvatno i kontinuirano obavljanje aktivnosti.
- (2) Izlazna strategija treba da uključi najmanje sljedeće:
 - a) definisanje ciljeva izlazne strategije, uključujući strategiju nastavka obavljanja eksternalizovane aktivnosti od strane drugog pružaoca usluga ili vraćanje aktivnosti unutar banke, te osiguravanje uslova za njihovo provođenje,
 - b) analizu uticaja na poslovanje proporcionalnu riziku eksternalizovanih aktivnosti, a kako bi se utvrdili potrebni finansijski i ljudski resursi, te neophodno vrijeme potrebno za implementaciju navedene izlazne strategije,
 - c) osiguranje potrebnih resursa, te raspodjelu odgovornosti i nadležnosti za upravljanje izlaznom strategijom i prenosom aktivnosti,
 - d) definisanje kriterija po kojima se ocjenjuje da li je prenos aktivnosti i podataka izvršen na adekvatan i uspješan način,
 - e) parametre koji će se primjenjivati za praćenje obavljanja aktivnosti koje su predmet nadzora (eksternalizovane aktivnosti), u skladu sa članom 26. ove odluke, uključujući i definisanje indikatora neprihvatljivog nivoa usluge koji iniciraju aktiviranje izlazne strategije.
- (3) Banka je dužna osigurati mogućnost otkaza ugovora o eksternalizaciji bez prekida obavljanja poslovnih aktivnosti, bez ograničavanja svoje usklađenosti sa regulatornim zahtjevima i bez štetnih posljedica za kontinuitet i kvalitetu vlastitog pružanja usluga klijentima banke. U

slučaju eksternalizacije materijalno značajne aktivnosti, navedeno uključuje minimalno sljedeće:

- a) izradu i provođenje izlaznih planova koji su sveobuhvatni, dokumentovani i, prema potrebi, testirani (npr. provođenjem analize mogućih troškova, efekata, resursa i vremenskih aspekata prenosa eksternalizovane aktivnosti),
- b) identifikovanje alternativnih rješenja i izradu prelaznih planova prenosa eksternalizovane aktivnosti na drugog pružaoca usluga ili integraciju aktivnosti u banku, ili poduzimanje drugih mjera kojima se osigurava kontinuirano obavljanje eksternalizovane aktivnosti na kontrolisan i dobro testiran način, a uzimajući u obzir i probleme do kojih može doći zbog lokacije podataka te poduzimanja odgovarajućih mjera za osiguranje kontinuiteta poslovanja tokom prelazne faze.

Član 24.

Sigurnost sistema i podataka

- (1) Banka je dužna osigurati da pružaoci usluga odnosno podizvođači, kad je to relevantno, poštuju odgovarajuće standarde IKT sigurnosti, uključujući preporuke proizvođača software, odnosno hardware, a najmanje u mjeri u kojoj bi bili primijenjeni u slučaju obavljanja istih aktivnosti unutar banke. Pri tome, banka je u potpunosti odgovorna za ispunjenje svih regulatornih zahtjeva, a koji se odnose na eksternalizovane aktivnosti.
- (2) Banka je dužna u ugovoru o eksternalizaciji utvrditi zahtjeve u pogledu sigurnosti podataka i sistema, te kontinuirano pratiti usklađenost sa tim zahtjevima, u mjeri u kojoj je to primjenjivo (npr. u slučaju eksternalizacije usluga računarstva u oblaku ili drugoj eksternalizaciji u području IKT-a).
- (3) U slučaju eksternalizacije pružiocima usluga računarstva u oblaku i drugih ugovora o eksternalizaciji koji uključuju rukovanje ličnim ili povjerljivim podacima, te njihov prenos, banka treba primjenjivati pristup zasnovan na procjeni rizika s obzirom na lokaciju ili lokacije (tj. zemlju ili regiju) za pohranu i obradu podataka, te po pitanju sigurnosti informacija.
- (4) Banka treba osigurati da ugovor o eksternalizaciji uključuje obavezu pružaoca usluga da čuva povjerljive, lične ili na drugi način osjetljive informacije, te da poštuje sve zakonske i regulatorne zahtjeve koji se odnose na zaštitu podataka, a primjenjuju se na banku (npr. zaštita ličnih podataka i poštovanje bankarske tajne ili sličnih zakonskih i regulatornih obaveza u pogledu povjerljivosti koje se odnose na informacije o klijentima, ukoliko je primjenjivo). Ukoliko se lokacija za pohranu i obradu podataka nalazi izvan teritorije BiH, neophodno je uzeti u obzir i razlike među nacionalnim propisima o zaštiti podataka. Lokacija za pohranu podataka ne može biti u državi koja ima manje standardne zaštite podataka od standarda koji su na snazi u BiH.

Član 25.

Pravo pristupa podacima i pravo na reviziju eksternalizovanih aktivnosti

- (1) Banka je dužna u okviru ugovora o eksternalizaciji pozvati se na ovlasti za prikupljanje informacija, kao i nadzornih ovlaštenja Agencije i ovlaštenja u postupku restrukturiranja.
- (2) Banka je dužna osigurati da se ugovorom o eksternalizaciji ili nekim drugim ugovorom ne sprječava, niti ugrožava njeno uspješno ostvarivanje prava pristupa i prava na nadzor/reviziju pružaoca usluga i podizvođača, od strane banke, Agencije ili trećih lica koje je imenovala Agencija ili banka, kao i uspješno ostvarivanje zakonom utvrđenih prava.
- (3) Banka je dužna osigurati da ugovori i revizorski nalazi, kao i izvještaji internih i eksternih revizora koji se odnose na eksternalizovane aktivnosti budu dostupni na jednom od službenih jezika u BiH.
- (4) Banka je dužna ostvarivati svoja prava pristupa i prava na reviziju, utvrđivati učestalost revizije i područja u kojima treba provesti reviziju, na osnovu pristupa zasnovanog na

- procjeni rizika, a uzimajući u obzir odredbe člana 27. ove odluke, te poštovati relevantne nacionalne i međunarodne standarde revizije.
- (5) Ne dovodeći u pitanje njihovu krajnju odgovornost u pogledu ugovora o eksternalizaciji, banka može primjenjivati:
 - a) grupne revizije organizovane zajedno sa drugim klijentima istog pružaoca usluga koje provode one same i ti klijenti ili treća strana koju su oni imenovali, kako bi se racionalnije iskoristili revizorski resursi, te kako bi se klijentima i pružaocu usluga smanjilo organizaciono opterećenje,
 - b) certifikate i revizorske izvještaje trećih strana ili izvještaje interne revizije koje je pružalac usluga stavio na raspolaganje.
 - (6) Ukoliko se radi o materijalno značajnim aktivnostima, banka treba procijeniti da li su certifikati i izvještaji trećih strana, navedeni u stavu (5) tačka b) ovog člana, adekvatni i dovoljni za ispunjavanje regulatornih zahtjeva, pri čemu se ne treba dugoročno oslanjati samo na ove izvještaje.
 - (7) Banka može koristiti metodu iz stava (5) tačke b) ovog člana samo u sljedećim slučajevima:
 - a) ako je plan revizije za eksternalizovanu aktivnost adekvatan,
 - b) ako osigura da obim certifikacije ili revizorskog izvještaja uključuje sisteme (postupke, aplikacije, infrastrukturu, informatičke centre i drugo) i kontrole koje je banka identifikovala kao ključne, kao i usklađenost sa relevantnim regulatornim zahtjevima,
 - c) ako detaljno i kontinuirano pregleda sadržaj i obuhvat revizorskih izvještaja ili certifikacije, te provjerava da navedeni nisu zastarjeli, odnosno da su važeći,
 - d) ako je osposobljenost društva, odnosno osoba koje obavljaju reviziju ili certifikaciju (npr. u pogledu promjene društva koje obavlja reviziju ili certifikaciju, kvalifikacija, stručnosti, ponovnog izvođenja/provjere dokaza u revizorskom dosijeu i sl.) adekvatna,
 - e) ako se uvjerila da se certifikati izdaju i revizije provode u skladu sa međunarodnim relevantnim profesionalnim standardima, te uključuju testiranje operativne efikasnosti postojećih ključnih kontrola,
 - f) ako ima ugovorno pravo zatražiti proširenje obuhvata certifikacije ili revizorskih izvještaja na druge relevantne sisteme i kontrole, pri čemu broj i učestalost takvih zahtjeva za izmjenu trebaju biti razumni i opravdani sa stanovišta upravljanja rizicima,
 - g) ako zadržava ugovorno pravo obavljanja, prema vlastitoj odluci, pojedinačnih revizija materijalno značajnih eksternalizovanih aktivnosti.
 - (8) Banka je dužna, kad je to relevantno, osigurati provođenje penetracionih testova eksternalizovane usluge, a kako bi provjerila efikasnost implementiranih mjera zaštite, kontrola i postupaka u području IKT-a.
 - (9) Banka, Agencija ili treće strane koje je Agencija ili banka imenovala trebaju pravovremeno obavijestiti pružaoca usluga o obavljanju nadzora odnosno revizije na lokaciji pružaoca usluga, osim u slučajevima kada to nije moguće zbog hitne ili krizne situacije ili bi dovelo do situacije u kojoj nadzor, odnosno revizija više ne bi bila efikasna.
 - (10) Pri obavljanju revizija u okruženjima sa više klijenata trebaju se preduzeti mjere kojima se izbjegavaju ili ublažavaju rizici za okruženje nekog drugog klijenta (npr. uticaj na nivo usluge, raspoloživost podataka, povjerljivost i sl.).
 - (11) Ako eksternalizacija podrazumijeva visok nivo tehničke složenosti, na primjer u slučaju eksternalizacije usluga računarstva u oblaku, banka treba provjeriti da li subjekt koji provodi reviziju, bez obzira na to radi li se o njenim internim revizorima, grupi revizora ili eksternim revizorima, ima odgovarajuće i relevantne vještine i znanja za efektivno provođenje relevantne revizije i/ili procjena. Isto se odnosi i na lica u banci koja vrše pregled revizorskih izvještaja i certifikate trećih strana.

Član 26.

Nadzor eksternalizovanih aktivnosti

- (1) Banka je dužna preduzeti odgovarajuće mjere i konstantno osiguravati da eksternalizovane aktivnosti zadovoljavaju standarde kvaliteta koji bi bili primijenjeni u slučaju obavljanja istih aktivnosti unutar banke.
- (2) Banka je dužna redovno ažurirati svoje procjene rizika, kao i materijalnu značajnost eksternalizovane usluge, u skladu sa čl. 6., 7. i 16. ove odluke, a najmanje jednom godišnje, i obavezno prilikom značajne promjene u pružanju eksternalizovane usluge. Banka je, u okviru navedenih procjena rizika, dužna pratiti i rizike koncentracije prouzrokovane eksternalizacijom i efikasno upravljati njima.
- (3) Banka je dužna redovno pratiti rad pružaoca usluga kada je riječ o svim ugovorima o eksternalizaciji, na bazi procjene rizika, a obavezno ukoliko se radi o eksternalizaciji materijalno značajnih aktivnosti. U okviru parametara praćenja, banka je dužna pratiti parametre koji se odnose na rizike dostupnosti, integriteta i povjerljivosti podataka, informacija i sistema. U slučaju promjene rizika, prirode ili veličine eksternalizovane aktivnosti, banka je dužna ponovno procijeniti materijalnu značajnost eksternalizovane aktivnosti, u skladu sa čl. 6. i 7. ove odluke.
- (4) Pri tome je banka dužna da:
 - a) osigura da joj pružaoci usluga dostavljaju odgovarajuće izvještaje, sa unaprijed definisanim sadržajem/strukturuom, vremenskoj periodičnosti i definisanom načinu,
 - b) ocjenjuje rad pružaoca usluga na osnovu ključnih pokazatelja uspješnosti, ključnih pokazatelja kontrole, izvještaja o isporuci usluge, relevantnih certifikata i izvještaja o nezavisnim provjerama i
 - c) prati i analizira sve druge relevantne informacije primljene od pružaoca usluge, uključujući planove kontinuiteta poslovanja i izvještaje o njihovom testiranju, te ako je relevantno, informacije o kontrolnom okruženju pružaoca usluga, te broju i vrsti incidenata u informacionom sistemu pružaoca usluga, uključujući informacije o cyber napadima, te adekvatnost odgovora na iste.
- (5) Banka je dužna poduzeti odgovarajuće mjere ako identifikuje nedostatke u pružanju eksternalizovane aktivnosti.
- (6) U slučaju naznake da pružalac usluga ne obavlja materijalno značajnu aktivnost efikasno, u skladu sa ugovorom ili u skladu sa primjenjivim zakonima i regulatornim zahtjevima, banka je dužna poduzeti odgovarajuće mjere koje mogu uključivati i otkaz ugovora o eksternalizaciji sa trenutnim efektom.

Član 27.

Interna revizija eksternalizovanih aktivnosti

- (1) Funkcija interne revizije banke dužna je redovno obavljati reviziju eksternalizovanih aktivnosti i o tome izvještavati odbor za reviziju i nadzorni odbor. Planom i programom rada interne revizije u ovom segmentu treba definisati učestalost i predmet revizije, a na osnovu pristupa zasnovanog na procjeni rizika koji proizilaze iz eksternalizacije. Bez obzira na rezultat procjene rizika, materijalno značajne eksternalizacije visokog nivoa rizika moraju biti predmetom revizije na godišnjem nivou, dok sve materijalno značajne eksternalizacije trebaju biti predmetom revizije najmanje jednom u pet godina.
- (2) Revizijom iz stava (1) ovog člana, potrebno je utvrditi najmanje sljedeće:
 - a) da li se okvir kojim banka uređuje eksternalizaciju, uključujući politiku upravljanja eksternalizacijom, provodi pravilno i efikasno, te da je u skladu sa primjenjivim zakonskim propisima i podzakonskim aktima donesenim na osnovu zakona, strategijom rizika i odlukama organa banke,
 - b) adekvatnost, kvalitet i efektivnost procjene materijalno značajnih aktivnosti,

- c) adekvatnost, kvalitet i efektivnost procjene rizika eksternalizacije te usklađenost procjene rizika sa strategijom za preuzimanje rizika banke,
- d) adekvatnost uključivanja banke u sam proces eksternalizacije,
- e) adekvatnost praćenja i upravljanja eksternalizovanim aktivnostima,
- f) adekvatnost kontrolnog okruženja kod pružaoca usluga i/ili podizvođača, gdje je to primjenjivo, uzimajući u obzir odredbe člana 25. ove odluke.

Član 28.

Obavještavanje Agencije

- (1) Ako banka namjerava eksternalizovati materijalno značajnu aktivnost, dužna je o tome prethodno obavijestiti Agenciju i dostaviti kompletnu propisanu dokumentaciju.
- (2) Agencija, u roku od 90 dana od dana prijema obavještenja, odnosno kompletne propisane dokumentacije iz člana 29. ove odluke, utvrđuje da li su ispunjeni uslovi za eksternalizaciju u skladu sa zakonskim i podzakonskim propisima i o rezultatima procjene obavještava banku.
- (3) Banka, nakon dobijanja obavještenja da su ispunjeni uslovi za eksternalizaciju iz stava (2) ovog člana, može sklopiti ugovor o materijalno značajnoj eksternalizaciji.
- (4) Banka je dužna, u slučaju materijalno značajnih aktivnosti, pravovremeno obavijestiti Agenciju o svakoj značajnoj promjeni (uključujući i angažovanje ili zamjenu angažovanih podizvođača) i/ili ozbiljnim događajima koji bi potencijalno mogli materijalno ugroziti ugovor o eksternalizaciji i imati posljedice na poslovne aktivnosti, profitabilnost ili reputaciju banke. Uz navedenu obavijest, potrebno je dostaviti i ponovnu procjenu rizika, uzimajući u obzir navedenu promjenu.
- (5) U slučaju raskida ugovora koji se odnose na eksternalizaciju materijalno značajnih aktivnosti, banka je dužna, najkasnije 30 dana prije raskida ugovora, obavijestiti Agenciju, te dostaviti izvještaj o načinu obavljanja aktivnosti, odnosno budućim planovima za nastavak obavljanja eksternalizovanih aktivnosti.
- (6) Banka je dužna pravovremeno obavijestiti Agenciju u slučaju promjene materijalne značajnosti prethodno eksternalizovane aktivnosti, te dostaviti procjene rizika navedene u čl. 6., 7. i 16. ove odluke.

Član 29.

Potrebna dokumentacija za obavještavanje o materijalno značajnim aktivnostima

U slučaju namjere eksternalizacije materijalno značajne aktivnosti, banka je dužna, uz obavještenje u skladu sa članom 28. ove odluke, dostaviti Agenciji sljedeće dokumente:

- a) nacrt odluke nadzornog odbora banke o eksternalizaciji, sa obrazloženjem koje sadrži opis aktivnosti koje se eksternalizuju i razlog eksternalizacije,
- b) izvod iz sudskog ili drugog odgovarajućeg registra, iz kojeg se može utvrditi vlasnička struktura pružaoca usluge, u originalu ili ovjerenoj kopiji, ne stariji od šest mjeseci od dana dostavljanja odluke definisane tačkim a),
- c) spisak lica u posebnom odnosu sa bankom, koja su ujedno povezana sa pružaocem usluga, te opis načina na koji su povezani,
- d) revizorski izvještaj pružaoca usluga za prethodnu kalendarsku godinu, odnosno posljednji raspoloživi, a ukoliko pružalac usluga ne podliježe obavezi revizije finansijskih izvještaja, posljednje raspoložive kopije bilansa stanja i bilansa uspjeha pružaoca usluga,
- e) dokaz o dosadašnjem iskustvu pružaoca usluga na poslovima koji su predmet eksternalizacije,
- f) dokaz da nije otvoren stečajni postupak, odnosno postupak likvidacije pružaoca usluga,
- g) nacrt ugovora, koji sadrži elemente definisane ovom odlukom, koji banka namjerava sklopiti sa pružaocem usluga u vezi sa eksternalizacijom materijalno značajnih aktivnosti,

- h) procjenu ispunjenosti uslova za eksternalizaciju iz člana 4. ove odluke, uključujući, u slučaju da pružatelj usluga ima sjedište i/ili posluje u trećim zemljama, dokaz da propisi države odnosno država u kojima pružatelj usluga posluje omogućavaju Agenciji:
 - 1) da u svrhu postizanja ciljeva supervizije obavi neposredni nadzor dijela poslovanja pružatelja usluga koji ima veze ili se može dovesti u vezu s eksternalizacijom, kao i neposredni nadzor obavljanja aktivnosti koje su predmet ugovora i
 - 2) pravovremen i neograničen pristup dokumentaciji i podacima koji su povezani s eksternalizacijom, a u posjedu su pružatelja usluga,
- i) procjenu ispunjenosti uslova za eksternalizaciju unutar bankarske grupe definisanih čl. 5. ove odluke, ako je primjenjivo,
- j) procjenu materijalne značajnosti eksternalizacije iz čl. 6. i 7. ove odluke,
- k) procjenu rizika povezanih sa eksternalizacijom, uključujući procjenu rizika definisanu čl. 15. i 16. ove odluke,
- l) dubinsku analizu pružaoca usluga, u skladu sa članom 17. ove odluke,
- m) izlaznu strategiju banke, u skladu sa članom 23. ove odluke,
- n) detaljan opis tehničkih i organizacionih rješenja koja omogućuju sigurno i kvalitetno obavljanje aktivnosti koje se namjeravaju eksternalizovati, uključujući opis načina zaštite povjerljivosti, raspoloživosti i integriteta podataka,
- o) izjavu banke da članovi organa banke nisu u direktnom ili indirektnom interesu sa pružaocem usluga, te da ne postoji nikakva druga vrsta sukoba interesa,
- p) podatke sadržane u registru informacija o eksternalizovanim aktivnostima definisanom članom 14. ove odluke,
- r) izvještaj funkcije Usklađenosti poslovanja o usklađenosti predmetnog Ugovora sa ovom odlukom,
- s) ostale akte koje banka smatra važnim za predmetnu eksternalizaciju,
- t) listu dostavljene dokumentacije sa referencama na odgovarajuće odredbe čl. 19. i 29. ove odluke.

Član 30.

Postupci Agencije

- (1) Prilikom procjene adekvatnosti upravljanja rizikom eksternalizacije, osim dokumentacije iz člana 29. ove odluke, Agencija može zatražiti i drugu dokumentaciju, za koju smatra da je potrebna za procjenu ispunjenosti uslova za eksternalizaciju, kao i detaljne informacije o bilo kojem ugovoru o eksternalizaciji, čak i ako se predmetni ugovor ne smatra materijalno značajnim.
- (2) U postupku procjene, Agencija, između ostalog, utvrđuje sljedeće:
 - a) predstavljaju li ugovori o eksternalizaciji materijalno značajnu promjenu uslova i obaveza iz inicijalnog odobrenja za rad koje je izdato banci,
 - b) mogućnost adekvatnog nadzora banke uključujući nadzor nad eksternalizovanim aktivnostima, te mogućnost direktnog nadzora i prava pristupa eksternalizovanim aktivnostima,
 - c) upravljanje rizicima eksternalizacije od strane banke, a što uključuje najmanje sljedeće:
 - 1) adekvatnost praćenja i upravljanja rizicima eksternalizacije od strane banke, uključujući prepoznavanje i upravljanje svim relevantnim rizicima,
 - 2) adekvatnost dostupnih resursa banke za upravljanje rizikom eksternalizacije,
 - 3) identifikaciju i adekvatnost upravljanja sukobima interesa u pogledu eksternalizovanih aktivnosti unutar grupe,
 - 4) adekvatnost uspostavljene organizacione strukture, sistema i procesa, kao i dostatnost resursa koji osiguravaju da banka raspolaže odgovarajućim mehanizmima potrebnima za identifikovanje, mjerenje i upravljanje rizicima.
- (3) U okviru procjene iz stava (2) ovog člana, Agencija će uzeti posebno u obzir:

- a) operativni rizik koji proizilazi iz ugovora o eksternalizaciji ili je povezan sa njima,
 - b) reputacijski rizik,
 - c) rizike koji mogu proisteći iz potrebe da će banka morati poduzimati aktivnosti i preuzimati obaveze u cilju održavanja kontinuiteta poslovanja pružaoca usluge (eng. „step in“ rizik),
 - d) koncentracijski rizik na pojedinačnoj i konsolidiranoj osnovi (unutar banke, odnosno bankarske grupe), uzrokovan većim brojem ugovora o eksternalizaciji sa istim pružaocem usluga ili usko povezanim pružaocima usluga ili većim brojem ugovora o eksternalizaciji unutar istog poslovnog područja,
 - e) koncentracijski rizik na nivou sektora, (npr. ako više banaka koristi istog pružaoca usluga ili malu grupu pružaoca usluga),
 - f) mjeru u kojoj banka koja zahtijeva eksternalizaciju kontroliše pružaoca usluga ili može uticati na njegovo djelovanje, smanjenje rizika do kojeg može doći zbog većeg nivoa kontrole, te da li je pružalac usluge uključen u konsolidovani nadzor bankarske grupe ili grupe društava,
 - g) sukobe interesa između banke i pružaoca usluga.
- (4) Agencija zadržava pravo nalaganja specifičnih uslova, odnosno zabrane eksternalizacije (zahtjev za izlazak iz jednog ili više ugovora) ukoliko procijeni da banka u namjeravanoj i/ili postojećoj eksternalizaciji ne može na odgovarajući način upravljati rizicima koji su povezani sa eksternalizacijom ili održati kontinuitet poslovanja, te ukoliko procijeni da bi eksternalizacija dovela do postojanja rizika prevelike izloženosti banke prema istom pružaocu usluga ili rizika izloženosti više banaka prema istom pružaocu usluga, što može imati potencijalni uticaj na banku ili bankarski sistem u cjelini.
- (5) U slučaju utvrđivanja koncentracijskog rizika, Agencije će pratiti kretanje tog rizika i ocijeniti njegov mogući uticaj na druge banke, te na stabilnost finansijskog tržišta.

Član 31.

Izveštavanje Agencije

- (1) Banka je dužna Agenciji dostaviti sljedeće interne izvještaje i akte:
- a) politiku upravljanja eksternalizacijom definisanu članom 12. ove odluke,
 - b) izvještaje nadzornog odbora banke u vezi s upravljanjem rizicima eksternalizovanih aktivnosti u banci, u skladu sa članom 10. tačka d) ove odluke,
 - c) godišnju procjenu rizika za eksternalizovane aktivnosti u banci, u skladu sa članom 26. st. (2) i (4),
 - d) izvještaje interne revizije o eksternalizovanim aktivnostima, u skladu sa članom 27. ove odluke.
- (2) Banka je dužna izvještaje i procjene iz tačke b), c) i d) iz stava (1) ovog člana dostavljati Agenciji do 5. marta tekuće godine, za prethodnu godinu.
- (3) Politike iz tačke a) stava (1) ovog člana, banka je dužna dostaviti 7 (sedam) dana po usvajanju od strane nadzornog odbora banke.

Član 32.

Prelazne i završne odredbe

- (1) Danom početka primjene ove odluke prestaje da važi Odluka o upravljanju eksternalizacijom u banci („Službene novine Federacije BiH“, broj 81/17).
- (2) Banka je dužna uskladiti svoje poslovanje sa odredbama ove odluke do 31.12.2022. godine.
- (3) Izuzetno od odredbi stava (2) ovog člana, banka je dužna dopuniti dokumentaciju o svim postojećim ugovorima o eksternalizaciji, kao i ugovorima sa trećim stranama, te uskladiti postojeće ugovore sa odredbama ove odluke najkasnije u roku od 12 mjeseci od dana stupanja na snagu ove odluke.

- (4) U slučaju da banka ne izvrši usklađivanje postojećih ugovora o eksternalizaciji u roku propisanim stavom (3) ovog člana, dužna je o tome obavijestiti Agenciju, te o razlozima za navedeno, kao i o mjerama i rokovima planiranim za usklađivanje ili mogućoj izlaznoj strategiji.

Član 33.

Stupanje na snagu

Ova odluka stupa na snagu osmog dana od dana objavljivanja u „Službenim novinama Federacije BiH“.

Broj: U.O.-02-05/22
Sarajevo, 13.09.2022. godine

PREDSJEDNICA
UPRAVNOG ODBORA

Ivanka Galić, dipl.ecc., s.r.