Na temelju čl. 75., 77. i 78. Zakona o bankama ("Službene novine Federacije BiH", broj 27/17), čl. 5. stavak (1) točka h) i 19. stavak (1) točka c) Zakona o Agenciji za bankarstvo Federacije Bosne i Hercegovine ("Službene novine Federacije BiH", broj 75/17) i članka 12. stavak (1) točka 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

O D L U K U
O UPRAVLJANJU EKSTERNALIZACIJOM U BANCI

Članak 1.
Predmet

(1) Odlukom o upravljanju eksternalizacijom u banci propisuju se uvjeti koje je banka dužna osigurati 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, uvjeti 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 daljnjem tekstu: FBiH) kojima je Agencija za bankarstvo Federacije Bosne i Hercegovine (u daljnjem tekstu: Agencija) izdala dozvolu za rad.
(3) Banka je dužna primjenjivati odluku na pojedinačnoj i konsolidiranoj osnovi.
(4) Na pitanja vezana za upravljanje eksternalizacijom i rizicima koji mogu proisteći iz eksternalizacije koja nisu regulirana ovom odlukom, a regulirana su drugim propisima, primjenjivat će se odredbe tog propisa.

Članak 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 pružateljima 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 financijskih usluga, uključujući i aktivnosti kojima se podržava obavljanje tih djelatnosti.
   c) **Rizik eksternalizacije** uključuje sve rizike koji nastaju kada banka ugovorno povjerava pružateljima usluga obavljanje aktivnosti koje bi inače sama obavljala.
   d) **Pružatelj usluga** je treća strana koja obavlja određenu eksternaliziranu aktivnost djelomično ili u cjelini na temelju ugovora zaključenog s bankom, a može biti:
      1) članica bankarske grupe,
      2) pravna osoba koja je prema propisima države u kojoj je osnovana, odnosno u kojoj ima sjedište ovlaštena za obavljanje djelatnosti koje je predmet eksternalizacije ili
      3) fizička osoba koja je prema propisima države u kojoj ima prebivalište ovlaštena za obavljanje djelatnosti koje je predmet eksternalizacije.
   e) **Podeksternalizacija** je situacija u kojoj pružatelj usluga, u okviru određenog ugovora o eksternalizaciji, eksternaliziranu uslugu ili neki njen dio povjerava nekom drugom pružatelju usluga, koji se u tom slučaju označava kao podizvođač pružatelja usluge (u daljnjem 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 informacijskog sustava (npr. mreže, serveri, uređaji za skladištenje

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

g) **Javni oblak** (eng. public cloud) jeste računalna infrastruktura kojoj može pristupiti šira javnost.
h) **Privatni oblak** (eng. private cloud) jeste računalna infrastruktura kojoj može pristupiti samo jedan subjekt.
i) **Zajednički oblak** (eng. community cloud) jeste računalna infrastruktura raspoloživa samo određenom broju subjekata.
j) **Hibridni oblak** (eng. hybrid cloud) jeste računalna infrastruktura koja je sastavljena od dvije ili više različitih računalnih infrastruktura u oblaku (npr. javni i privatni).
k) **Penetracijski test** (eng. penetration testing) predstavlja specijaliziranu vrstu procjene koja se provodi na informacijskom sustavu ili njegovim pojedinim dijelovima, a s 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 razini usluga** (eng. Service Level Agreement SLA) predstavlja formalni ugovor kojim se definira razina kvalitete usluge koju banka očekuje od pružatelja usluge.

(2) Pojmovi koji se koriste u ovoj odluci, a nisu definirani u istoj, imaju značenje kao u Zakonu o bankama i drugim podzakonskim aktima Agencije u kojima su definirani.

Članak 3.
Aktivnosti koje ne predstavljaju eksternalizaciju

U smislu ove odluke, eksternalizacijom se ne smatraju:

a) aktivnosti koje po zakonu obavlja pružatelj usluga (npr. vanjska revizija),
b) usluge globalnih servisa za međubankarsku/financijsku komunikaciju (npr. SWIFT) u slučaju kada se ključni resursi informacijskog sustava 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) sustavi poravnanja i usluge namirenja između klirinških kuća, središnjih drugih ugovornih strana, te institucija za namirenje i njihovih članica,
g) zakup i nabava robe,
h) druge aktivnosti koje banka inače ne obavlja sama (npr. arhitektonske usluge, usluge čišćenja, usluge održavanja objekata, usluge sigurnosti imovine i osoba, usluge osiguranja imovine i osoba, 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-konzultantska mišljenja konzultantskih 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 računala, namještaja i dr.), izvršenje radova, nabavu robe i usluga, usluge vezane uz upotrebu telekomunikacijske infrastrukture i slično).

Članak 4.
Uvjeti za eksternalizaciju

(1) Banka smije eksternalizirati aktivnosti koje joj omogućavaju obavljanje djelatnosti pružanja bankarskih i financijskih usluga, uključujući i aktivnosti kojima se podržava obavljanje tih djelatnosti, pod uvjetima utvrđenim Zakonom, ako eksternalizacija ne narušava:
   a) obavljanje redovnog poslovanja banke, odnosno pružanje usluga korisnicima u skladu s važećim zakonskim i drugim propisima, te dobrom bankarskom praksom,
   b) upravljanje i nadzor nad poslovanjem i aktivnostima banke, uključujući i nad aktivnostima koje su eksternalizirane,
   c) efikasno upravljanje rizicima banke, uključujući rizike informacijske i komunikacijske tehnologije (u daljnjem tekstu: IKT) i rizike financijske tehnologije (FinTech),
   d) sustav unutarnjih kontrola i kontrolne funkcije banke,
   e) obavljanje nadzora od strane Agencije nad eksternaliziranim aktivnostima na lokacijama na kojima će se pružati eksternalizirane usluge, pohranjivati i obrađivati podaci,
   f) mogućnost provedbe izlazne strategije za eksternalizirane aktivnosti, koja uključuje jednu od sljedećih mjera u odgovarajućem primjerenom roku: prijenos aktivnosti na drugog pružatelja usluge, ponovnu integraciju procesa i aktivnosti u banku ili prestanak poslovne aktivnosti.

(2) Banka ne smije eksternalizirati djelatnost pružanja bankarskih i financijskih usluga za koje je dobila dozvolu za rad i ovlaštenje od strane Agencije sukladno 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 obveze organa banke koje su definirane Zakonom.

(4) Banka ostaje potpuno odgovorna i zadužena za osiguravanje usklađenosti sa svim svojim zakonskim i regulatornim obvezama, uključujući sposobnost nadziranja eksternaliziranih aktivnosti.

(5) Banka ne smije eksternalizirati kontrolne funkcije banke koje su definirane Zakonom, osim aktivnosti podrške kontrolnim funkcijama, na način na koji je to definirano unutar bankarske grupe i u čl. 5. i 6. ove odluke.

(6) Odgovornost banke prema trećim osobama ni u kojem slučaju se ne smije prenositi na pružatelje usluga.

Članak 5.
Primjena unutar bankarske grupe

(1) U slučaju eksternalizacije aktivnosti na razini bankarske grupe ili podgrupe, bez obzira je li pružatelj 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 stavka (1) ovoga članka, banka koja je članica bankarske grupe ili podgrupe, dužna je osigurati da su sustavi, postupci i mehanizmi upravljanja eksternalizacijom dosljedno primijenjeni, pravilno integrirani i primjereni za efikasnu primjenu regulatornih zahtjeva iz ove odluke na svim relevantnim razinama.

(3) U slučaju eksternalizacije aktivnosti podrške kontrolnim funkcijama u okviru iste bankarske grupe odnosno podgrupe, a sukladno članku 4. stavak (5) ove odluke, banka treba osigurati, za potrebe praćenja provođenja i revizije ugovora o eksternalizaciji, uspješno provođenje tih aktivnosti, uključujući i putem odgovarajućih izvješća.

(4) U slučaju eksternalizacije materijalno značajne aktivnosti banke na razini bankarske grupe odnosno podgrupe čiji je banka član, a pri čemu je operativno praćenje eksternalizacije centralizirano:
   a) banka je dužna osigurati mogućnost neovisnog provođenja praćenja pružatelja usluga i odgovarajući nadzor, uključujući primanje izvješća o praćenju eksternalizacije, barem

jednom godišnje odnosno na zahtjev, sa sažetkom procjene rizika i praćenja izvršavanja, kao i sažetak relevantnih revizorskih izvješća, a u slučaju zahtjeva, potpuno revizorsko izvješće (osiguravajući pri tome da procjena rizika i nadzor eksternaliziranih aktivnosti obuhvaćaju elemente definirane čl. 16. i 26. ove odluke),

b) banka treba osigurati da organi banke budu pravodobno obaviješteni o relevantnim planiranim promjenama u pogledu pružanja eksternalizirane usluge, te o mogućem utjecaju tih promjena na materijalno značajne aktivnosti banke koje su predmet eksternalizacije, uključujući sažetak analize rizika, među ostalim pravnih rizika, usklađenost s regulatornim zahtjevima i razinom usluge, a kako bi se mogao procijeniti utjecaj tih promjena,
c) u slučaju da se na razini 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 sukladna čl. 15. i 16. ove odluke,
d) u slučaju oslanjanja na izlazni plan koji je uspostavljen na razini 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 eksternaliziranim aktivnostima banke, a koji je definiran člankom 14. ove odluke.

(5) U slučaju eksternalizacije aktivnosti na razini bankarske grupe ili podgrupe čiji je banka član, Agencija zadržava mogućnost obavljanja nadzora eksternaliziranih aktivnosti, sukladno zaključenom sporazumu o suradnji i razmjeni informacija između Agencije i nadležnih tijela odgovornih za nadzor pružatelja usluga, banke/bankarske grupe u matičnoj zemlji.

Članak 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 utjecaj na mogućnost banke da zadovolji zakonske i regulatorne zahtjeve i/ili nastavi svoje poslovanje, odnosno pružanje bankarskih/financijskih usluga,
b) aktivnosti koje mogu imati značajan utjecaj na upravljanje rizicima, sustav unutarnjih kontrola i financijski rezultat banke,
c) aktivnosti koje omogućavaju banci obavljanje osnovnih poslovnih linija i ključnih funkcija, sukladno propisima Agencije koji se odnose na restrukturiranje banaka i sadržaj plana oporavka banke,
d) sve aktivnosti vezane za podršku kontrolnim funkcijama, u skladu s člankom 4. stavak (5) ove odluke,
e) sve bankarske i financijske aktivnosti u mjeri za koju bi bilo potrebno odobrenje za rad Agencije.

Članak 7.
Procjena materijalne značajnosti

(1) Prilikom procjene je li aktivnost koja se eksternalizira materijalno značajna, banka je dužna, pored procjene rizika iz članka 16. ove odluke, uzeti u obzir i sljedeće:

a) je li eksternalizacija direktno povezana s pružanjem bankarskih odnosno financijskih usluga i obavljanjem poslova za koje je banka dobila dozvolu za rad,
b) mogući utjecaj bilo kakvog prekida eksternalizirane aktivnosti ili nemogućnost pružatelja usluga da kontinuirano i na adekvatan način obavlja eksternalizirane aktivnosti na:
   1) kratkoročnu i dugoročnu financijsku otpornost i održivost, uključujući, ako je primjenjivo, njenu imovinu, kapital, troškove, izvore financiranja, 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 utjecaj eksternalizacije na sposobnost banke da:
1) identificira i prati sve rizike te upravlja njima,
2) ispunjava sve zahtjeve propisane zakonskim propisima i podzakonskim aktima,
3) provodi reviziju eksternaliziranih aktivnosti.

d) mogući utjecaj na usluge koje banka pruža klijentima,

e) sve eksternalizacije, ukupnu izloženost banke prema istom pružatelju usluga i mogući kumulativni efekt 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 eksternalizirane aktivnosti bez izmjene ili dopune osnovnog ugovora,

h) mogućnost prijenosa, ugovorno i u praksi, eksternalizacije na drugog pružatelja 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 eksternalizirane aktivnosti unutar banke, ako je to potrebno ili poželjno,

k) zaštitu podataka i mogući utjecaj 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 članku 6. ove odluke i stavku (1) ovoga članka.

(3) Banka smije eksternalizirati materijalno značajne aktivnosti pružateljima usluga definiranim u članku 2. stavku (1) točka d) alineja 1) i 2) ove odluke.

Članak 8.
Uspostava sustava za upravljanje rizikom eksternalizacije

(1) Banka je dužna, kao dio sveobuhvatnog okvira i mehanizama unutarnje kontrole i sustava upravljanja rizicima, uspostaviti efikasno upravljanje rizikom eksternalizacije.

(2) Ispunjenje zahtjeva iz stavka (1) ovoga članka omogućava banci donošenje adekvatnih odluka o preuzimanju rizika eksternalizacije i osigurava provođenje adekvatnih mjera za upravljanje rizikom eksternalizacije, uključujući rizike povezane s kibernetskim napadima koji se smatraju sigurnosnim aspektom rizika IKT-a.

Članak 9.
Sustav za upravljanje rizikom eksternalizacije

(1) Banka je dužna, uzimajući u obzir princip proporcionalnosti, identificirati, procijeniti i pratiti sve rizike koji proizlaze iz ugovora s trećim stranama, kojima jesu ili bi mogle biti izložene, bez obzira da li ugovor predstavlja eksternalizaciju ili ne, te upravljati tim rizicima. Rizike koje proizlaze iz ugovora s trećim stranama, uključujući i IKT i kibernetske rizike, treba procijeniti sukladno članku 16. ove odluke.

(2) Upravljanje rizicima koji proizlaze iz ugovora s trećim stranama treba biti sastavni dio internog sustava upravljanja rizicima banke, sukladno propisima Agencije koji reguliraju oblast upravljanja rizicima u bankama, kao i propisima vezanim za zaštitu osobnih podataka klijenta banke.

(3) Banka je dužna uspostaviti efikasan sustav upravljanja eksternalizacijom i rizikom eksternalizacije, razmjeran profilu rizičnosti, vrsti i poslovnom modelu, veličini i složenosti poslova banke, kao i složenosti eksternaliziranih aktivnosti i rizika koji proizlaze 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 eksternaliziranim aktivnostima, te da eksternalizirane aktivnosti budu na adekvatan način obuhvaćene sustavom unutarnjih kontrola banke.

(5) Banka je dužna:

a) uspostaviti odgovarajuću podjelu nadležnosti, te jasno dodijeliti odgovornosti za dokumentiranje, 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 dokumentiranje 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 povezanima s eksternalizacijom, pri čemu se kod malih i manje složenih banaka odgovornost za eksternalizaciju može dodijeliti i članu uprave,
d) u okviru uspostavljenog okvira (sustava) unutarnje 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 eksternalizirane aktivnosti (vlasnika eksternalizacije).

(6) Banka je dužna u svakom trenutku održavati adekvatnu razinu poslovanja, te minimalno:

a) u svakom trenutku ispunjavati sve uvjete odobrenja za rad, uključujući efikasnost organa banke na izvršavanju dužnosti i odgovornosti propisanih čl. 10. i 11. ove odluke,
b) zadržati odgovarajuću organizacijsku strukturu s jasno definiranim, preglednim i usklađenim odgovornostima unutar banke, te usklađenu sa zakonskim i podzakonskim zahtjevima,
c) ako se eksternaliziraju aktivnosti podrške kontrolnim funkcijama, sukladno članku 4. stavku (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 proizlaze iz eksternalizacije,
d) raspolagati s dovoljnim resursima i kapacitetima za osiguravanje usklađenosti s točkama a) do c) ovoga stavka.

Članak 10.
Dužnosti i odgovornosti nadzornog odbora banke

Nadzorni odbor dužan je, kao minimum:

a) uspostaviti, nadzirati i unapređivati sustav upravljanja eksternalizacijom i rizikom eksternalizacije, te svih drugih rizika povezanih s eksternalizacijom,
b) usvojiti adekvatne strategije, odnosno politiku za upravljanje eksternalizacijom, osigurati uvjete za njihovo provođenje, te nadzirati njihovo provođenje i periodično ih revidirati, a uzimajući u obzir poslovni model banke i sklonost ka preuzimanju rizika,
c) nadzirati provođenje identifikacije, procijene i upravljanja potencijalnim sukobom interesa vezanim uz ugovore s trećim stranama i poduzimati odgovarajuće mjere za eliminiranje sukoba interesa,

d) propisati sadržaj i periodičnost izvješćivanja nadzornog odbora i drugih relevantnih odbora, tijela ili osoba u vezi s eksternaliziranim aktivnostima i rizicima, a najmanje na godišnjoj razini,
e) donijeti odluku o svakoj pojedinačnoj materijalno značajnoj eksternalizaciji,
f) uspostaviti, održavati i unapređivati efikasan sustav unutarnjih kontrola u banci i osiguravati da uprava banke osigura uvjete za njihovo provođenje, odnosno da kontrolne funkcije banke kontinuirano prate i provjeravaju da li se eksternalizacija obavlja sukladno zakonu, ovoj odluci, drugim propisima, strategiji, politikama, procedurama i drugim internim aktima banke.

Članak 11.
Dužnosti i odgovornosti uprave banke

Uprava banke dužna je, kao minimum:
a) pripremati i nadzornom odboru predlagati strategije, odnosno politiku za upravljanje eksternalizacijom, koje je potrebno najmanje jednom godišnje analizirati i prilagoditi promjenama ekonomskih i tržišnih uvjeta,
b) donositi ostale interne akte u vezi s eksternalizacijom,
c) uspostaviti i osigurati primjenu adekvatnih metoda i procedura za identifikaciju, mjerenje, odnosno procjenu, praćenje, analizu i kontrolu rizika eksternalizacije, te svih drugih rizika povezanih s eksternalizacijom,
d) osigurati praćenje ekonomskih i tržišnih uvjeta radi predviđanja mogućih promjena, uključujući financijsko stanje pružatelja usluga,
e) osigurati provođenje efikasnog sustava unutarnje kontrole,
f) osigurati povjerljivost u smislu zaštite podataka i drugih informacija putem ugovora,
g) osigurati uvjete za identifikaciju i uvjete za procjenu potencijalnog sukoba interesa vezanih uz ugovore s trećim stranama,
h) osigurati neometan tok relevantnih informacija s pružateljem usluga,
i) pravodobno osigurati neometano provođenje eksternaliziranih aktivnosti koje su materijalno značajne (npr. kada se ta aktivnost prenosi na drugog pružatelja usluga, kada banka preuzima navedenu aktivnost od pružatelja usluge i slično),
j) uspostaviti i implementirati odgovarajući sustav izvješćivanja o eksternaliziranim aktivnostima.

Članak 12.
Politike i procedure upravljanja eksternalizacijom

(1) Banka je dužna usvojiti, provoditi i redovno ažurirati politiku upravljanja eksternalizacijom.
(2) Politika upravljanja eksternalizacijom treba obuhvatiti sve faze životnog ciklusa ugovora o eksternalizaciji i definira načela, odgovornosti i postupke povezane s eksternalizacijom, te treba obuhvatiti najmanje sljedeće:
   a) jasno definirane 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 osoba u pogledu ugovora o eksternalizaciji,
   c) procedure i postupke koji se provode prije sklapanja ugovora s pružateljem usluga, uključujući:
      1) definiranje poslovnih zahtjeva u pogledu ugovora o eksternalizaciji,
      2) postupke za utvrđivanje ispunjavanja uvjeta za eksternalizaciju propisanih člankom 4. ove odluke,
      3) postupke za utvrđivanje ispunjavanja uvjeta 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 proizlaze iz eksternalizacije, a minimalno uključujući aktivnosti propisane čl. 15. i 16. ove odluke,
6) način provođenja dubinske analize potencijalnih pružatelja usluga, a minimalno uključujući aktivnosti propisane člankom 17. ove odluke,
7) postupke za utvrđivanje i procjenu potencijalnih sukoba interesa, upravljanje tim sukobima i njihovo smanjenje, sukladno propisima kojima je reguliran sustav internog upravljanja u banci i člankom 13. ove odluke,
8) način planiranja kontinuiteta poslovanja, a kako je propisano člankom 22. ove odluke,
9) definiranje načina i kriterija za izbor pružatelja usluga,
10) postupak odobravanja novih ugovora o eksternalizaciji,

d) način provođenja, praćenja i upravljanja ugovorima o eksternalizaciji, uključujući:
1) kontinuiranu procjenu rada pružatelja usluga, u skladu s člankom 26. ove odluke,
2) postupke obavještavanja o promjenama i postupanja banke u slučaju promjene ugovora o eksternalizaciji ili okolnostima u vezi s pružateljem usluga (npr. financijsko stanje, organizacijska ili vlasnička struktura, odnosi s podizvođačima i drugo),
3) neovisnu provjeru usklađenosti sa zakonskim i regulatornim propisima i internim aktima banke od strane funkcije praćenja usklađenosti poslovanja,
4) postupke obnavljanja ugovora,

e) način dokumentiranja i vođenja registra informacija o eksternaliziranim aktivnostima, uzimajući u obzir zahtjeve članka 14. ove odluke,
f) način definiranja izlaznih strategija i postupaka za otkaz ili raskid ugovora, uključujući zahtjev za dokumentirani izlazni plan, a uzimajući u obzir zahtjeve definirane člankom 23. ove odluke,
g) način obavljanja nadzora aktivnosti koje su predmet ugovora, odnosno obveze i odgovornosti nadležnog organizacijskog dijela, osiguravajući adekvatnu razinu znanja i iskustva zaposlenih koji obavljaju nadzor i upravljanje eksternalizacijom,
h) način i periodičnost izvješćivanja organa banke o aktivnostima i rizicima eksternalizacije,
i) sustave izvješćivanja 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 njegova 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) pružateljima usluga koji su pod nadzorom relevantnog nadležnog tijela i onima koji nisu,
d) pružateljima usluga u BiH i eksternalizacija pružateljima usluga u drugim zemljama.

(4) Banka treba osigurati da politika upravljanja eksternalizacijom obuhvaća utvrđivanje sljedećih mogućih utjecaja eksternalizacije, te uzimanje istih u obzir u postupku donošenja odluke:
a) profil rizičnosti,
b) mogućnost nadziranja pružatelja usluge i upravljanje rizicima,
c) utjecaj 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 definirati:

a) odgovornost banke za sve eksternalizirane aktivnosti i odluke o upravljanju koje proizlaze iz njih, jasno navodeći da eksternalizacija ne oslobađa banku od regulatornih obveza i ugovorenih obveza prema klijentu,
b) aktivnosti koje treba poduzeti 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 s nadzornim ograničenjima u pogledu aktivnosti koje su eksternalizirane,
c) unutargrupnu eksternalizaciju (odnosno usluge koje pruža pravni subjekt unutar bankarske grupe) i uzeti u obzir sve posebne okolnosti eksternalizacije na razini bankarske grupe i odluke o upravljanju koje proizlaze iz njih, jasno navodeći da eksternalizacija ne oslobađa banku od regulatornih obveza i obveza prema klijentu,
d) obvezu provjere uspostave odgovarajućih etičkih standarda i kodeksa ponašanja pri odabiru pružatelja usluga materijalno značajnih aktivnosti.

Članak 13.
Sukob interesa

Sukladno propisima kojima je reguliran sustav internog upravljanja u banci, banka je dužna identificirati, procijeniti i upravljati sukobima interesa u pogledu ugovora o eksternalizaciji, uključujući:
a) ako banka utvrdi da iz eksternalizacije proizlaze materijalni sukobi interesa, uključujući između subjekata unutar bankarske grupe, banka je dužna poduzeti odgovarajuće mjere za upravljanje tim sukobima interesa,
b) ako eksternaliziranu aktivnost obavlja pružatelj usluga koji je dio bankarske grupe ili je u vlasništvu grupe ili banke, ili osoba u posebnom odnosu s bankom, uvjete (uključujući financijske uvjete) za eksternalizirane usluge treba utvrđivati po tržišnim uvjetima,
c) u slučaju eksternalizacije iz točke b) ovoga članka, pri određivanju cijena usluga mogu se uzeti u obzir sinergije koje proizlaze iz pružanja istih ili sličnih usluga za nekoliko subjekata unutar bankarske grupe, pod uvjetom da pružatelj usluga ostane samostalno održiv, bez obzira na likvidaciju odnosno tečaj bilo kojeg drugog subjekta bankarske grupe.

Članak 14.
Registar informacija o eksternaliziranim aktivnostima

(1) Banka je dužna dokumentirati 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 s drugim relevantnim zakonima, čuvati dokumentaciju o završenim ugovorima o eksternalizaciji, kao i prateću dokumentaciju.
(2) Banka je dužna voditi ažuran registar informacija o eksternaliziranim aktivnostima svih ugovora o eksternalizaciji, a koji treba sadržavati 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 godišnjoj razini,
d) predmet eksternalizacije, opis eksternaliziranih aktivnosti, podatke koji se eksternaliziraju i informaciju o tome da li se vrši prijenos osobnih podataka i njihova obrada,
e) kategoriju koju dodjeljuje banka, a koja odražava prirodu eksternalizirane aktivnosti u točki d) ovoga stavka (npr. IT informacijske tehnologije (sustav), naziv poslovne aktivnosti i slično),
f) naziv i sjedište pružatelja usluge,

g) zemlju ili zemlje gdje će se usluga obavljati, 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 organizacijskog dijela banke odgovornog za eksternalizaciju,
j) ključno osoblje pružatelja usluge zaduženo za pružanje usluga banci,
k) u slučaju eksternalizacije pružatelju usluga računarstva u oblaku, tip usluge, model upotrebe, vrstu podataka i lokaciju čuvanja podataka,
l) datum posljednje procjene materijalne značajnosti eksternalizirane aktivnosti.

(3) U slučaju eksternalizacije materijalno značajnih aktivnosti, registar informacija o eksternaliziranim aktivnostima, pored podataka/informacija iz stavka (2) ovoga članka, treba sadržavati i sljedeće podatke/informacije:
a) popis svih banaka ili društava unutar iste bankarske grupe koji koriste te eksternalizirane usluge, ukoliko je primjenjivo,
b) podatak je li pružatelj 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 danu eksternalizaciju i pregled glavnih zaključaka,
e) datum posljednje i sljedeće planirane revizije pružatelja usluga, ako je primjenjivo,
f) nazive svih podizvođača kojima je eksternalizirano obavljanje dijelova materijalno značajnih aktivnosti, uključujući zemlju u kojoj je registriran podizvođač, u kojoj će se pružati usluga, i ako je primjenjivo, lokaciju na kojoj će se skladištiti podaci,
g) rezultat procjene zamjenjivosti pružatelja usluga (jednostavno, teško, nemoguće), te mogućnost integracije eksternalizirane materijalno značajne aktivnosti u banku i utjecaj prekida u obavljanju materijalno značajne aktivnosti,
h) identifikaciju alternativnih pružatelja usluga u skladu s točkom g) ovoga stavka,
i) podatak o tome je li eksternalizirana materijalno značajna aktivnost vezana/podržava poslovne aktivnosti koje su vremenski kritične.

Članak 15.
Analiza prije eksternalizacije

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

ili bi mogao imati veze s eksternalizacijom, te mogućnost direktnog nadzora same eksternalizacije koja je predmet ugovora, a u svrhu postizanja ciljeva supervizije,

h) identificirati i procijeniti sukobe interesa koji bi mogli proizaći iz eksternalizacije, te poduzeti odgovarajuće mjere za upravljanje tim sukobima interesa, sukladno propisima kojima je reguliran sustav internog upravljanja u banci i članku 13. ove odluke.

(2) Odluka o eksternalizaciji treba biti usklađena s poslovnom strategijom i ciljevima banke i sadržati obrazloženje koje obuhvaća detaljan opis aktivnosti koje se namjeravaju eksternalizirati i razloge donošenja odluke o eksternalizaciji.

(3) U slučaju nabave resursa informacijskog sustava, 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 eksternaliziranu aktivnost, banka je dužna, prije same kupovine navedenog resursa, prijaviti predmetnu eksternalizaciju Agenciji i postupiti sukladno odredbama ove odluke.

Članak 16.
Procjena rizika koji proizlaze iz ugovora o eksternalizaciji

Banka je dužna, prije donošenja odluke o eksternalizaciji, kao i tijekom praćenja rada pružatelja usluge, identificirati i procijeniti sve rizike koji proizlaze iz eksternalizacije, a najmanje:

a) identificirati i razvrstati relevantne aktivnosti i povezane podatke i sustave s obzirom na njihovu osjetljivost i potrebne mjere zaštite,

b) provesti detaljnu analizu aktivnosti i povezanih podataka i sustava koje obuhvaća 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 eksternalizirane usluge i u kojima su pohranjeni ili će se vjerojatno pohraniti podaci,

c) pregledati politike upravljanja rizicima i, ako je primjenjivo, kontrole informacijskog sustava, kao i kontrolno okruženje kod pružatelja usluga, a kako bi osigurala da oni zadovoljavaju interne ciljeve upravljanja rizicima banke i prihvatljive razine rizika,

d) u okviru procjene operativnog rizika, za materijalno značajne eksternalizirane aktivnosti, treba uključivati, prema potrebi, scenarije mogućih događaja povezanih s rizikom, uključujući događaje s velikim gubicima. U okviru analize scenarija, banka treba procijeniti mogući utjecaj prekida pružanja usluga ili neadekvatnog pružanja usluga, uključujući rizike koji proizlaze iz neuspješnih ili neadekvatnih procesa, sustava, ljudi ili vanjskih događaja. Banka je dužna, uzimajući u obzir princip proporcionalnosti, dokumentirati navedene izvršene analize i njihove rezultate, te procjene u kojoj mjeri bi eksternalizacija povećala odnosno smanjila operativni rizik. Navedena analiza bi trebala uključivati upotrebu unutarnjih i vanjskih podataka o gubicima, ako su dostupni,

e) razmotriti utjecaj lokacije pružatelja usluga (u BiH ili izvan BiH), moguća ograničenja u pogledu nadzora povezanih sa zemljama u kojima će se pružati eksternalizirane 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 pružatelja usluga, te sva ograničenja do kojih bi došlo s obzirom na hitan oporavak podataka banke,

g) definirati adekvatnu razinu zaštite povjerljivosti podataka, kontinuiteta eksternaliziranih aktivnosti kod pružatelja usluga, te integriteta i sljedivosti (mogućnosti praćenja) podataka i sustava 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 s adekvatnom arhitekturom upravljanja ključevima. U okviru procjene kontinuiteta poslovanja pružatelja usluge, banka je dužna procijeniti usklađenost kontinuiteta poslovanja

pružatelja usluga u vezi s uslugama koje će se eksternalizirati te usuglašenost s 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 proisteći iz predloženog ugovora, a uzimajući u obzir najmanje:
   1) rizik koncentracije koji proizlazi iz eksternalizacije značajnom pružatelju usluga kojeg nije jednostavno zamijeniti i većeg broja ugovora o eksternalizaciji sklopljenih sa istim pružateljem usluga ili povezanim pružateljima usluga,
   2) ukupne rizike koji proizlaze iz eksternaliziranih aktivnosti banke, kao i ukupne rizike na konsolidiranoj osnovi,
   3) rizik koji može proizaći iz potrebe pružanja financijske podrške pružatelju usluga koji se suočava s poteškoćama ili zbog potrebe preuzimanja njegovih poslovnih djelatnosti,
   4) mjere koje provodi banka s ciljem upravljanja rizicima i njegovog smanjivanja.

i) uzeti u obzir činjenicu je li pružatelj usluga matično društvo ili podređeno društvo banke odnosno bankarske grupe ili grupe društava kojoj banka pripada, je li 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 kontrolira ili može utjecati na njegove radnje, sukladno članku 5. ove odluke,

j) ako ugovor o eksternalizaciji materijalno značajne aktivnosti uključuje mogućnost da pružatelj usluga angažira podizvođača, banka je dužna uzeti u obzir sve povezane rizike, uključujući dodatne rizike koji mogu nastati ako je lokacija podizvođača u zemlji različitoj od one u kojoj je pružatelj usluga, kao i rizike smanjenja efikasne sposobnosti nadziranja eksternalizirane aktivnosti od strane banke ili nadzora Agencije u slučaju dugih i složenih lanaca podizvođača.

Članak 17.
Dubinska analiza pružatelja usluge

(1) Prije zaključenja ugovora o eksternalizaciji aktivnosti, banka je dužna, u okviru svojih postupaka odabira i procjene, utvrditi primjerenost pružatelja usluga, odnosno utvrditi da pružatelj usluga ima poslovni ugled, odgovarajuće i dovoljne sposobnosti, stručnost, kapacitete, resurse (npr. ljudske, IKT, financijske resurse), te da je registriran odnosno ima dozvolu nadležnog tijela za obavljanje predmetne eksternalizirane aktivnosti.

(2) U slučaju eksternalizacije materijalno značajnih aktivnosti, banka treba provesti dubinsku analizu pružatelja usluga koja treba uključivati, između ostaloga, i sljedeće:
   a) analizu poslovnog modela potencijalnog pružatelja usluga, prirodu, veličinu, složenost, financijsko stanje i vlasničku strukturu odnosno strukturu grupe,
   b) dugoročne odnose s pružateljima usluga koji su već procijenjeni i pružaju usluge banci,
   c) analizu stručnosti ključnog osoblja pružatelja usluga koji će biti odgovorni za pružanje eksternalizirane usluge banci,
   d) je li pružatelj usluga pod nadzorom nadležnih tijela.

(3) Ako eksternalizacija uključuje obradu osobnih ili povjerljivih podataka, banka se treba uvjeriti da pružatelj usluga provodi odgovarajuće tehničke i organizacijske mjere potrebne za zaštitu podataka.

(4) Banka treba poduzeti odgovarajuće korake kako bi utvrdila postupaju li pružatelji usluga sukladno njenim korporativnim vrijednostima i kodeksu ponašanja. Naročito, kada je riječ o pružateljima usluga u drugim zemljama i, ako je primjenjivo, njihovim podizvođačima, banka se treba uvjeriti da pružatelj usluga posluje na etički i društveno odgovoran način.

Članak 18.
Dokumentiranost

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

Članak 19.
Ugovorni odnos banke i pružatelja usluga

(1) Pri sklapanju ugovora s pružateljem usluga banka je dužna voditi računa o tome da ugovorne odredbe prema svom opsegu i sadržaju budu odgovarajuće, odnosno razmjerne rizicima eksternalizacije, te opsegu i složenosti eksternaliziranih aktivnosti.
(2) Banka je dužna s pružateljem usluga sklopiti ugovor u pisanom obliku, kojim će jasno definirati svi relevantni pojmovi, uvjeti, prava, obveze i odgovornosti ugovornih strana.
(3) Ugovor o eksternalizaciji aktivnosti koje nisu materijalno značajne treba, kao minimum, sadržavati sljedeće:
   a) jasan i detaljan opis usluga koje su predmet ugovora,
   b) mjesto, vrijeme i način ispunjavanja ugovornih obveza,
   c) datum početka i datum završetka, odnosno trajanje ugovora, te otkazne rokove za pružatelja usluga i za banku,
   d) opis očekivane kvalitete i razine usluga,
   e) financijske obveze ugovornih strana,
   f) način nadzora obavljanja aktivnosti koje su predmet ugovora od strane banke na kontinuiranoj osnovi, te obvezu izvješćivanja banke od strane pružatelja usluga,
   g) obvezu pružatelja 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, sustavima, mrežama, informacijama i podacima, koji se koriste za pružanje eksternalizirane aktivnosti, odnosno koji se mogu dovesti u vezi s pružanjem eksternaliziranih aktivnosti, kao i svim povezanim financijskim informacijama, odgovornim osobama i vanjskim revizorima pružatelja usluge,
   h) obvezu pružatelja usluga da surađuje s Agencijom, uključujući i drugim osobama koje ona imenuje,
   i) obvezu pružatelja usluga da neće trećim osobama otkriti ili objaviti posjetu od strane Agencije,
   j) obvezu čuvanja bankovne i poslovne tajne, te obvezu čuvanja i način zaštite povjerljivih podataka, a u skladu s propisima,
   k) odredbe u pogledu pravodobnog otklanjanja sigurnosnih rizika i drugih nedostataka identificiranih u pružanju usluge (na zahtjev banke ili po nalogu Agencije),
   l) obvezu pružatelja usluga da prije zaključenja ugovora s podizvođačem zatraži prethodnu pisanu suglasnost banke, te da osigura da je ugovor pružatelja usluga s podizvođačem usuglašen sa stavkama ugovora banke i pružatelja usluga,
   m) obvezu pružatelja usluga da pravodobno obavijesti banku o svim činjenicama i promjenama okolnosti koje značajno utječu, ili bi mogle značajno utjecati, na sposobnost pružatelja usluga da efikasno izvršava eksternaliziranu aktivnost sukladno dogovorenoj razini usluge i sukladno primjenjivim zakonima i regulatornim zahtjevima, uključujući i izvješćivanje o fluktuaciji ključnog osoblja pružatelja usluga,

n) detaljan opis uvjeta za raskid i/ili otkaz ugovora, uključujući pravo banke da raskine, odnosno otkaže ugovor s pružateljem usluga (na zahtjev banke ili po nalogu Agencije), sukladno članku 21. ove odluke,
o) detaljan opis prava i obveza ugovornih strana u slučaju prijevremenog prestanka ugovora radi osiguranja kontinuiteta pružanja usluga,
p) izbor mjerodavnog prava,
q) način rješavanja sporova.

(4) Ugovor o eksternalizaciji materijalno značajnih aktivnosti, pored točaka iz stavka (3) ovoga članka, treba sadržavati i sljedeće:
a) opis očekivane kvalitete i razine usluga, a što treba uključivati precizne kvantitativne i kvalitativne ciljeve uspješnosti za eksternaliziranu aktivnost, kako bi se omogućilo adekvatno i pravodobno praćenje te time i poduzimanje odgovarajućih korektivnih mjera ako se ne postigne dogovorena razina usluge,
b) lokaciju gdje će se aktivnost izvršavati, uključujući obradu podataka i eventualno skladištenje podataka i uvjete koji se moraju ispuniti, te zahtjev o obavještavanju banke ukoliko pružatelj usluge ima namjeru promijeniti lokaciju obavljanja aktivnosti,
c) odredbe o mogućnosti angažiranja podizvođača, kao i uvjete pod kojima je dopuštena podeksternalizacija, a u skladu s člankom 20. ove odluke:
d) zahtjeve u pogledu uvođenja i testiranja planova poslovanja u kriznim situacijama,
e) potrebu da pružatelj usluga poduzme obvezne mjere osiguranja od određenih rizika, te prema potrebi, razinu pokrića osiguranja koje se traži,
f) odredbe u pogledu pristupa podacima, dostupnosti, integriteta, privatnosti i sigurnosti relevantnih podataka, a kako je navedeno u članku 24. ove odluke,
g) detaljan opis prava i obveza ugovornih strana u slučaju pokretanja postupka restrukturiranja banke, posebno uzevši u obzir ovlaštenja Agencije iz Zakona, uključujući i nemogućnost jednostranog raskida ugovora od strane pružatelja eksternalizirane usluge zbog pokretanja postupka restrukturiranja nad bankom, pod uvjetom da se obveze plaćanja i isporuke i dalje izvršavaju,
h) ključno osoblje pružatelja usluge koje je zaduženo za pružanje usluga banci,
i) odredbe kojima se osigurava pravo pristupa i raspolaganja bančinim podacima, a koji su u posjedu pružatelja usluga, u slučaju stečaja, restrukturiranja ili prekida poslovnih aktivnosti pružatelja usluga,
j) obvezu pružatelja usluga da treba biti pravodobno usuglašen s regulatornim zahtjevima i industrijskim standardima, gdje je to primjenjivo.

Članak 20.
Angažiranje podizvođača

(1) U ugovoru s pružateljem usluga, banka je dužna definirati mogućnost angažiranja podizvođača, a sukladno članku 19. stavak (4) točka c) ove odluke.
(2) U slučaju da je dopuštena podeksternalizacija materijalno značajne aktivnosti, banka je dužna utvrditi je li 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 eksternaliziranim aktivnostima propisan člankom 14. ove odluke.
(3) Ako se radi o podeksternalizaciji koja je ocijenjena materijalno značajnim dijelom eksternalizacije, sukladno stavku (2) ovoga članka, banka je dužna, u okviru ugovora s pružateljem usluga, definirati sljedeće:
a) sve vrste aktivnosti koje su isključene iz podeksternalizacije,
b) uvjete koje je potrebno ispuniti u slučaju podeksternalizacije,
c) obvezu pružatelja usluga da nadzire usluge koje je podugovorio kako bi se osiguralo kontinuirano ispunjavanje svih ugovornih obveza između pružatelja usluga i banke,

d) obvezu pružatelja usluge da u pisanom obliku i sukladno ugovorenim rokovima obavijesti banku o svakom planiranom angažiranju ili izmjeni podizvođača ili značajnim promjenama u obavljanju podeksternalizirane usluge, posebno ukoliko one mogu utjecati na sposobnost pružatelja usluga da ispuni svoje obveze iz ugovora o eksternalizaciji, navedena obavijest treba najmanje sadržavati detaljan opis aktivnosti koje će biti prenesene na podizvođača, kao i mjesto, vrijeme i način obavljanja dijela podeksternalizirane aktivnosti, uključujući lokaciju, gdje će se aktivnosti izvršavati, lokaciju obrade podataka i eventualnog skladištenja podataka,
e) obvezu pružatelja usluga da prije podeksternalizacije podataka pribavi posebno ili opće pisano odobrenje od banke,
f) odredbu kojom se zahtijeva izričito odobrenje banke za angažiranje podizvođača, planiranu izmjenu podizvođača ili značajnu promjenu,
g) mogućnost banke da raskine ugovor u slučaju da prijenos usluga na podizvođača povećava rizike kojima je banka izložena samom eksternalizacijom ili ako pružatelj usluga izvrši angažiranje, odnosno izmjenu podizvođača bez pisane suglasnosti banke.

(4) Banka može dopustiti podeksternalizaciju samo pod sljedećim uvjetima:
a) da pružatelj usluga osigura da je ugovor pružatelja usluga s podizvođačem usuglašen s ugovornim odredbama banke i pružatelja usluga,
b) da pružatelj usluga osigura da podizvođač ispunjava sve zahtjeve definirane ugovorom, ovom odlukom, drugim zakonskim i podzakonskim propisima,
c) da podizvođač osigura prava pristupa i nadzora banci i Agenciji, kao što je osigurao pružatelj usluga.

(5) Banka je dužna osigurati da pružatelj usluga na odgovarajući način nadzire podizvođača usluga, sukladno politici koju definira banka. Ako bi namjeravana podeksternalizacija mogla značajno negativno utjecati na ugovor o eksternalizaciji materijalno značajne aktivnosti ili bi dovela do materijalno značajnog povećanja rizika, uključujući ako se ne bi ispunili uvjeti iz stavka (4) ovoga članka, banka treba ostvariti svoje pravo na otkaz ugovora.

Članak 21.
Pravo na otkaz

(1) Ugovor o eksternalizaciji mora sadržavati ugovornu odredbu koja omogućava banci otkazivanje ugovora u skladu s mjerodavnim pravom, a uključujući i sljedeće situacije:
a) ako pružatelj usluga krši ugovoreno pravo, propise ili ugovorne odredbe, uključujući dogovorenu razinu usluge,
b) ako se utvrde realizirani rizici, nastali gubici, odnosno prepreke koje bi mogle izmijeniti način obavljanja eksternalizirane aktivnosti,
c) ako postoje materijalno značajne promjene koje utječu na eksternalizaciju ili pružatelja usluga (promjena podizvođača za obavljanje aktivnosti koje je procjenjuju kao materijalno značajne bez prethodne suglasnosti banke, a sukladno članku 20. odluke, povećana fluktuacija osoblja, značajno smanjenje broja zaposlenih, promjena fizičke lokacije obavljanja usluge, negativni publicitet za koji banka procijeni da utječe značajno na reputaciju banke, istek licenci za koje je zadužen podizvođač i sl.),
d) ako postoje slabosti u pogledu upravljanja povjerljivim, osobnim ili na drugi način osjetljivim podacima ili informacijama ili u pogledu njihove sigurnosti,
e) ako ugovor nije u skladu s 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 definirati postupak prijenosa eksternalizacije na drugog pružatelja usluga ili vraćanja aktivnosti unutar banke. U tu svrhu pisanim ugovorom o eksternalizaciji treba:

a) jasno utvrditi obveze postojećeg pružatelja usluga u slučaju prijenosa eksternalizirane aktivnosti na drugog pružatelja usluga ili vraćanja aktivnosti unutar banke, uključujući obveze u pogledu postupanja s podacima,
b) utvrditi odgovarajući otkazni rok kako bi se smanjio rizik prekida obavljanja eksternalizirane aktivnosti,
c) utvrditi obvezu pružatelja usluga da pruži podršku banci prilikom prijenosa aktivnosti, na odgovarajući način, u slučaju raskida i/ili otkaza ugovora o eksternalizaciji.

Članak 22.
Planovi kontinuiteta poslovanja

(1) Banka je dužna uspostaviti, održavati i redovno testirati odgovarajuće planove kontinuiteta poslovanja u pogledu eksternaliziranih materijalno značajnih aktivnosti, uzimajući u obzir i planove kontinuiteta poslovanja pružatelja usluga (uključujući i podizvođače), njihovu usuglašenost s planovima kontinuiteta poslovanja banke, te se uvjeriti u njihovu izvodivost.
(2) U okviru redovnog testiranja kontinuiteta poslovanja iz stavka (1) ovoga članka, banka je dužna uključiti i scenarij vezan za nemogućnost pružatelja usluga (uključujući i podizvođača usluga) da na adekvatan način obavlja eksternalizirane materijalno značajne aktivnosti.
(3) Planovi kontinuiteta poslovanja trebaju uzeti u obzir i mogućnost stečaja ili likvidacije pružatelja usluga ili utjecaj relevantnih rizika na poslovanje pružatelja usluge (uključujući i podizvođača usluge), npr. politički rizici u državi pružatelja usluga.

Članak 23.
Izlazna strategija

(1) Banka je dužna za svaku eksternaliziranu aktivnost, donijeti izlaznu strategiju i postupke, koji su sukladni politici upravljanja eksternalizacijom i planovima kontinuiteta poslovanja banke, a uzimajući u obzir najmanje sljedeće mogućnosti:
a) otkaz ugovora o eksternalizaciji,
b) stečaj ili likvidaciju pružatelja usluga,
c) narušavanje kvalitete obavljanja eksternaliziranih aktivnosti, potencijalnih poslovnih poremećaja prouzrokovanih neodgovarajućim ili neuspješnim obavljanjem eksternaliziranih aktivnosti,
d) nastanak ili povećanje materijalno značajnih rizika koji ugrožavaju adekvatno i kontinuirano obavljanje aktivnosti.
(2) Izlazna strategija treba uključiti najmanje sljedeće:
a) definiranje ciljeva izlazne strategije, uključujući strategiju nastavka obavljanja eksternalizirane aktivnosti od strane drugog pružatelja usluga ili vraćanje aktivnosti unutar banke, te osiguravanje uvjeta za njihovo provođenje,
b) analizu utjecaja na poslovanje proporcionalnu riziku eksternaliziranih aktivnosti, a kako bi se utvrdili potrebni financijski 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 prijenosom aktivnosti,
d) definiranje kriterija po kojima se ocjenjuje je li prijenos aktivnosti i podataka izvršen na adekvatan i uspješan način,
e) parametre koji će se primjenjivati za praćenje obavljanja aktivnosti koje su predmet nadzora (eksternalizirane aktivnosti), sukladno članku 26. ove odluke, uključujući i definiranje indikatora neprihvatljive razine 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 s 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, dokumentirani i, prema potrebi, testirani (npr. provođenjem analize mogućih troškova, efekata, resursa i vremenskih aspekata prijenosa eksternalizirane aktivnosti),
b) identificiranje alternativnih rješenja i izradu prelaznih planova prijenosa eksternalizirane aktivnosti na drugog pružatelja usluga ili integraciju aktivnosti u banku, ili poduzimanje drugih mjera kojima se osigurava kontinuirano obavljanje eksternalizirane aktivnosti na kontroliran 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 tijekom prelazne faze.

Članak 24.
Sigurnost sustava i podataka

(1) Banka je dužna osigurati da pružatelji usluga odnosno podizvođači, kad je to relevantno, poštuju odgovarajuće standarde IKT sigurnosti, uključujući preporuke proizvođača softvera, odnosno hardvera, 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 eksternalizirane aktivnosti.
(2) Banka je dužna u ugovoru o eksternalizaciji utvrditi zahtjeve u pogledu sigurnosti podataka i sustava, te kontinuirano pratiti usklađenost s 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 pružateljima usluga računarstva u oblaku i drugih ugovora o eksternalizaciji koji uključuju rukovanje osobnim ili povjerljivim podacima, te njihov prijenos, 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 obvezu pružatelja usluga da čuva povjerljive, osobne 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 osobnih podataka i poštovanje bankarske tajne ili sličnih zakonskih i regulatornih obveza u pogledu povjerljivosti koje se odnose na informacije o klijentima, ukoliko je primjenjivo). Ukoliko se lokacija za pohranu i obradu podataka nalazi izvan teritorija 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.

Članak 25.
Pravo pristupa podacima i pravo na reviziju eksternaliziranih 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 pružatelja usluga i podizvođača, od strane banke, Agencije ili trećih osoba 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 izvješća unutarnjih i vanjskih revizora koji se odnose na eksternalizirane aktivnosti budu dostupna 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 temelju pristupa zasnovanog na

procjeni rizika, a uzimajući u obzir odredbe članka 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 organizirane zajedno s drugim klijentima istog pružatelja 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 pružatelju usluga smanjilo organizacijsko opterećenje,
   b) certifikate i revizorska izvješća trećih strana ili izvješća unutarnje revizije koje je pružatelj usluga stavio na raspolaganje.

(6) Ukoliko se radi o materijalno značajnim aktivnostima, banka treba procijeniti jesu li certifikati i izvješća trećih strana, navedeni u stavku (5) točka b) ovoga članka, adekvatni i dovoljni za ispunjavanje regulatornih zahtjeva, pri čemu se ne treba dugoročno oslanjati samo na ova izvješća.

(7) Banka može koristiti metodu iz stavka (5) točke b) ovoga članka samo u sljedećim slučajevima:
   a) ako je plan revizije za eksternaliziranu aktivnost adekvatan,
   b) ako osigura da opseg certifikacije ili revizorskog izvješća uključuje sustave (postupke, aplikacije, infrastrukturu, informatičke centre i drugo) i kontrole koje je banka identificirala kao ključne, kao i usklađenost s relevantnim regulatornim zahtjevima,
   c) ako detaljno i kontinuirano pregleda sadržaj i obuhvat revizorskih izvješća 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 dosjeu i sl.) adekvatna,
   e) ako se uvjerila da se certifikati izdaju i revizije provode u skladu s međunarodnim relevantnim profesionalnim standardima, te uključuju testiranje operativne efikasnosti postojećih ključnih kontrola,
   f) ako ima ugovorno pravo zatražiti proširenje obuhvata certifikacije ili revizorskih izvješća na druge relevantne sustave 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 eksternaliziranih aktivnosti.

(8) Banka je dužna, kada je to relevantno, osigurati provođenje penetracijskih testova eksternalizirane 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 pravodobno obavijestiti pružatelja usluga o obavljanju nadzora odnosno revizije na lokaciji pružatelja 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 s više klijenata trebaju se poduzeti mjere kojima se izbjegavaju ili ublažavaju rizici za okruženje nekog drugog klijenta (npr. utjecaj na razinu usluge, raspoloživost podataka, povjerljivost i sl.).

(11) Ako eksternalizacija podrazumijeva visoku razinu tehničke složenosti, na primjer u slučaju eksternalizacije usluga računarstva u oblaku, banka treba provjeriti ima li subjekt koji provodi reviziju, bez obzira na to radi li se o njenim unutarnjim revizorima, grupi revizora ili vanjskim revizorima, odgovarajuće i relevantne vještine i znanja za efektivno provođenje relevantne revizije i/ili procjena. Isto se odnosi i na osobe u banci koje obavljaju pregled revizorskih izvješća i certifikate trećih strana.

Članak 26.
Nadzor eksternaliziranih aktivnosti

(1) Banka je dužna poduzeti odgovarajuće mjere i konstantno osiguravati da eksternalizirane aktivnosti zadovoljavaju standarde kvalitete koji bi bili primijenjeni u slučaju obavljanja istih aktivnosti unutar banke.
(2) Banka je dužna redovno ažurirati svoje procjene rizika, kao i materijalnu značajnost eksternalizirane usluge, sukladno čl. 6., 7. i 16. ove odluke, a najmanje jednom godišnje, i obavezno prilikom značajne promjene u pružanju eksternalizirane 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 pružatelja 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 sustava. U slučaju promjene rizika, prirode ili veličine eksternalizirane aktivnosti, banka je dužna ponovno procijeniti materijalnu značajnost eksternalizirane aktivnosti, sukladno čl. 6. i 7. ove odluke.
(4) Pri tome je banka dužna:
   a) osigurati da joj pružatelji usluga dostavljaju odgovarajuća izvješća, s unaprijed definiranim sadržajem/strukturom, vremenskoj periodičnosti i definiranom načinu,
   b) ocjenjuje rad pružatelja usluga na temelju ključnih pokazatelja uspješnosti, ključnih pokazatelja kontrole, izvješća o isporuci usluge, relevantnih certifikata i izvješća o neovisnim provjerama,
   c) prati i analizira sve druge relevantne informacije primljene od pružatelja usluge, uključujući planove kontinuiteta poslovanja i izvješća o njihovom testiranju, te ako je relevantno, informacije o kontrolnom okruženju pružatelja usluga, te broju i vrsti incidenata u informacijskom sustavu pružatelja usluga, uključujući informacije o cyber napadima, te adekvatnost odgovora na iste.
(5) Banka je dužna poduzeti odgovarajuće mjere ako identificira nedostatke u pružanju eksternalizirane aktivnosti.
(6) U slučaju naznake da pružatelj usluga ne obavlja materijalno značajnu aktivnost efikasno, sukladno ugovoru ili sukladno primjenjivim zakonima i regulatornim zahtjevima, banka je dužna poduzeti odgovarajuće mjere koje mogu uključivati i otkaz ugovora o eksternalizaciji s trenutnim efektom.

Članak 27.
Unutarnja revizija eksternaliziranih aktivnosti

(1) Funkcija unutarnje revizije banke dužna je redovno obavljati reviziju eksternaliziranih aktivnosti i o tome izvješćivati odbor za reviziju i nadzorni odbor. Planom i programom rada unutarnje revizije u ovom segmentu treba definirati učestalost i predmet revizije, a na temelju pristupa zasnovanog na procjeni rizika koji proizlaze iz eksternalizacije. Bez obzira na rezultat procjene rizika, materijalno značajne eksternalizacije visoke razine rizika moraju biti predmetom revizije na godišnjoj razini, dok sve materijalno značajne eksternalizacije trebaju biti predmetom revizije najmanje jednom u pet godina.
(2) Revizijom iz stavka (1) ovoga članka, 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 s primjenjivim zakonskim propisima i podzakonskim aktima donesenim na temelju zakona, strategijom rizika i odlukama organa banke,
   b) adekvatnost, kvalitetu i efektivnost procjene materijalno značajnih aktivnosti,

c) adekvatnost, kvalitetu 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 eksternaliziranim aktivnostima,
f) adekvatnost kontrolnog okruženja kod pružatelja usluga i/ili podizvođača, gdje je to primjenjivo, uzimajući u obzir odredbe članka 25. ove odluke.

Članak 28.
Obavještavanje Agencije

(1) Ako banka namjerava eksternalizirati 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 obavijesti, odnosno kompletne propisane dokumentacije iz članka 29. ove odluke, utvrđuje jesu li ispunjeni uvjeti za eksternalizaciju sukladno zakonskim i podzakonskim propisima i o rezultatima procjene obavještava banku.
(3) Banka, nakon dobivanja obavijesti da su ispunjeni uvjeti za eksternalizaciju iz stavka (2) ovoga članka, može sklopiti ugovor o materijalno značajnoj eksternalizaciji.
(4) Banka je dužna, u slučaju materijalno značajnih aktivnosti, pravodobno obavijestiti Agenciju o svakoj značajnoj promjeni (uključujući i angažiranje ili zamjenu angažiranih 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 izvješće o načinu obavljanja aktivnosti, odnosno budućim planovima za nastavak obavljanja eksternaliziranih aktivnosti.
(6) Banka je dužna pravodobno obavijestiti Agenciju u slučaju promjene materijalne značajnosti prethodno eksternalizirane aktivnosti, te dostaviti procjene rizika navedene u čl. 6., 7. i 16. ove odluke.

Članak 29.
Potrebna dokumentacija za obavještavanje o materijalno značajnim aktivnostima

U slučaju namjere eksternalizacije materijalno značajne aktivnosti, banka je dužna, uz obavijest u skladu s člankom 28. ove odluke, dostaviti Agenciji sljedeće dokumente:
a) nacrt odluke nadzornog odbora banke o eksternalizaciji, s obrazloženjem koje sadrži opis aktivnosti koje se eksternaliziraju i razlog eksternalizacije,
b) izvod iz sudskog ili drugog odgovarajućeg registra, iz kojeg se može utvrditi vlasnička struktura pružatelja usluge, u originalu ili ovjerenoj kopiji, ne stariji od šest mjeseci od dana dostavljanja odluke definirane točkom a),
c) popis osoba u posebnom odnosu s bankom, koje su ujedno povezane s pružateljem usluga, te opis načina na koji su povezani,
d) revizorsko izvješće pružatelja usluga za prethodnu kalendarsku godinu, odnosno posljednje raspoloživo, a ukoliko pružatelj usluga ne podliježe obvezi revizije financijskih izvještaja, posljednje raspoložive kopije bilance stanja i računa dobiti i gubitka pružatelja usluga,
e) dokaz o dosadašnjem iskustvu pružatelja usluga na poslovima koji su predmet eksternalizacije,
f) dokaz da nije otvoren stečajni postupak, odnosno postupak likvidacije pružatelja usluga,
g) nacrt ugovora, koji sadrži elemente definirane ovom odlukom, koji banka namjerava sklopiti s pružateljem usluga u vezi s eksternalizacijom materijalno značajnih aktivnosti,

h) procjenu ispunjenosti uvjeta za eksternalizaciju iz članka 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,
   2) pravodoban i neograničen pristup dokumentaciji i podacima koji su povezani s eksternalizacijom, a u posjedu su pružatelja usluga,
i) procjenu ispunjenosti uvjeta za eksternalizaciju unutar bankarske grupe definiranih čl. 5. ove odluke, ako je primjenjivo,
j) procjenu materijalne značajnosti eksternalizacije iz čl. 6. i 7. ove odluke,
k) procjenu rizika povezanih s eksternalizacijom, uključujući procjenu rizika definiranu čl. 15. i 16. ove odluke,
l) dubinsku analizu pružatelja usluga, u skladu s člankom 17. ove odluke,
m) izlaznu strategiju banke, u skladu s člankom 23. ove odluke,
n) detaljan opis tehničkih i organizacijskih rješenja koja omogućuju sigurno i kvalitetno obavljanje aktivnosti koje se namjeravaju eksternalizirati, uključujući opis načina zaštite povjerljivosti, raspoloživosti i integriteta podataka,
o) izjavu banke da članovi organa banke nisu u direktnom ili indirektnom interesu s pružateljem usluga, te da ne postoji nikakva druga vrsta sukoba interesa,
p) podatke sadržane u registru informacija o eksternaliziranim aktivnostima definiranom člankom 14. ove odluke,
r) izvješće funkcije Usklađenosti poslovanja o usklađenosti predmetnog Ugovora s ovom odlukom,
s) ostale akte koje banka smatra važnim za predmetnu eksternalizaciju,
t) listu dostavljene dokumentacije s referencama na odgovarajuće odredbe čl. 19. i 29. ove odluke.

Članak 30.
Postupci Agencije

(1) Prilikom procjene adekvatnosti upravljanja rizikom eksternalizacije, osim dokumentacije iz članka 29. ove odluke, Agencija može zatražiti i drugu dokumentaciju, za koju smatra da je potrebna za procjenu ispunjenosti uvjeta 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 uvjeta i obveza iz inicijalnog odobrenja za rad koje je izdato banci,
   b) mogućnost adekvatnog nadzora banke uključujući nadzor nad eksternaliziranim aktivnostima, te mogućnost direktnog nadzora i prava pristupa eksternaliziranim 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 eksternaliziranih aktivnosti unutar grupe,
      4) adekvatnost uspostavljene organizacijske strukture, sustava i procesa, kao i dostatnost resursa koji osiguravaju da banka raspolaže odgovarajućim mehanizmima potrebnima za identificiranje, mjerenje i upravljanje rizicima.
(3) U okviru procjene iz stavka (2) ovoga članka, Agencija će uzeti posebno u obzir:

a) operativni rizik koji proizlazi 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 obveze u cilju održavanja kontinuiteta poslovanja pružatelja usluge (eng. „step in“ rizik),
d) koncentracijski rizik na pojedinačnoj i konsolidiranoj osnovi (unutar banke, odnosno bankarske grupe), uzrokovan većim brojem ugovora o eksternalizaciji s istim pružateljem usluga ili usko povezanim pružateljima usluga ili većim brojem ugovora o eksternalizaciji unutar istog poslovnog područja,
e) koncentracijski rizik na razini sektora, (npr. ako više banaka koristi istog pružatelja usluga ili malu grupu pružatelja usluga),
f) mjeru u kojoj banka koja zahtijeva eksternalizaciju kontrolira pružatelja usluga ili može utjecati na njegovo djelovanje, smanjenje rizika do kojeg može doći zbog veće razine kontrole, te je li pružatelj usluge uključen u konsolidirani nadzor bankarske grupe ili grupe društava,
g) sukobe interesa između banke i pružatelja usluga.

(4) Agencija zadržava pravo nalaganja specifičnih uvjeta, 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 s eksternalizacijom ili održati kontinuitet poslovanja, te ukoliko procijeni da bi eksternalizacija dovela do postojanja rizika prevelike izloženosti banke prema istom pružatelju usluga ili rizika izloženosti više banaka prema istom pružatelju usluga, što može imati potencijalni utjecaj na banku ili bankovni sustav u cjelini.

(5) U slučaju utvrđivanja koncentracijskog rizika, Agencije će pratiti kretanje tog rizika i ocijeniti njegov mogući utjecaj na druge banke, te na stabilnost financijskog tržišta.

Članak 31.
Izvješćivanje Agencije

(1) Banka je dužna Agenciji dostaviti sljedeća interna izvješća i akte:
a) politiku upravljanja eksternalizacijom definiranu člankom 12. ove odluke,
b) izvješća nadzornog odbora banke u vezi s upravljanjem rizicima eksternaliziranih aktivnosti u banci, u skladu s člankom 10. točka d) ove odluke,
c) godišnju procjenu rizika za eksternalizirane aktivnosti u banci, u skladu s člankom 26. st. (2) i (4) ove odluke,
d) izvješća unutarnje revizije o eksternaliziranim aktivnostima, u skladu s člankom 27. ove odluke.

(2) Banka je dužna izvješća i procjene iz točke b), c) i d) iz stavka (1) ovoga članka dostavljati Agenciji do 5. ožujka tekuće godine, za prethodnu godinu.

(3) Politike iz točke a) stavka (1) ovoga članka, banka je dužna dostaviti 7 (sedam) dana po usvajanju od strane nadzornog odbora banke.

Članak 32.
Prijelazne i završne odredbe

(1) Danom početka primjene ove odluke prestaje važiti Odluka o upravljanju eksternalizacijom u banci („Službene novine Federacije BiH“, broj 81/17).

(2) Banka je dužna uskladiti svoje poslovanje s odredbama ove odluke do 31.12.2022. godine.

(3) Iznimno od odredbi stavka (2) ovoga članka, banka je dužna dopuniti dokumentaciju o svim postojećim ugovorima o eksternalizaciji, kao i ugovorima s trećim stranama, te uskladiti postojeće ugovore s 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 stavkom (3) ovoga članka, dužna je o tome obavijestiti Agenciju, te o razlozima za navedeno, kao i o mjerama i rokovima planiranim za usklađivanje ili mogućoj izlaznoj strategiji.

Članak 33.
Stupanje na snagu

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

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

PREDSJEDNICA
UPRAVNOG ODBORA

Ivanka Galić, dipl. oec., v.r.