EBA/REC/2017/03

28/03/2018

Preporuke

za eksternalizaciju pružateljima usluga računarstva u oblaku

1. Obveze usklađenosti i izvještavanja

Status ovih preporuka

1. Ovaj dokument sadrži preporuke izdane u skladu s člankom 16. Uredbe (EU) br. 1093/2010[1]. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela i financijske institucije moraju ulagati napore da se usklade s preporukama.

2. Preporuke iznose EBA-ino stajalište o odgovarajućim nadzornim praksama unutar Europskog sustava financijskog nadzora ili o tome kako bi se pravo Unije trebalo primjenjivati u određenom području. Nadležna tijela određena člankom 4. stavkom 2. Uredbe (EU) br. 1093/2010 na koja se preporuke primjenjuju trebala bi se s njima uskladiti tako da ih na odgovarajući način uključe u svoje prakse (npr. izmjenama svojeg pravnog okvira ili nadzornih postupaka), uključujući i u slučajevima kada su preporuke prvenstveno upućene institucijama.

Zahtjevi za izvješćivanje

3. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela moraju obavijestiti EBA-u o tome jesu li usklađena ili se namjeravaju uskladiti s ovim preporukama, odnosno o razlozima neusklađenosti do 28/05/2018. U slučaju izostanka obavijesti unutar ovog roka EBA će smatrati da nadležna tijela nisu usklađena. Obavijesti se dostavljaju slanjem popunjenog obrasca koji se nalazi na internetskoj stranici EBA-e na adresu compliance@eba.europa.eu s uputom „EBA/REC/2017/03”. Obavijesti bi trebale slati osobe s odgovarajućom nadležnošću za izvješćivanje o usklađenosti u ime svojih nadležnih tijela. Svaka se promjena statusa usklađenosti također mora prijaviti EBA-i.

4. Obavijesti će biti objavljene na EBA-inoj internetskoj stranici u skladu s člankom 16. stavkom 3.

[1] Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ, (SL L 331, 15. 12. 2010., str. 12.).

2. Predmet, područje primjene i definicije

Predmet i područje primjene

1. U ovim se preporukama dodatno određuju uvjeti za eksternalizaciju u skladu sa smjernicama o eksternalizaciji Odbora europskih nadzornih tijela za bankarstvo (CEBS) od 14. prosinca 2006. te se one odnose na institucije definirane člankom 4. stavkom 1. točkom (3) Uredbe (EU) br. 575/2013 koje eksternaliziraju aktivnosti pružateljima usluga u oblaku.

Adresati

2. Ove su Smjernice upućene nadležnim tijelima koja su definirana u članku 4. stavku 2. točki (i) Uredbe (EU) br. 1093/2010 i institucijama koje su definirane u članku 4. stavku 1. točki (3) Uredbe (EU) br. 575/2013.[2]

Definicije

3. Osim ako je drukčije navedeno, pojmovi upotrijebljeni i utvrđeni u Direktivi 2013/36/EU[3] o kapitalnim zahtjevima te u smjernicama CEBS-a imaju isto značenje i u ovim preporukama. Osim toga, za potrebe ovih smjernica primjenjuju se sljedeće definicije:

Usluge računarstva u oblaku	Usluge koje se pružaju putem računarstva u oblaku, odnosno model kojim se na zahtjev omogućuje široko rasprostranjen, pogodan mrežni pristup zajedničkom skupu podesivih računalnih resursa (npr. mreže, poslužitelji, uređaji za pohranu podataka, aplikacije i usluge) koji se mogu trenutačno pribaviti i otpustiti uz minimalnu upravljačku aktivnost ili prisutnost pružatelja usluge.
Javni oblak	Infrastruktura za usluge računarstva u oblaku kojoj može pristupiti šira javnost.
Privatni oblak	Infrastruktura za usluge računarstva u oblaku kojoj može pristupiti samo jedna institucija.
Zajednički oblak	Infrastruktura za usluge računarstva u oblaku dostupna samo određenoj skupini institucija, uključujući nekoliko institucija iz jedne grupe.

[2] Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012.

[3] Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ.

Hibridni oblak	Infrastruktura za usluge u oblaku sastavljena od dviju ili više različitih infrastruktura za usluge u oblaku.

3. Provedba

Datum primjene

5. Ove se preporuke primjenjuju od 1. srpnja 2018.

4. Preporuke za eksternalizaciju pružateljima usluga računarstva u oblaku

4.1 Procjena materijalne značajnosti

1. Prije bilo kakve eksternalizacije svojih aktivnosti institucije procjenjuju koje bi se aktivnosti trebale smatrati materijalno značajnima. Institucije trebaju procijeniti značajnost aktivnosti sukladno smjernici 1. točki (f) smjernica CEBS-a te, posebno u pogledu eksternalizacije pružateljima usluga računarstva u oblaku, trebaju uzeti u obzir sve sljedeće činitelje:

   (a) kritičnost i profil inherentnih rizika za aktivnosti koje će se eksternalizirati, odnosno je li riječ o aktivnostima koje su ključne za kontinuitet/održivost institucije i njezinih obveza prema klijentima;

   (b) izravni učinak prekida rada na poslovanje te povezani pravni i reputacijski rizici;

   (c) učinak koji bilo kakav poremećaj aktivnosti može imati na buduće prihode institucije;

   (d) potencijalni učinak povrede povjerljivosti ili narušavanja integriteta podataka na instituciju i njezine klijente.

4.2 Dužnost primjerenog obavještavanja nadzornih tijela

2. Institucije trebaju primjereno obavijestiti nadležna tijela o materijalno značajnim aktivnostima koje će se eksternalizirati pružateljima usluga računarstva u oblaku. Institucije trebaju tako postupati u skladu sa stavkom 4.3 smjernica CEBS-a te u svakom slučaju nadležnim tijelima staviti na raspolaganje sljedeće informacije:

   (a) naziv pružatelja usluga računarstva u oblaku i naziv matičnog društva (ako postoji);
   (b) opis aktivnosti i podataka koji će se eksternalizirati;
   (c) zemlju ili zemlje u kojoj će usluga biti pružena (uključujući lokaciju podataka);
   (d) datum početka pružanja usluge;
   (e) posljednji datum obnove ugovora (ako je to primjenjivo);
   (f) mjerodavno pravo primjenjivo na ugovor;
   (g) datum završetka pružanja usluge ili sljedeći datum obnove ugovora (ako je to primjenjivo).

3. Nadalje, u skladu s informacijama navedenima u prethodnom stavku, nadležno tijelo može zatražiti od institucije dodatne informacije o njezinoj analizi rizika za materijalno značajne aktivnosti koje će se eksternalizirati, kao što su informacije o tome:

(a) ima li pružatelj usluga računarstva u oblaku plan kontinuiteta poslovanja koji je primjeren za usluge koje će biti pružene instituciji koja eksternalizira svoje aktivnosti;
(b) ima li institucija izlaznu strategiju u slučaju raskida ugovora od bilo koje strane ili prekida u pružanju usluga u oblaku;
(c) održava li institucija potrebne vještine i resurse za primjereno praćenje eksternaliziranih aktivnosti.

4. Institucija treba redovito ažurirati registar informacija o svim svojim materijalno značajnim aktivnostima i onima koje nisu materijalno značajne, a koje su eksternalizirane pružateljima usluga računarstva u oblaku na razini institucije i grupe. Institucija treba nadležnom tijelu, na zahtjev, dostaviti presliku ugovora o eksternalizaciji, kao i sve povezane informacije iz tog registra, neovisno o tome je li institucija aktivnost eksternaliziranu pružatelju usluga računarstva u oblaku procijenila materijalno značajnom ili ne.

5. U registru spomenutom u prethodnom stavku moraju biti sadržane barem sljedeće informacije:

(a) informacije iz stavka 2. točke od (a) do (g), ako nisu već prije dostavljene;
(b) vrsta eksternalizacije (model usluge u oblaku i model uporabe oblaka, odnosno javni / privatni / hibridni / zajednički oblak);
(c) strane koje koriste usluge u oblaku na temelju ugovora o eksternalizaciji;
(d) dokaz da su upravljačko tijelo ili njegovi delegirani odbori odobrili eksternalizaciju, ako je primjenjivo;
(e) imena podizvođača ako je primjenjivo;
(f) zemlja u kojoj je pružatelj usluga u oblaku / glavni podizvođač registriran;
(g) je li eksternalizacija procijenjena kao materijalno značajna (da/ne);
(h) datum posljednje procjene materijalne značajnosti eksternaliziranih aktivnosti;
(i) podržavaju li pružatelj(i) usluga računarstva u oblaku / podizvođač(i) poslovne aktivnosti koje su vremenski kritične (da/ne);
(j) procjena zamjenjivosti pružatelja usluga u oblaku (jednostavna, teška ili nije moguća);
(k) utvrđivanje alternativnog pružatelja usluge ako je to moguće;
(l) datum posljednje procjene rizika ugovora o eksternalizaciji ili ugovora s podizvođačem.

4.3 Pravo pristupa i pravo na reviziju

Za institucije

6. Temeljem smjernice 8. stavka 2. točke (g) smjernica CEBS-a te u svrhu eksternalizacije u oblaku, institucije koje eksternaliziraju svoje aktivnosti trebaju dodatno osigurati da su sklopile pisani ugovor s pružateljem usluga u oblaku na temelju kojeg se potonji obvezuje na sljedeće:

(a) da će pružati instituciji, bilo kojoj trećoj strani koju institucija odredi u tu svrhu i ovlaštenom revizoru institucije neograničen pristup svojim poslovnim prostorima (glavnim uredima i operativnim/podatkovnim centrima), uključujući pristup cijelom nizu uređaja, sustava, mreža i podataka koji se upotrebljavaju za pružanje eksternaliziranih usluga (pravo pristupa);

(b) da će dati instituciji, bilo kojoj trećoj strani koju je institucija odredila za tu svrhu i ovlaštenom revizoru institucije neograničeno pravo inspekcije i revizije u pogledu eksternaliziranih usluga (pravo na reviziju);

7. Ugovorne odredbe ne bi trebale ometati ili ograničavati učinkovito ostvarivanje prava pristupa i revizije. Ako provedba revizije ili upotreba revizijskih tehnika mogu stvoriti rizik za okruženje drugog klijenta, potrebno je pronaći alternativne načine kako bi se osigurala slična razina uvjerenja za instituciju.

8. Institucija treba ostvarivati svoje pravo pristupa i pravo na reviziju temeljem procjene rizika. Kada institucija nema na raspolaganju vlastite resurse za provedbu revizije, trebala bi razmotriti upotrebu barem jednog od sljedećih alata:

(a) Skupne revizije organizirane zajedno s drugim klijentima istog pružatelja usluga računarstva u oblaku tako da reviziju provode ti klijenti ili treća strana koju su oni ugovorili, kako bi se učinkovitije upotrijebili resursi za reviziju te kako bi se klijentima i pružatelju usluga računarstva u oblaku smanjilo organizacijsko opterećenje.

(b) Certifikati trećih strana i revizorska izvješća trećih strana ili izvješća unutarnje revizije koje je pružatelj usluga u oblaku učinio dostupnima pod uvjetom da:

i. institucija osigura da obuhvat certifikacije ili revizorskog izvješća uključuje sustave (tj. postupke, aplikacije, infrastrukturu, podatkovne centre itd.) i kontrole koje je ta institucija utvrdila kao ključne;
ii. institucija kontinuirano detaljno pregledava sadržaj certifikacija ili revizorskih izvješća i posebno osigurava da su ključne kontrole još uključene u buduće verzije revizorskog izvješća te provjerava da certifikat ili revizorsko izvješće nisu zastarjeli;
iii. institucija je zadovoljna osposobljenošću društva / osoba koje obavljaju reviziju ili certifikaciju (npr. u pogledu rotacije društva za reviziju ili certifikaciju, kvalifikacija, stručnosti, ponovnog izvođenja / provjere dokaza u temeljnom revizijskom dosjeu);
iv. certifikati se izdaju i revizije provode u skladu s općepriznatim standardima te uključuju testiranje operativne učinkovitosti postojećih ključnih kontrola;
v. institucija ima ugovorno pravo zatražiti proširenje obuhvata certifikacije ili revizorskih izvješća kako bi se uključili neki sustavi i/ili kontrole koji su relevantni. Broj i učestalost takvih zahtjeva za izmjenu obuhvata trebaju biti razumni i opravdani sa stajališta upravljanja rizicima.

9. S obzirom na to da su rješenja računarstva u oblaku tehnički vrlo složena, institucija koja eksternalizira svoje aktivnosti treba provjeriti imaju li zaposlenici koji provode reviziju – bilo da je riječ o njezinim unutarnjim revizorima ili skupini revizora koji djeluju u njezino ime ili imenovanim revizorima pružatelja usluga računarstva u oblaku – ili, kad je to prikladno, osoblje koje pregledava certifikaciju treće strane ili revizorska izvješća pružatelja usluga primjerene vještine i znanje kako bi proveli učinkovitu i relevantnu reviziju i/ili procjenu rješenja računarstva u oblaku.

Za nadležna tijela

10. Na temelju smjernice 8. stavka 2. točke (h) smjernica CEBS-a te za potrebe eksternalizacije, institucije trebaju osigurati da su sklopile pisani ugovor s pružateljem usluga računarstva u oblaku prema kojem se potonji obvezuje na sljedeće:

    (a) da će pružiti nadležnom tijelu koje nadzire instituciju (ili bilo kojoj trećoj strani koju je to tijelo odredilo u tu svrhu) neograničen pristup poslovnim prostorima pružatelja usluga u oblaku (glavnim uredima i operativnim centrima), uključujući pristup cijelom nizu uređaja, sustava, mreža i podataka koji se upotrebljavaju za pružanje usluga instituciji (pravo pristupa);

    (b) da će dati nadležnom tijelu koje nadzire instituciju (ili bilo kojoj trećoj strani koju je to tijelo odredilo u tu svrhu) neograničeno pravo inspekcije i revizije u pogledu eksternaliziranih usluga (pravo na reviziju).

11. Institucija treba osigurati da ugovorne odredbe ne sprječavaju njezino nadležno tijelo u izvršavanju svoje nadzorne funkcije i u ostvarenju svojih ciljeva.

12. Informacije koje nadležna tijela dobiju prilikom ostvarivanja prava pristupa i revizije trebaju podlijegati zahtjevima koji se odnose na čuvanje poslovne tajne i povjerljivost, navedenim u članku 53. *et seq.* Direktive 2013/36/EU (CRD IV). Nadležna tijela ne bi trebala sklapati nikakve ugovore ili davati izjave koje bi ih sprječavale u primjeni odredbi prava Unije o povjerljivosti, čuvanju poslovne tajne i razmjeni informacija.

13. Nadležno tijelo treba adresirati sve nedostatke na temelju nalaza iz svojeg nadzora, ako je potrebno, izravnim nalaganjem mjera instituciji koja eksternalizira svoje aktivnosti.

4.4 Posebno u pogledu prava pristupa

14. Ugovor iz stavaka 6. i 10. treba sadržavati sljedeće odredbe:

    (a) Strana koja namjerava ostvariti pravo pristupa (institucija, nadležno tijelo, revizor ili treća strana koja djeluje u ime institucije ili nadležnog tijela) treba prije planiranog izravnog posjeta lokaciji poslati obavijest u razumnom vremenskom roku prije tog izravnog posjeta relevantnom poslovnom prostoru, osim kada zbog hitnog slučaja ili krizne situacije nije moguće poslati prethodnu obavijest.

    (b) Pružatelj usluga računarstva u oblaku mora u potpunosti surađivati s odgovarajućim nadležnim tijelima, kao i s institucijom i njezinim revizorom, u vezi s izravnim posjetom.

4.5 Sigurnost podataka i sustava

15. Kao što se navodi u smjernici 8. stavku 2. točki (e) smjernica CEBS-a, ugovor o eksternalizaciji treba sadržavati odredbu prema kojoj pružatelj usluga eksternalizacije mora čuvati povjerljive informacije koje je dobio od financijske institucije. U skladu sa smjernicom 6. stavkom 6. točkom (e) smjernica CEBS-a, institucije trebaju provesti mjere kojima će osigurati kontinuitet usluga koje pružaju pružatelji usluga eksternalizacije. Na temelju smjernice 8. stavka 2. točke (b) i smjernice 9. smjernica CEBS-a, odgovarajuće potrebe institucija u pogledu kvalitete i performansi trebaju biti obuhvaćene ugovorima o eksternalizaciji i ugovorima o razini usluge. Ti se sigurnosni aspekti također trebaju kontinuirano pratiti (smjernica 7.).

16. Za potrebe prethodnog stavka, institucija bi trebala prije eksternalizacije te u svrhu donošenja relevantne odluke na temelju odgovarajućih informacija učiniti barem sljedeće:

    (a) utvrditi i klasificirati svoje aktivnosti, postupke i povezane podatke i sustave u pogledu osjetljivosti i potrebnih zaštitnih mjera;

    (b) provesti, uzimajući u obzir rizike, temeljit odabir aktivnosti, postupaka i povezanih podataka i sustava za koje se razmatra eksternalizacija pružatelju usluga računarstva u oblaku;

    (c) definirati i donijeti odluku o primjerenoj razini zaštite povjerljivosti podataka, kontinuitetu eksternaliziranih aktivnosti te integritetu i sljedivosti podataka i sustava u kontekstu planirane eksternalizacije u oblaku. Institucije bi također trebale razmotriti konkretne mjere gdje je to potrebno za podatke u prijenosu, podatke u memoriji i pohranjene podatke, kao što je upotreba tehnologija enkripcije, zajedno s odgovarajućom arhitekturom upravljanja ključevima.

17. U skladu s time, institucije bi trebale imati sklopljen pisani ugovor s pružateljem usluga računarstva u oblaku u kojem su, među ostalim, obveze potonjeg iz stavka 16. točke (c) jasno navedene.

18. Institucije bi trebale kontinuirano pratiti izvršavanje aktivnosti i sigurnosnih mjera u skladu sa smjernicom 7. CEBS-ovih smjernica, uključujući incidente, te preispitivati, ako je to prikladno, je li njihova eksternalizacija aktivnosti u skladu s prethodnim stavcima i odmah poduzeti sve potrebne korektivne mjere.

4.6 Lokacija i obrada podataka

19. Kao što je navedeno u smjernici 4. stavku 4. CEBS-ovih smjernica, institucije trebaju obraćati posebnu pažnju prilikom sklapanja ugovora o eksternalizaciji i upravljanju njima kad je riječ o području izvan Europskog gospodarskog prostora zbog mogućih rizika u pogledu zaštite podataka i učinkovitog nadzora od strane nadzornog tijela.

20. Institucija treba uvesti pristup temeljen na procjeni rizika za odlučivanje o lokaciji podataka i obrade podataka prilikom eksternalizacije u oblaku. Prilikom procjenjivanja trebaju se uzeti u obzir potencijalni učinci na rizike, uključujući pravne rizike i pitanja usklađenosti te ograničenja nadzora povezana sa zemljama u kojima se pružaju ili će se vjerojatno pružati eksternalizirane usluge, kao i gdje se ti podaci pohranjuju ili gdje će se vjerojatno pohranjivati. Pri procjenjivanju treba uzeti u obzir širu političku i sigurnosnu stabilnost predmetnih jurisdikcija; zakone na snazi u tim jurisdikcijama (uključujući zakone o zaštiti podataka); te odredbe o tijelima zaduženim za provođenja zakona na snazi u tim jurisdikcijama, uključujući odredbe stečajnog zakona koje bi se primjenjivale u slučaju propasti pružatelja usluga u oblaku. Institucija koja provodi eksternalizaciju treba osigurati da su ti rizici unutar prihvatljivih granica, s obzirom na značajnost eksternalizirane aktivnosti.

4.7 „Lančana" eksternalizacija

21. Kao što je navedeno u smjernici 10. CEBS-ovih smjernica, institucije trebaju uzimati u obzir rizike povezane s „lančanom" eksternalizacijom ako pružatelj usluge eksternalizacije sklapa ugovore s podizvođačima za elemente usluga. Institucija treba pristati na „lančanu" eksternalizaciju samo ako će se podizvođač također u potpunosti uskladiti s postojećim obvezama između institucije koja provodi eksternalizaciju i pružatelja usluga eksternalizacije. Nadalje, institucija treba poduzeti odgovarajuće mjere za adresiranje rizika od slabosti ili neizvršavanja podugovorenih aktivnosti koji ima značajan učinak na sposobnost pružatelja usluge eksternalizacije za ispunjavanje svojih obveza iz ugovora o eksternalizaciji.

22. Ugovor o eksternalizaciji sklopljen između institucije i pružatelja usluga računarstva u oblaku treba sadržavati sve vrste aktivnosti koje su izuzete iz potencijalnog podizvođenja i u njemu treba biti navedeno da pružatelj usluga računarstva u oblaku zadržava potpunu odgovornost za usluge za koje je sklopio ugovor s podizvođačem kao i za nadzor nad tim uslugama.

23. Ugovor o eksternalizaciji također treba sadržavati odredbu o obvezi pružatelja usluga računarstva u oblaku u pogledu obavještavanja institucije o svim planiranim značajnim promjenama u pogledu podizvođača ili usluga za koje je sklopljen ugovor o podizvođenju, navedenih u originalnom ugovoru, koje bi mogle utjecati na sposobnost pružatelja usluge da ispuni svoje obveze sukladno ugovoru o eksternalizaciji. Potrebno je prethodno ugovorno odrediti rok za slanje obavijesti o takvim promjenama kako bi institucija mogla procijeniti rizike od utjecaja koje će predložene promjene imati prije nego što promjene podizvođača ili podugovorenih usluga zaista stupe na snagu.

24. U slučaju da pružatelj usluga računarstva u oblaku planira promjene u pogledu podizvođača ili usluga za koje sklapa ugovor o podizvođenju, a koje bi imale štetan utjecaj na procjenu rizika za ugovorene usluge, institucija treba imati pravo raskinuti ugovor.

25. Institucija treba kontinuirano preispitivati i pratiti uspješnost sveukupno pruženih usluga, bez obzira na to pruža li ih pružatelj usluga računarstva u oblaku ili njegovi podizvođači.

4.8 Planovi za nepredviđene događaje i izlazne strategije

26. Sukladno smjernici 6.1 stavku 6. točki (6) i smjernici 8. stavku 2. točki (d) CEBS-ovih smjernica, institucija koja eksternalizira svoje aktivnosti treba planirati i provesti mjere za održavanje kontinuiteta poslovanja u slučaju nepružanja usluga pružatelja usluga eksternalizacije ili pada kvalitete pruženih usluga do neprihvatljive razine. Takve mjere trebaju uključivati planove za nepredviđene događaje i jasno definiranu izlaznu strategiju. Nadalje, ugovor o eksternalizaciji treba sadržavati klauzulu o raskidu i upravljanju izlaznom strategijom kojom se omogućuje prijenos aktivnosti koje obavlja pružatelj usluga eksternalizacije na drugog pružatelja usluga eksternalizacije ili vraćanje obavljanja tih aktivnosti u instituciju.

27. Institucija također mora prema potrebi osigurati provedivost svoje izlazne strategije u pogledu ugovora o eksternalizaciji i to bez nepotrebnog prekida u pružanju svojih usluga ili negativnog učinka na usklađenost s regulatornim odredbama te bez štetnih posljedica za kontinuitet i kvalitetu vlastitog pružanja usluga klijentima. Kako bi to ostvarila, institucija treba:

    (a) izraditi i provesti izlazne planove koji su sveobuhvatni, dokumentirani i dovoljno testirani ako je to potrebno;

    (b) utvrditi alternativna rješenja i razviti prijelazne planove kako bi mogla ukloniti i prenijeti, na kontroliran i dobro testiran način, postojeće aktivnosti i podatke s pružatelja usluga računarstva u oblaku na svoja rješenja, uzimajući u obzir pitanja lokacije podataka i održavanja kontinuiteta poslovanja tijekom prijelazne faze;

    (c) osigurati da je u ugovoru o eksternalizaciji određena obveza pružatelja usluga računarstva u oblaku da dostatno podrži instituciju u urednom prijenosu aktivnosti na drugog pružatelja usluge ili u izravnom upravljanju same institucije u slučaju raskida ugovora o eksternalizaciji.

28. Pri izradi izlaznih strategija, institucija treba razmotriti sljedeće:

    (a) razvijanje ključnih pokazatelja rizika kako bi se utvrdila neprihvatljiva razina usluge;

    (b) provođenje analize utjecaja na poslovanje, proporcionalno eksternaliziranim aktivnostima kako bi se utvrdili ljudski i materijalni resursi koji su potrebni za provedbu izlaznog plana te koliko će vremena za to biti potrebno;

(c) dodjelu uloga i odgovornosti za upravljanje izlaznim planovima i prijelaznim aktivnostima;

(d) definiranje kriterija uspjeha prijelazne faze.

29. U svoje kontinuirano praćenje i nadzor usluga koje pruža pružatelj usluga računarstva u oblaku institucija treba uključiti pokazatelje koji mogu aktivirati izlazni plan.