

EBA/REC/2017/03

28/03/2018

Priporočila

o oddajanju v zunanje izvajanje ponudnikom storitev v oblaku

1. Obveznosti v zvezi s skladnostjo in poročanjem

Vloga teh priporočil

1. Dokument vsebuje smernice, izdane v skladu s členom 16 Uredbe (EU) št. 1093/2010¹. V skladu s členom 16(3) Uredbe (EU) št. 1093/2010 si morajo pristojni organi in finančne institucije na vsak način prizadevati za upoštevanje priporočil.
2. V priporočilih je predstavljeno stališče organa EBA o ustreznih nadzorniških praksah v Evropskem sistemu finančnega nadzora in o tem, kako bi bilo treba zakonodajo Unije uporabljati na določenem področju. Pristojni organi iz člena 4(2) Uredbe (EU) št. 1093/2010, za katere priporočila veljajo, bi jih morali upoštevati tako, da jih ustrezno vključijo v svoje prakse (npr. s spremembo svojega pravnega okvira ali nadzorniških postopkov), tudi če so priporočila namenjena predvsem institucijam.

Dolžnost poročanja

3. Pristojni organi morajo v skladu s členom 16(3) Uredbe (EU) št. 1093/2010 do 28.05.2018 organ EBA uradno obvestiti, ali ravnajo oziroma ali nameravajo ravnati v skladu s temi priporočili, ali pa mu sporočiti razloge za njihovo neupoštevanje. Če pristojni organi do tega roka ne bodo poslali uradnega obvestila, bo organ EBA štel, da ne upoštevajo smernic. Uradna obvestila je treba poslati na obrazcu, ki je na voljo v spletišču organa EBA, na elektronski naslov compliance@eba.europa.eu z navedbo sklica „EBA/REC/2017/03“. Predložiti jih morajo osebe, ki so ustrezno pooblaščen za poročanje o skladnosti v imenu svojih pristojnih organov. Organu EBA je treba sporočiti tudi vsako spremembo stanja glede upoštevanja smernic.
4. Uradna obvestila bodo v skladu s členom 16(3) objavljena v spletišču organa EBA.

¹ Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12).

2. Predmet urejanja, področje uporabe in opredelitev pojmov

Predmet urejanja in področje uporabe

1. S temi priporočili se podrobneje določajo pogoji za zunanje izvajanje, navedeni v smernicah odbora CEBS o zunanjem izvajanju z dne 14. decembra 2006. Priporočila veljajo za zunanje izvajanje dejavnosti, ki jih institucije, kakor so opredeljene v točki (3) člena 4(1) Uredbe (EU) št. 575/2013, oddajajo ponudnikom storitev v oblaku.

Naslovniki

2. Ta priporočila so naslovljena na pristojne organe, kakor so opredeljeni v točki (i) člena 4(2) Uredbe (EU) št. 1093/2010, in institucije, kakor so opredeljene v točki (3) člena 4(1) Uredbe (EU) št. 575/2013².

Opredelitev pojmov

3. Če ni določeno drugače, imajo izrazi v teh priporočilih enak pomen kot izrazi, uporabljeni in opredeljeni v Direktivi 2013/36/EU³ o kapitalskih zahtevah ter smernicah odbora CEBS. Poleg tega se za namene teh priporočil uporabljajo naslednje opredelitve pojmov:

Storitve v oblaku	Storitve, ponujene prek računalništva v oblaku, tj. modela za zagotavljanje vseprisotnega priročnega omrežnega dostopa na zahtevo do deljenega nabora računalniških virov (kamor sodijo omrežja, strežniki, diskovni prostor, aplikacije in storitve), ki jih je mogoče konfigurirati ter hitro pripraviti za uporabo in hitro sprostiti, oboje z minimalnim trudom in z minimalno interakcijo ponudnika storitev.
Javni oblak	Infrastruktura v oblaku, ki jo lahko prosto uporablja splošna javnost.
Zasebni oblak	Infrastruktura v oblaku, ki jo lahko uporablja izključno ena sama institucija.
Skupnostni oblak	Infrastruktura v oblaku, ki jo lahko uporablja izključno določena skupnost institucij, vključno z več institucijami v okviru ene skupine.

² Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe (EU) št. 648/2012.

³ Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES.

Hibridni oblak	Infrastruktura v oblaku, ki je sestavljena iz dveh ali več ločenih infrastruktur v oblaku.
----------------	--

3. Izvajanje

Datum začetka uporabe

5. Ta priporočila se začnejo uporabljati 1. julija 2018.

4. Priporočila o oddajanju v zunanje izvajanje ponudnikom storitev v oblaku

4.1 Ocenjevanje pomembnosti

1. Institucije, ki oddajajo dejavnosti v zunanje izvajanje, bi morale pred oddajo oceniti, katere dejavnosti bi morale šteti kot bistvene (pomembne). Institucije bi morale pomembnost dejavnosti oceniti na podlagi smernice odbora CEBS št. 1(f) in v zvezi z oddajanjem v zunanje izvajanje ponudnikom storitev v oblaku upoštevati vse naslednje:
 - (a) kritičnost in profil tveganja pri delovanju dejavnosti, ki bodo oddane v zunanje izvajanje, tj. ali so dejavnosti kritične za neprekinjeno poslovanje/sposobnost preživetja institucije ter njene obveznosti do strank;
 - (b) neposredni operativni vpliv morebitnih izpadov ter povezana pravna tveganja in tveganja izgube poslovnega ugleda;
 - (c) vpliv, ki bi ga morebitna prekinitve dejavnosti lahko imela na predvidene prihodke institucije;
 - (d) možen vpliv, ki bi ga morebitna kršitev zaupnosti ali kršitev celovitosti podatkov lahko imelo na institucijo in njene stranke.

4.2 Dolžnost ustreznega obveščanja nadzornikov

2. Institucije, ki oddajajo dejavnosti v zunanje izvajanje, bi morale ustrezno obveščati pristojne organe o bistvenih dejavnostih, ki jih bodo oddale ponudnikom storitev v oblaku. Institucije bi morale to opraviti na podlagi odstavka 4.3 smernic odbora CEBS in v vsakem primeru pristojnim organom zagotoviti naslednje informacije:
 - (a) ime ponudnika storitev v oblaku in (morebitnega) nadrejenega podjetja;
 - (b) opis dejavnosti in podatkov, ki bodo oddani v zunanje izvajanje;
 - (c) državo oz. države, kjer bo storitev izvedena (vključno z lokacijo podatkov);
 - (d) datum začetka storitve;
 - (e) datum zadnje obnovitve pogodbe, če je bila pogodba obnovljena;
 - (f) pravo, ki se uporablja za pogodbo;
 - (g) datum izteka pogodbe ali naslednje obnovitve pogodbe (kjer je primerno).
3. Pristojni organ lahko od institucije, ki oddaja dejavnosti v zunanje izvajanje, poleg informacij, zagotovljenih v skladu s prejšnjim odstavkom, zahteva dodatne informacije o njeni analizi tveganja za bistvene dejavnosti, ki bodo oddane v zunanje izvajanje, na primer:

- (a) ali ima ponudnik storitev v oblaku načrt neprekinjenega poslovanja, ki ustreza storitvam, ki jih ponuja instituciji, ki oddaja dejavnosti v zunanje izvajanje;
 - (b) ali ima institucija, ki oddaja dejavnosti v zunanje izvajanje, strategijo izstopa za primer, če katera izmed strank prekine pogodbo ali če pri ponudniku storitev v oblaku pride do motenj v zagotavljanju storitev;
 - (c) ali ima institucija, ki oddaja dejavnosti v zunanje izvajanje, veščine in vire, ki so potrebni za ustrezno spremljanje dejavnosti, oddanih v zunanje izvajanje.
4. Institucija, ki oddaja dejavnosti v zunanje izvajanje, bi morala voditi posodobljen register informacij o vseh svojih bistvenih in nebistvenih dejavnostih, ki jih oddajajo v zunanje izvajanje ponudnikom storitev v oblaku, in sicer na ravni institucije ter na ravni skupine. Institucija, ki oddaja dejavnosti v zunanje izvajanje, bi morala pristojnemu organu na zahtevo predložiti kopijo pogodbe o zunanjem izvajanju in povezane informacije iz omenjenega registra, ne glede na to, ali je dejavnost, oddano v zunanje izvajanje ponudniku storitev v oblaku, ocenila kot bistveno ali ne.
5. Register iz prejšnjega odstavka bi moral vključevati vsaj naslednje informacije:
- (a) informacije iz odstavka 2(a)–(g), če niso bile že predložene pristojnemu organu;
 - (b) vrsto zunanjega izvajanja (model storitve v oblaku in model postavitve oblaka, tj. javni/zasebni/hibridni/skupnostni oblak);
 - (c) stranke, za katere se v skladu s pogodbo o zunanjem izvajanju izvajajo storitve v oblaku;
 - (d) po potrebi dokaz, da je zunanje izvajanje odobril upravljalni organ ali njegovi delegirani odbori;
 - (e) imena morebitnih podizvajalcev;
 - (f) državo, v kateri je registriran ponudnik storitev v oblaku/glavni podizvajalec;
 - (g) ali je bilo zunanje izvajanje ocenjeno kot bistveno (da/ne);
 - (h) datum zadnje ocene pomembnosti dejavnosti, oddanih v zunanje izvajanje, ki jo je izvedla institucija;
 - (i) ali ponudnik storitev v oblaku ali podizvajalec oz. podizvajalci podpirajo poslovne operacije, ki so časovno kritične (da/ne);
 - (j) oceno nadomestljivosti ponudnika storitev v oblaku (lahko nadomestljiv/težko nadomestljiv/nadomestitev ni mogoča);
 - (k) določitev nadomestnega ponudnika storitev, če je mogoča;
 - (l) datum zadnje ocene tveganja pri pogodbi o zunanjem izvajanju ali pogodbi s podizvajalcem.

4.3 Pravici do dostopa in revizije

Za institucije

6. Na podlagi smernice odbora CEBS št. 8(2)(g) bi morale institucije, ki oddajajo dejavnosti v zunanje izvajanje v oblaku, nadalje zagotoviti, da imajo s ponudnikom storitev v oblaku sklenjeno pisno pogodbo, v skladu s katero se ponudnik obveže:

- (a) da instituciji, morebitni tretji osebi, ki jo za ta namen imenuje institucija, in zakonitemu revizorju institucije zagotovi poln dostop do svojih poslovnih prostorov (sedeža podjetja ter operativnih centrov), vključno z vsemi napravami, sistemi, omrežji in podatki, uporabljenimi pri zagotavljanju storitev, oddanih v zunanje izvajanje (pravica do dostopa);
 - (b) da instituciji, morebitni tretji osebi, ki jo za ta namen imenuje institucija, in zakonitemu revizorju institucije podeli neomejene pravice do pregledovanja in revizije v zvezi z storitvami, oddanimi v zunanje izvajanje (pravica do revizije).
7. Učinkovito uveljavljanje pravic do dostopa in revizije ne bi smelo biti ovirano ali omejeno s pogodbenimi dogovori. Če bi izvajanje revizij ali uporaba nekaterih revizijskih tehnik lahko pomenila tveganje za okolje druge stranke, je potreben dogovor glede drugih načinov doseganja podobne stopnje zagotovil, kot jih zahteva institucija.
8. Institucija, ki oddaja dejavnosti v zunanje izvajanje, bi morala svoji pravici do revizije in dostopa uveljavljati na podlagi ocene tveganja. Kadar institucija nima lastnih revizijskih virov, bi morala razmisliti o uporabi vsaj enega izmed naslednjih orodij:
- (a) Skupnih revizij, organiziranih skupaj z drugimi strankami istega ponudnika storitev v oblaku, ki jih izvedejo te stranke ali tretja oseba, ki jo te stranke imenujejo. S tem bi bili revizijski viri učinkoviteje uporabljeni in bi se zmanjšalo organizacijsko breme tako za stranke kot za ponudnika storitev v oblaku.
 - (b) Certifikate tretjih oseb in revizijska poročila tretjih oseb ali notranja revizijska poročila, ki jih zagotovi ponudnik storitev v oblaku, pod naslednjimi pogoji:
 - i. Institucija, ki oddaja dejavnosti v zunanje izvajanje, zagotovi, da področje certifikata oz. revizijskega poročila zajema sisteme (tj. procese, aplikacije, infrastrukturo, podatkovne centre itd.) in kontrole, ki jih institucija določi kot ključne.
 - ii. Institucija, ki oddaja dejavnosti v zunanje izvajanje, redno temeljito ocenjuje vsebino certifikatov oz. revizijskih poročil in zlasti zagotovi, da bodo ključne kontrole še zajete v prihodnjih različicah revizijskega poročila, ter preveri, da certifikat oz. revizijsko poročilo ni zastarelo.
 - iii. Institucija, ki oddaja dejavnosti v zunanje izvajanje, je zadovoljna z usposobljenostjo osebe, ki izvaja certificiranje oz. revizijo (npr. glede rotacije podjetja, ki izvaja certificiranje oz. revizijo, kvalifikacij, strokovnega znanja, ponovnega izvajanja/preverjanja dokazov v zadevnem revizijskem dosjeju).
 - iv. Certifikati in revizije se izdajajo oz. izvajajo na podlagi splošno priznanih standardov ter vključujejo preizkus operativne učinkovitosti vzpostavljenih ključnih kontrol.
 - v. Institucija, ki oddaja dejavnosti v zunanje izvajanje, ima pogodbeno pravico, da zahteva razširitev področja certifikatov oz. revizijskih poročil na nekatere sisteme in/ali kontrole, ki so relevantni. Število in pogostost takih zahtev za

spremembo področja bi morala biti razumna ter upravičena z vidika upravljanja tveganj.

9. Glede na to, da so rešitve v oblaku tehnično precej zapletene, bi morala institucija, ki oddaja dejavnosti v zunanje izvajanje, preveriti, da ima osebje, ki izvaja revizijo – notranji revizorji, skupina revizorjev, ki deluje v njenem imenu, ali revizorji, ki jih je imenoval ponudnik storitev v oblaku – ali po potrebi osebje, ki pregleduje certifikate tretjih oseb ali revizijska poročila ponudnika storitev, ustrezne veščine in znanje, da izvaja učinkovite ter relevantne revizije in/ali ocene rešitev v oblaku.

Za pristojne organe

10. Na podlagi smernice odbora CEBS št. 8(2)(h) bi morale institucije, ki oddajajo dejavnosti v zunanje izvajanje v oblaku, zagotoviti, da imajo s ponudnikom storitev v oblaku sklenjeno pisno pogodbo, v skladu s katero se ponudnik obveže:

- (a) da pristojnemu organu, ki nadzoruje institucijo, ki oddaja dejavnosti v zunanje izvajanje (ali morebitni tretji osebi, ki jo za ta namen imenuje ta organ), zagotovi poln dostop do svojih poslovnih prostorov (sedeža podjetja ter operativnih centrov), vključno z vsemi napravami, sistemi, omrežji in podatki, uporabljenimi pri zagotavljanju storitev, oddanih in zunanje izvajanje (pravica do dostopa);
- (b) da pristojnemu organu, ki nadzoruje institucijo, ki oddaja dejavnosti v zunanje izvajanje (ali morebitni tretji osebi, ki jo za ta namen imenuje ta organ), podeli neomejene pravice do pregledovanja in revizije v zvezi z storitvami, oddanimi v zunanje izvajanje (pravica do revizije).

11. Institucija, ki oddaja dejavnosti v zunanje izvajanje, bi morala zagotoviti, da s pogodbenimi dogovori ne ovira svojega pristojnega organa pri izvajanju njegove nadzorniške funkcije in ciljev.

12. Za informacije, ki jih pristojni organi pridobijo pri uveljavljanju pravic do dostopa in revizije, bi morale veljati zahteve glede poklicne skrivnosti ter zaupnosti iz člena 53 in naslednjih členov Direktive 2013/36/EU (CRD IV). Pristojni organi bi se morali vzdržati kakršnih koli pogodbenih dogovorov ali izjav, zaradi katerih ne bi mogli upoštevati določb prava Unije o zaupnosti, poklicni skrivnosti in izmenjavi informacij.

13. Pristojni organ bi moral na podlagi ugotovitev svoje revizije obravnavati vse prepoznane pomanjkljivosti, po potrebi tako, da instituciji, ki oddaja dejavnosti v zunanje izvajanje, neposredno naloži ustrezne ukrepe.

4.4 Pravica do dostopa

14. Pogodba iz odstavkov 6 do 10 bi morala vsebovati naslednje določbe:

- (a) Stranka, ki namerava uveljaviti svojo pravico do dostopa (institucija, pristojni organ, revizor ali tretja stranka, ki deluje v imenu institucije ali pristojnega

organa), bi morala v razumnem roku pred načrtovanim obiskom na kraju samem ponudnika storitev v oblaku obvestiti o obisku zadevnega poslovnega prostora, razen če zgodnje vnaprejšnje obvestilo zaradi izrednih ali kriznih razmer ni možno.

- (b) Ponudnik storitev v oblaku mora v zvezi z obiskom na kraju samem v celoti sodelovati z ustreznimi pristojnimi organi ter z institucijo in njenim revizorjem.

4.5 Varnost podatkov in sistemov

15. Kot je navedeno v smernici odbora CEBS št. 8(2)(e), bi morala pogodba o zunanjem izvajanju ponudnika storitev zunanjega izvajanja obvezovati, da varuje zaupnost informacij, ki mu jih posreduje finančna institucija. V skladu s smernico odbora CEBS št. 6(6)(e) bi morale institucije vzpostaviti ureditve, s katerimi zagotovijo neprekinjenost storitev, ki jih zagotavljajo ponudniki storitev zunanjega izvajanja. Na podlagi smernice odbora CEBS št. 8(2)(b) in smernice št. 9 bi morale biti ustrezne potrebe institucije, ki oddaja dejavnosti v zunanje izvajanje, glede kakovosti in uspešnosti upoštevane v pisnih pogodbah o zunanjem izvajanju in sporazumih o ravni storitve. Tudi ti varnostni vidiki bi se morali redno spremljati (smernica št. 7).

16. Za namene prejšnjega odstavka bi morala institucija pred oddajo dejavnosti v zunanje izvajanje in za namen obveščanja o zadevni odločitvi opraviti vsaj naslednje:

- (a) prepoznati in razvrstiti svoje dejavnosti, procese ter povezane podatke in sisteme glede na občutljivost ter potrebno zaščito;
- (b) na podlagi tveganja skrbno izbere dejavnosti, procese ter povezane podatke in sisteme, za katere se razmišlja, da bi bili oddani v zunanje izvajanje z rešitvijo računalništva v oblaku;
- (c) opredeliti in določiti ustrezno stopnjo varovanja zaupnosti podatkov, neprekinjenosti dejavnosti, oddanih v zunanje izvajanje, in celovitosti ter sledljivosti podatkov in sistemov v okviru načrtovanega zunanjega izvajanja v oblaku; institucije bi morale po potrebi razmisliti tudi o določenih ukrepih za podatke med prenašanjem, podatke v pomnilniku in podatke med shranjevanjem, kot je uporaba tehnologij šifriranja v kombinaciji z ustrezno arhitekturo za upravljanje ključev.

17. Posledično bi morale institucije zagotoviti, da imajo s ponudnikom storitev v oblaku sklenjeno pisno pogodbo, v kateri so med drugim določene obveznosti slednjega v skladu z odstavkom 16(c).

18. Institucije bi morale redno spremljati izvajanje dejavnosti in varnostnih ukrepov v skladu s smernico odbora CEBS št. 7, vključno z incidenti, ter ustrezno pregledovati, ali je zunanje izvajanje dejavnosti v skladu s prejšnjimi odstavki, in nemudoma sprejeti morebitne potrebne popravne ukrepe.

4.6 Lokacija podatkov in obdelava podatkov

19. Kot je navedeno v smernici odbora CEBS št. 4(4), bi morale biti institucije posebno previdne pri sklepanju in upravljanju pogodb o zunanjem izvajanju s ponudniki zunaj EGS zaradi možnih tveganj glede varstva podatkov in učinkovitega nadzora s strani nadzornega organa.
20. Institucija, ki oddaja dejavnosti v zunanje izvajanje v oblaku, bi morala za odločanje o lokaciji podatkov in obdelave podatkov sprejeti pristop na podlagi ocene tveganj. Pri ocenjevanju bi morala upoštevati možne vplive tveganj, vključno s pravnimi tveganji in težavami v zvezi s skladnostjo, ter omejitve pri nadzoru, povezane z državami, kjer se bodo ali se verjetno bodo izvajale storitve, oddane v zunanje izvajanje, in kjer se bodo ali se verjetno bodo hranili podatki. Pri ocenjevanju bi morala upoštevati tudi širšo politično in varnostno stabilnost zadevnih jurisdikcij, veljavno zakonodajo v teh jurisdikcijah (vključno z zakonodajo na področju varstva podatkov) ter veljavne določbe glede izvrševanja zakonodaje v teh jurisdikcijah, vključno z določbami insolvenčnega prava, ki bi se uporabljale v primeru, če bi ponudnik storitev v oblaku propadel. Institucija, ki oddaja dejavnost v zunanje izvajanje, bi morala zagotoviti, da je stopnja teh tveganj ves čas na sprejemljivi ravni, ki je sorazmerna s pomembnostjo dejavnosti, oddane v zunanje izvajanje.

4.7 Verižno oddajanje v zunanje izvajanje

21. Kot je navedeno v smernici odbora CEBS št. 10, bi morale institucije upoštevati tveganja v zvezi z „verižnim“ oddajanjem v zunanje izvajanje, pri katerem ponudnik storitev zunanjega izvajanja dele storitve odda drugim ponudnikom kot podizvajalcem. Institucija, ki oddaja dejavnosti v zunanje izvajanje, ne bi smela privoliti v verižno oddajanje v zunanje izvajanje, razen če bo podizvajalec v celoti izpolnjeval obveznosti, ki jih ima ponudnik storitev zunanjega izvajanja do institucije. Poleg tega bi morala v tem primeru institucija, ki oddaja dejavnosti v zunanje izvajanje, sprejeti ustrezne ukrepe za odpravo tveganja, da pri izvajanju dejavnosti, oddanih podizvajalcu, pride do kakršnih koli pomanjkljivosti ali pa se te sploh ne izvedejo, če bi to znatno vplivalo na zmožnost ponudnika storitev zunanjega izvajanja, da izpolni svoje obveznosti iz pogodbe o zunanjem izvajanju.
22. V pogodbi o zunanjem izvajanju med institucijo, ki oddaja dejavnosti v zunanje izvajanje, in ponudnikom storitev v oblaku bi morale biti določene morebitne vrste dejavnosti, ki so izključene iz možnosti oddajanja podizvajalcem. Navedeno bi moralo biti tudi, da ponudnik storitev v oblaku ohranja polno odgovornost za storitve, ki jih odda podizvajalcem, in izvaja nadzor nad njimi.
23. Pogodba o zunanjem izvajanju bi morala vključevati tudi obveznost ponudnika storitev v oblaku, da institucijo, ki oddaja dejavnosti v zunanje izvajanje, obvesti o morebitnih pomembnih načrtovanih spremembah glede podizvajalcev ali storitev, oddanih podizvajalcem, navedenih v prvotni pogodbi, če bi te spremembe lahko vplivale na zmožnost ponudnika storitev zunanjega izvajanja, da izpolni svoje obveznosti iz pogodbe o zunanjem izvajanju. V pogodbi bi se morali stranki vnaprej dogovoriti o roku za obveščanje o teh spremembah, da bi lahko institucija, ki

oddaja dejavnosti v zunanje izvajanje, ocenila tveganja učinkov predlaganih sprememb, preden se sprememba glede podizvajalcev ali storitev, oddanih podizvajalcem, dejansko zgodi.

24.V primeru, da ponudnik storitev v oblaku načrtuje spremembe glede podizvajalcev ali storitev, oddanih podizvajalcem, ki bi negativno vplivale na oceno tveganja dogovorjenih storitev, bi morala imeti institucija, ki oddaja dejavnosti v zunanje izvajanje, pravico, da prekine pogodbo.

25.Institucija, ki oddaja dejavnosti v zunanje izvajanje, bi morala redno pregledovati in spremljati uspešnost storitve kot celote, ne glede na to, ali jo zagotavlja ponudnik storitev v oblaku ali njegovi podizvajalci.

4.8 Krizni načrti in strategije izstopa

26.Kot je navedeno v smernici odbora CEBS št. 6.1, smernici št. 6(6)(e) in smernici št. 8(2)(d), bi morala institucija, ki oddaja dejavnosti v zunanje izvajanje, načrtovati ter vzpostaviti ureditve za neprekinjeno poslovanje v primeru, da ponudnik storitev zunanjega izvajanja preneha z zagotavljanjem storitev ali pa kakovost storitev pade na nesprejemljivo raven. Te ureditve bi morale vključevati krizne načrte in jasno opredeljeno strategijo izstopa. Poleg tega bi morala pogodba o zunanjem izvajanju vključevati klavzulo o prekinitvi in upravljanju izstopa, ki omogoča, da se dejavnosti, ki jih izvaja ponudnik storitev zunanjega izvajanja, prenesejo na drugega ponudnika storitev zunanjega izvajanja ali pa jih ponovno prevzame institucija.

27.Institucija, ki oddaja dejavnosti v zunanje izvajanje, bi morala tudi zagotoviti, da ima, če se izkaže za potrebno, možnost izstopiti iz ureditev zunanjega izvajanja v oblaku tako, da ne pride do prevelikih motenj v njenem zagotavljanju storitev ali negativnih učinkov na njeno skladnost z regulativnim režimom ter da nista ogroženi neprekinjenost in kakovost zagotavljanja storitev strankam. Institucija, ki oddaja dejavnosti v zunanje izvajanje, bi morala za doseg tega:

- (a) oblikovati in vzpostaviti načrte izstopa, ki so celoviti, dokumentirani in, kjer je primerno, ustrezno preizkušeni;
- (b) določiti nadomestne rešitve in oblikovati načrte prehoda, s katerimi bi odstranila obstoječe dejavnosti in podatke od ponudnika storitev v oblaku ter jih prenesla na te rešitve na nadzorovan in ustrezno preizkušen način, pri čemer upošteva vprašanje lokacije podatkov ter zagotavljanje neprekinjenosti poslovanja v prehodnem obdobju;
- (c) zagotoviti, da pogodba o zunanjem izvajanju vključuje obveznost ponudnika storitev v oblaku, da v primeru prekinitve pogodbe o zunanjem izvajanju ustrezno podpira institucijo pri urejenem prenosu dejavnosti na drugega ponudnika storitev ali pri njenem neposrednem upravljanju.

28.Pri oblikovanju strategije izstopa bi morala institucija, ki oddaja dejavnosti v zunanje izvajanje:

- (a) oblikovati ključne kazalnike tveganj, s katerimi bi prepoznala nesprejemljivo raven storitve;

- (b) opraviti analizo vpliva na poslovanje, sorazmerno z dejavnostmi, oddanimi v zunanje izvajanje, s katero bi ugotovila, kakšne človeške in materialne vire ter koliko časa bi potrebovala za izvedbo načrta izstopa;
- (c) opredeliti vloge in odgovornosti za upravljanje načrtov izstopa in dejavnosti prehoda;
- (d) opredeliti merila uspešnosti prehoda.

29. Institucija, ki oddaja dejavnosti v zunanje izvajanje, bi morala kazalnike, ki lahko sprožijo izvedbo načrta izstopa, vključiti v svoje redno spremljanje in nadzor storitev, ki jih zagotavlja ponudnik storitev v oblaku.