EBA/REC/2017/03

28/03/2018

Odporúčania

týkajúce sa outsourcingu poskytovateľom cloudových služieb

1. Dodržiavanie predpisov a povinnosť podávať správy

Status týchto odporúčaní

1. Tento dokument obsahuje odporúčania vydané podľa článku 16 nariadenia (EÚ) č. 1093/2010[1]. V súlade s článkom 16 ods. 3 nariadenia (EÚ) č. 1093/2010 príslušné orgány a finančné inštitúcie musia vynaložiť všetko úsilie na dodržanie týchto odporúčaní.

2. Tieto odporúčania predstavujú názor orgánu EBA na príslušné postupy dohľadu v rámci európskeho systému finančného dohľadu alebo na spôsob uplatňovania právnych predpisov Únie v konkrétnej oblasti. Príslušné orgány, ako sú vymedzené v článku 4 ods. 2 nariadenia (EÚ) č. 1093/2010, na ktoré sa tieto odporúčania vzťahujú, ich majú dodržiavať tak, že ich začlenia do svojich postupov dohľadu podľa potreby (napr. zmenou svojho právneho rámca alebo postupov dohľadu), a to aj v prípade, keď sú tieto odporúčania zamerané prevažne na inštitúcie.

Požiadavky na vykazovanie

3. Podľa článku 16 ods. 3 nariadenia (EÚ) č. 1093/2010 musia príslušné orgány oznámiť orgánu EBA, či tieto odporúčania dodržiavajú alebo majú v úmysle dodržať, alebo musia uviesť dôvody ich nedodržania do 28.05.2018. Ak do tohto dátumu nebude doručené žiadne oznámenie, orgán EBA sa bude domnievať, že ich príslušné orgány nedodržiavajú. Oznámenia sa majú zaslať prostredníctvom formulára dostupného na webovom sídle orgánu EBA na adresu compliance@eba.europa.eu spolu s označením „EBA/REC/2017/03“. Oznámenia majú v mene príslušných orgánov predkladať osoby, ktoré sú oprávnené podávať správy o dodržaní v mene svojich príslušných orgánov. Akúkoľvek zmenu stavu dodržiavania ustanovení treba takisto oznámiť orgánu EBA.

4. Oznámenia budú uverejnené na webovom sídle orgánu EBA v súlade s článkom 16 ods. 3.

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12).

2. Predmet úpravy, rozsah pôsobnosti a vymedzenia pojmov

Predmet úpravy a rozsah pôsobnosti

1. V týchto odporúčaniach sa bližšie určujú podmienky pre outsourcing uvedené v usmerneniach CEBS o outsourcingu zo 14. decembra 2006, pričom sa vzťahujú na outsourcing inštitúcií vymedzených v článku 4 ods. 1 bode 3 nariadenia (EÚ) č. 575/2013 poskytovateľom cloudových služieb.

Adresáti

2. Tieto odporúčania sú určené príslušným orgánom vymedzeným v článku 4 ods. 2 bode i) nariadenia (EÚ) č. 1093/2010 a inštitúciám vymedzeným v článku 4 ods. 1 bode 3 nariadenia (EÚ) č. 575/2013.[2]

Vymedzenie pojmov

3. Pokiaľ nie je uvedené inak, pojmy použité a vymedzené v smernici 2013/36/EÚ[3] o kapitálových požiadavkách a v usmerneniach CEBS majú v týchto odporúčaniach rovnaký význam. Na účely týchto odporúčaní sa okrem toho uplatňujú tieto vymedzenia pojmov:

Cloudové služby	Služby poskytované pomocou cloud computingu, teda modelu umožňujúceho všadeprítomný, pohodlný sieťový prístup na požiadanie k spoločne využívaným prostriedkom výpočtovej techniky (napr. siete, servery, úložisko, aplikácie a služby), ktorý sa môže rýchlo zriadiť a zrušiť s minimálnou potrebou riadenia a minimálnou interakciou s poskytovateľom služby.
Verejný cloud	Cloudová infraštruktúra, ktorá je k dispozícii na otvorené použitie širokou verejnosťou.
Súkromný cloud	Cloudová infraštruktúra, ktorá je k dispozícii na výlučné použitie jednou inštitúciou.
Komunitný cloud	Cloudová infraštruktúra, ktorá je k dispozícii na výlučné použitie konkrétnou komunitou inštitúcií vrátane niekoľkých inštitúcií jednej skupiny.

[2] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012.

[3] Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES.

Hybridný cloud	Cloudová infraštruktúra, ktorá pozostáva z dvoch alebo viacerých odlišných cloudových infraštruktúr.

3. Implementácia

Dátum uplatňovania

5. Tieto odporúčania sa uplatňujú od 1. júla 2018.

4. Odporúčania týkajúce sa outsourcingu poskytovateľom cloudových služieb

4.1 Hodnotenie významnosti

1. Inštitúcie využívajúce outsourcing by mali pred každým outsourcingom svojich činností posúdiť, ktoré činnosti by sa mali považovať za významné. Inštitúcie by mali vykonať toto posúdenie významnosti činností na základe usmernenia 1 písm. f) usmernení CEBS a najmä pokiaľ ide o outsourcing poskytovateľom cloudových služieb, mali by vziať do úvahy tieto skutočnosti:

    (a) kritickosť a profil inherentného rizika činností, ktoré majú byť outsourcované, t. j. či sú to činnosti, ktoré sú rozhodujúce pre kontinuitu činnosti/životaschopnosť inštitúcie a jej povinnosti voči zákazníkom;

    (b) priamy prevádzkový vplyv výpadkov a súvisiace právne riziká a riziká straty dobrej povesti;

    (c) vplyv, ktorý môže mať akékoľvek narušenie činnosti na finančné vyhliadky inštitúcie;

    (d) potenciálny vplyv, ktorý by mohlo mať porušenie dôvernosti alebo zlyhanie integrity údajov na inštitúciu a jej zákazníkov.

4.2 Povinnosť primerane informovať orgány dohľadu

2. Inštitúcie využívajúce outsourcing by mali primerane informovať príslušné orgány o významných činnostiach, ktoré plánujú outsourcovať poskytovateľom cloudových služieb. Inštitúcie by tu mali konať na základe odseku 4.3 usmernení CEBS a v každom prípade by mali príslušným orgánom sprístupniť tieto informácie:

    (a) názov poskytovateľa cloudových služieb a názov jeho materskej spoločnosti (ak existuje);
    (b) opis činností a údajov, ktoré sa majú outsourcovať;
    (c) krajina alebo krajiny, v ktorých sa má služba vykonávať (vrátane umiestnenia údajov);
    (d) dátum začiatku poskytovania služby;
    (e) prípadný dátum posledného predĺženia zmluvy;
    (f) rozhodné právo, ktorým sa riadi zmluva;
    (g) dátum uplynutia platnosti služby alebo prípadný dátum ďalšieho predĺženia zmluvy.

3. V nadväznosti na informácie poskytnuté v súlade s predchádzajúcim odsekom môže príslušný orgán požiadať inštitúciu, ktorá využíva outsourcing o ďalšie informácie o jej analýze rizík pre významné činnosti, ktoré sa majú outsourcovať, napríklad:

   (a) či má poskytovateľ cloudových služieb plán na zabezpečenie kontinuity činnosti, ktorý je vhodný pre služby poskytované inštitúcii, ktorá outsourcing využíva;
   (b) či má inštitúcia využívajúca outsourcing stratégiu ukončenia angažovanosti v prípade, že jedna zo strán zmluvu ukončí alebo v prípade prerušenia poskytovania služieb poskytovateľom cloudových služieb;
   (c) či inštitúcia využívajúca outsourcing udržiava zručnosti a zdroje potrebné na primerané monitorovanie outsourcovaných činností.

4. Inštitúcia využívajúca outsourcing by mala viesť aktualizovaný register informácií o všetkých jej významných a nevýznamných činnostiach outsourcovaných poskytovateľom cloudových služieb na úrovni inštitúcie a skupiny. Inštitúcia využívajúca outsourcing by mala príslušnému orgánu na jeho žiadosť sprístupniť kópiu dohody o outsourcingu a súvisiace informácie zaznamenané v tomto registri, bez ohľadu na to, či činnosť outsourcovaná poskytovateľovi cloudových služieb bola inštitúciou vyhodnotená ako významná.

5. V uvedenom registri by mali byť obsiahnuté prinajmenšom tieto informácie:

   (a) informácie uvedené v odseku 2 písm. a) až g), ak ešte neboli poskytnuté;
   (b) druh outsourcingu (model cloudových služieb a model používania cloudu, t. j. verejný/súkromný/hybridný/komunitný cloud);
   (c) strany, ktoré prijímajú cloudové služby podľa dohody o outsourcingu;
   (d) prípadný doklad o schválení outsourcingu riadiacim orgánom alebo jeho delegovanými výbormi;
   (e) názvy prípadných subdodávateľov;
   (f) krajina, v ktorej je poskytovateľ cloudových služieb/hlavný subdodávateľ zaregistrovaný;
   (g) či bol outsourcing vyhodnotený ako významný (áno/nie);
   (h) dátum posledného hodnotenia významnosti outsourcovaných činností inštitúcie;
   (i) či poskytovateľ cloudových služieb/subdodávateľ, resp. subdodávatelia podporujú obchodné operácie, ktoré sú časovo kritické (áno/nie);
   (j) hodnotenie nahraditeľnosti poskytovateľa cloudových služieb (ako jednoduché, náročné alebo nemožné);
   (k) identifikácia alternatívneho poskytovateľa služieb, ak je to možné;
   (l) dátum posledného vyhodnotenia rizika dohody o outsourcingu alebo subdodávateľskej dohody.

4.3 Prístupové a audítorské práva

Pre inštitúcie

6. Na základe usmernenia 8 ods. 2 písm. g) usmernení CEBS a na účely cloudového outsourcingu by inštitúcie využívajúce outsourcing mali ďalej zabezpečiť, aby uzavreli písomnú dohodu s poskytovateľom cloudových služieb, ktorou tento preberá záväzok:

(a) poskytovať inštitúcii, tretej strane na tento účel vymenovanej inštitúciou a štatutárnemu audítorovi inštitúcie úplný prístup do svojich obchodných priestorov (ústredí a prevádzkových centier), ako aj k celej škále zariadení, systémov, sietí a údajov používaných na poskytovanie outsourcovaných služieb (právo na prístup);

(b) udeliť inštitúcii, tretej strane na tento účel vymenovanej inštitúciou a štatutárnemu audítorovi inštitúcie neobmedzené práva na previerku a audit v súvislosti s outsourcovanými službami (právo na audit).

7. Účinný výkon práv na prístup a audit by nemal byť marený alebo obmedzovaný zmluvnými podmienkami. V prípade, že by vykonávanie auditov alebo použitie určitých audítorských techník mohlo predstavovať riziko pre zariadenia iného klienta, mali by sa dohodnúť alternatívne spôsoby na zabezpečenie podobného stupňa spoľahlivosti, ktorý inštitúcia vyžaduje.

8. Inštitúcia využívajúca outsourcing by mala uplatňovať svoje práva na audit a prístup na základe informácií o riziku. V prípade, že inštitúcia využívajúca outsourcing nepoužíva vlastné audítorské zdroje, mala by zvážiť použitie aspoň jedného z týchto nástrojov:

(a) spoločné audity organizované spoločne s inými klientmi toho istého poskytovateľa cloudových služieb a vykonávané týmito klientmi alebo nimi určenou treťou stranou s cieľom efektívnejšie využívať audítorské zdroje a znížiť organizačné zaťaženie ako klientov, tak aj poskytovateľa cloudových služieb;

(b) certifikácie tretích strán a správy tretích strán alebo správy o vnútornom audite sprístupnené poskytovateľom cloudových služieb za predpokladu, že:

i. inštitúcia využívajúca outsourcing zabezpečí, aby rozsah certifikácie alebo správy o audite pokrýval systémy (t. j. procesy, aplikácie, infraštruktúru, dátové centrá atď.) a kontroly označené inštitúciou využívajúcou outsourcing ako kľúčové;
ii. inštitúcia využívajúca outsourcing priebežne dôkladne hodnotí obsah certifikácie alebo správ o audite a zabezpečí najmä, aby boli kľúčové kontroly stále zahrnuté v budúcich verziách správy o audite a overí, či certifikácia alebo správa o audite nie sú zastarané;
iii. inštitúcia využívajúca outsourcing je spokojná so schopnosťami strany poskytujúcej certifikáciu alebo vykonávajúcej audit (napr. s ohľadom na rotáciu spoločnosti poskytujúcej certifikáciu alebo vykonávajúcej audit, kvalifikácie, odborné znalosti, opätovné vykonávanie/overovanie dôkazov v základnom audítorskom spise);
iv. certifikáty sa vydávajú a audity sa vykonávajú podľa všeobecne uznávaných noriem a zahŕňajú skúšku prevádzkovej účinnosti zavedených kľúčových kontrol;
v. inštitúcia využívajúca outsourcing má zmluvné právo požiadať o rozšírenie rozsahu certifikácie alebo správ o audite na niektoré relevantné systémy a/alebo kontroly. Počet a frekvencia takýchto žiadostí o zmenu rozsahu by mali byť primerané a legitímne z hľadiska riadenia rizík.

9. Vzhľadom na to, že cloudové riešenia majú vysokú úroveň technickej zložitosti, inštitúcia využívajúca outsourcing by mala overiť, či zamestnanci vykonávajúci audit – či už ide o vlastných vnútorných audítorov alebo o skupinu audítorov konajúcich v jej mene, alebo o audítorov určených poskytovateľom cloudových služieb – alebo, v prípade potreby, zamestnanci, ktorí skúmajú certifikáty tretích strán alebo správy poskytovateľa služieb o audite, majú potrebné zručnosti a znalosti na vykonávanie účinných a relevantných auditov a/alebo hodnotení cloudových riešení.

Pre príslušné orgány

10. Na základe usmernenia 8 ods. 2 písm. h) usmernení CEBS a na účely cloudového outsourcingu by inštitúcie využívajúce outsourcing mali zabezpečiť uzavretie písomnej dohody s poskytovateľom cloudových služieb, ktorou tento preberá záväzok:

    (a) poskytovať príslušnému orgánu vykonávajúcemu dohľad nad inštitúciou využívajúcou outsourcing (alebo tretej strane, ktorú tento orgán určil na tento účel) úplný prístup do obchodných priestorov poskytovateľa cloudových služieb (ústredí a prevádzkových centier), ako aj k celej škále zariadení, systémov, sietí a údajov používaných na poskytovanie služieb inštitúcii využívajúcej outsourcing (právo na prístup);

    (b) udeliť príslušnému orgánu vykonávajúcemu dohľad nad inštitúciou využívajúcou outsourcing (alebo tretej strane, ktorú tento orgán určil na tento účel) neobmedzené práva na previerku a audit v súvislosti s outsourcovanými službami (právo na audit).

11. Inštitúcia využívajúca outsourcing by mala zabezpečiť, aby zmluvné podmienky nebránili príslušnému orgánu vo vykonávaní jeho funkcie dohľadu a cieľov.

12. Informácie, ktoré príslušné orgány získajú z výkonu práv na prístup a audit by mali podliehať požiadavkám na služobné tajomstvo a dôvernosť, podľa článku 53 a nasl. smernice 2013/36/EÚ (CRD IV). Príslušné orgány by sa mali zdržať uzatvárania akýchkoľvek zmluvných dohôd alebo vyhlásení, ktoré by im bránili dodržiavať ustanovenia práva Únie týkajúce sa dôvernosti, služobného tajomstva a výmeny informácií.

13. Na základe zistení svojho auditu by mal príslušný orgán riešiť všetky zistené nedostatky, ak je to potrebné, uložením opatrení priamo inštitúcii využívajúcej outsourcing.

4.4 Predovšetkým v prípade práva na prístup

14. Dohoda uvedená v odsekoch 6 a 10 by mala zahŕňať tieto ustanovenia:

    (a) Strana, ktorá má v úmysle uplatniť svoje právo na prístup (inštitúcia, príslušný orgán, audítor alebo tretia strana konajúca v mene inštitúcie alebo príslušného orgánu) by mala pred plánovanou prehliadkou relevantných obchodných priestorov na mieste v primeranom čase túto prehliadku oznámiť, s výnimkou

prípadu, ak v dôsledku núdzovej alebo krízovej situácie nie je možné včasné oznámenie.

(b) Poskytovateľ cloudových služieb je v súvislosti s prehliadkou na mieste povinný plne spolupracovať s príslušnými orgánmi, ako aj s inštitúciou a jej audítorom.

4.5 Bezpečnosť údajov a systémov

15. Ako sa uvádza v usmernení 8 ods. 2 písm. e) usmernení CEBS, zmluvou o outsourcingu by sa poskytovateľovi outsourcingových služieb mala ukladať povinnosť chrániť dôvernosť informácií zasielaných finančnou inštitúciou. V súlade s usmernením 6 ods. 6 písm. e) usmernení CEBS by inštitúcie mali vykonávať opatrenia na zabezpečenie kontinuity služieb, ktoré poskytujú poskytovateľmi outsourcingových služieb. Vychádzajúc z usmernenia 8 ods. 2 písm. b) a z usmernenia 9 usmernení CEBS by sa príslušné potreby inštitúcií využívajúcich outsourcing týkajúce sa kvality a výkonnosti mali zohľadniť v písomných zmluvách o outsourcingu a dohodách o úrovni poskytovaných služieb. Tieto bezpečnostné hľadiská by sa okrem toho mali priebežne monitorovať (usmernenie 7).

16. Na účely predchádzajúceho odseku by mala inštitúcia pred vykonaním outsourcingu a na účely oznámenia príslušného rozhodnutia vykonať aspoň nasledujúce:

(a) identifikovať a klasifikovať svoje činnosti, procesy a súvisiace údaje a systémy, pokiaľ ide o citlivosť a požadovanú ochranu;

(b) vykonať dôkladný výber činností, procesov a súvisiacich údajov a systémov na základe rizík, pri ktorých sa zvažuje ich outsourcing prostredníctvom využitia cloud computingu;

(c) definovať a rozhodnúť o primeranej úrovni ochrany dôvernosti údajov, kontinuity outsourcovaných činností a celistvosti a vysledovateľnosti údajov a systémov v kontexte plánovaného cloudového outsourcingu. Inštitúcie by v prípade potreby mali zvážiť aj špecifické opatrenia pre prenášané údaje, údaje v pamäti a uložené údaje, napríklad použitie šifrovacích technológií v kombinácii s vhodnou štruktúrou správy kľúčov.

17. Následne by inštitúcie mali zabezpečiť, aby mali uzavretú písomnú dohodu s poskytovateľom cloudových služieb, v ktorej sú okrem iného stanovené záväzky uvedené v odseku 16 písm. c).

18. Inštitúcie by mali priebežne monitorovať vykonávanie činností a bezpečnostných opatrení v súlade s usmernením 7 usmernení CEBS vrátane incidentov, a podľa potreby by mali preskúmať, či ich outsourcing činností je v súlade s predchádzajúcimi odsekmi a ihneď podniknúť potrebné nápravné opatrenia.

4.6 Umiestnenie údajov a spracovanie údajov

19. Ako sa uvádza v usmernení 4 ods. 4 usmernení CEBS, inštitúcie by mali venovať osobitnú pozornosť uzatváraniu a riadeniu dohôd o outsourcingu vykonávaných mimo EHP z dôvodu možných rizík súvisiacich s ochranou údajov a rizík v oblasti účinného dohľadu zo strany orgánu dohľadu.

20. Inštitúcia využívajúca outsourcing by pri outsourcingu do cloudového prostredia mala pri údajoch a úvahách o umiestnení spracovania údajov uplatňovať prístup na základe rizík. Hodnotenie by sa malo týkať potenciálnych vplyvov rizika vrátane právnych rizík a problémov súvisiacich s dodržiavaním predpisov, ako aj obmedzení dohľadu súvisiacich s krajinami, v ktorých sú outsourcované služby poskytované alebo sa pravdepodobne môžu poskytovať a kde sa ukladajú alebo sa môžu ukladať údaje. Hodnotenie by malo zahŕňať úvahy o širšej politickej a bezpečnostnej stabilite príslušných jurisdikcií; o zákonoch platných v týchto jurisdikciách (vrátane zákonov o ochrane údajov); a o ustanoveniach o výkone práva platných v týchto jurisdikciách, ako aj ustanoveniach o platobnej neschopnosti, ktoré by platili v prípade zlyhania poskytovateľa cloudových služieb. Inštitúcia využívajúca outsourcing by mala zabezpečiť, aby sa tieto riziká udržiavali v prijateľných medziach zodpovedajúcich významnosti outsourcovanej činnosti.

4.7 Reťazový outsourcing

21. Ako sa uvádza v usmernení 10 usmernení CEBS, inštitúcie by mali brať do úvahy riziká spojené s reťazovým outsourcingom, pri ktorom poskytovateľ outsourcingových služieb zadá prvky služby iným poskytovateľom. Inštitúcia využívajúca outsourcing by mala súhlasiť s reťazovým outsourcingom iba vtedy, ak aj subdodávateľ bude v plnej miere plniť povinnosti existujúce medzi inštitúciou využívajúcou outsourcing a poskytovateľom outsourcingových služieb. Inštitúcia využívajúca outsourcing by okrem toho mala podniknúť primerané kroky na riešenie rizika akéhokoľvek nedostatku alebo zlyhania pri poskytovaní subdodávateľsky zadaných činností, ktoré majú významný vplyv na schopnosť poskytovateľa outsourcingových služieb plniť jeho povinnosti vyplývajúce z dohody o outsourcingu.

22. V dohode o outsourcingu medzi inštitúciou využívajúcou outsourcing a poskytovateľom cloudových služieb by sa mali špecifikovať všetky druhy činností, ktoré sú vylúčené z potenciálnych subdodávateľských zmlúv, a malo by sa stanoviť, že poskytovateľ cloudových služieb nesie plnú zodpovednosť za služby, ako aj dohľad nad službami, ktoré zadal subdodávateľom.

23. V dohode o outsourcingu by mala byť zahrnutá aj povinnosť poskytovateľa cloudových služieb informovať inštitúciu využívajúcu outsourcing o všetkých plánovaných významných zmenách v subdodávateľoch alebo subdodávateľských službách uvedených v pôvodnej dohode, ktoré by mohli ovplyvniť schopnosť poskytovateľa služieb plniť jeho povinnosti podľa dohody o outsourcingu. Lehota na oznámenie týchto zmien by mala byť vopred zmluvne dohodnutá, aby inštitúcia využívajúca outsourcing mohla vykonať hodnotenie rizika vplyvov navrhovaných zmien

pred tým, ako skutočná zmena v subdodávateľoch alebo subdodávateľských službách nadobudne účinnosť.

24. V prípade, že poskytovateľ cloudových služieb plánuje zmeny v subdodávateľoch alebo subdodávateľských službách, ktoré by mali nepriaznivý vplyv na hodnotenie rizika dohodnutých služieb, inštitúcia využívajúca outsourcing by mala mať právo vypovedať zmluvu.

25. Inštitúcia využívajúca outsourcing by mala priebežne skúmať a monitorovať vykonávanie celej služby, a to bez ohľadu na to, či ju poskytuje poskytovateľ cloudových služieb alebo jeho subdodávatelia.

4.8 Pohotovostné plány a stratégie ukončenia angažovanosti

26. Ako sa uvádza v usmernení 6.1, usmernení 6 ods. 6 písm. e) a usmernení 8 ods. 2 písm. d) usmernení CEBS, inštitúcia využívajúca outsourcing by mala plánovať a vykonávať opatrenia na udržanie kontinuity svojej činnosti v prípade, že poskytovateľ outsourcingových služieb zlyhá alebo sa zhorší v neprijateľnom rozsahu. Tieto opatrenia by mali obsahovať pohotovostné plánovanie a jasne vymedzenú stratégiu ukončenia angažovanosti. Okrem toho by zmluva o outsourcingu mala obsahovať doložku o vypovedaní a riadení ukončenia angažovanosti, ktorá umožní prevod činností, ktoré poskytuje poskytovateľ outsourcingových služieb, na iného poskytovateľa outsourcingových služieb, alebo ich opätovné začlenenie do pôvodnej inštitúcie.

27. Inštitúcia využívajúca outsourcing by mala okrem toho zabezpečiť, aby v prípade potreby mohla ukončiť dohodu o outsourcingu, a to bez neprimeraného narušenia poskytovania jej služieb alebo bez nepriaznivých vplyvov na jej dodržiavanie regulačného režimu a bez nepriaznivého vplyvu na kontinuitu a kvalitu poskytovania jej služieb klientom. Na dosiahnutie tohto cieľa by inštitúcia využívajúca outsourcing mala:

    (a) vypracovať a vykonávať komplexné, zdokumentované a prípadne aj dostatočne overené plány ukončenia angažovanosti;

    (b) identifikovať alternatívne riešenia a vypracovať plány prechodu, aby mohla odstrániť a presunúť existujúce činnosti a údaje od poskytovateľa cloudových služieb na tieto riešenia kontrolovaným a dostatočne overeným spôsobom, pri zohľadnení problémov s umiestnením údajov a udržiavaním kontinuity činnosti počas fázy prechodu;

    (c) zabezpečiť, aby dohoda o outsourcingu obsahovala povinnosť poskytovateľa cloudových služieb dostatočne podporovať inštitúciu využívajúcu outsourcing pri riadnom presune činnosti na iného poskytovateľa služieb alebo pod priame riadenie inštitúcie využívajúcej outsourcing v prípade vypovedania dohody o outsourcingu.

28. Pri vytváraní stratégií ukončenia angažovanosti by inštitúcia využívajúca outsourcing mala zvážiť tieto skutočnosti:

    (a) vypracovanie kľúčových ukazovateľov rizika s cieľom určiť neprijateľnú úroveň služieb;

(b) vykonanie analýzy vplyvu na činnosť primeranú outsourcovaným činnostiam s cieľom určiť, aké ľudské a materiálne zdroje by boli potrebné na vykonanie plánov ukončenia angažovanosti a koľko času by to trvalo;

(c) pridelenie úloh a zodpovedností pri riadení plánov ukončenia angažovanosti a prechodných činností;

(d) definovať kritériá úspešnosti prechodu.

29. Inštitúcia využívajúca outsourcing by do svojho priebežného monitorovania služieb a dohľade nad službami poskytovanými poskytovateľom cloudových služieb mala zahrnúť ukazovatele, ktoré môžu spustiť plán ukončenia angažovanosti.