

EBA/REC/2017/03

28/03/2018

Doporučení

ohledně zajištění cloudových služeb u externích poskytovatelů

1. Dodržování předpisů a oznamovací povinnost

Status těchto doporučení

1. Tento dokument obsahuje doporučení vydaná podle článku 16 nařízení (EU) č. 1093/2010¹. V souladu s čl. 16 odst. 3 nařízení (EU) č. 1093/2010 příslušné orgány a finanční instituce vynaloží veškeré úsilí, aby se těmito doporučeními řídily.
2. Doporučení formulují názor orgánu EBA na náležité postupy dohledu v rámci Evropského systému dohledu nad finančním trhem nebo na to, jak by unijní právní předpisy měly být uplatňovány v konkrétní oblasti. Příslušné orgány ve smyslu čl. 4 odst. 2 nařízení (EU) č. 1093/2010, na které se tato doporučení vztahují, by s nimi měly být v souladu a začlenit je do svých postupů (např. pozměněním právního rámce nebo dohledových postupů), včetně případů, kdy jsou doporučení zaměřena v první řadě na instituce.

Oznamovací povinnosti

3. V souladu s čl. 16 odst. 3 nařízení (EU) č. 1093/2010 musí příslušné orgány do 28.05.2018 orgánu EBA oznámit, zda se těmito doporučeními řídí nebo hodlají řídit, a v opačném případě uvést do tohoto data důvody, proč se jimi neřídí či nehodlají řídit. Neposkytnou-li příslušné orgány oznámení v této lhůtě, bude mít orgán EBA za to, že se těmito doporučeními neřídí nebo nehodlají řídit. Oznámení by měla být zasílána na formuláři, který je k dispozici na internetových stránkách orgánu EBA, na adresu compliance@eba.europa.eu s označením „EBA/REC/2017/03“. Oznámení by měly předkládat osoby s příslušným oprávněním oznamovat, zda se jejich příslušné orgány těmito doporučeními řídí nebo hodlají řídit. Jakoukoli změnu stavu dodržování doporučení je rovněž nutno oznámit orgánu EBA.
4. Oznámení budou zveřejněna na internetových stránkách orgánu EBA v souladu s čl. 16 odst. 3.

¹ Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovníctví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12).

2. Předmět, oblast působnosti a definice

Předmět a oblast působnosti

1. Tato doporučení dále upřesňují podmínky pro externí zajištění služeb uvedené v rámci pokynů Evropského výboru orgánů bankovního dohledu (CEBS) k externímu zajištění služeb ze dne 14. prosince 2006 a vztahují se na externí zajištění služeb institucemi podle čl. 4 odst. 1 bodu 3 nařízení (EU) č. 575/2013 u poskytovatelů cloudových služeb.

Adresáti

2. Tato doporučení jsou určena příslušným orgánům podle čl. 4 odst. 2 bodu i) nařízení (EU) č. 1093/2010 a institucím podle čl. 4 odst. 1 bodu 3 nařízení č. 575/2013².

Definice

3. Není-li uvedeno jinak, pojmy použité a vymezené ve směrnici 2013/36/EU³, které se týkají kapitálových požadavků, a v pokynech CEBS mají v těchto doporučeních stejný význam. Kromě toho pro účely těchto doporučení platí tyto definice:

Cloudové služby	Služby poskytované za použití cloud computingu, což je model, který na žádost umožňuje pohodlný síťový přístup kdykoliv a odkudkoliv ke sdílené množině konfigurovatelných výpočetních zdrojů (např. sítím, serverům, úložištím, aplikacím a službám), které lze rychle poskytnout či spustit s vynaložením minimálních prostředků pro řízení příslušné operace a bez zásahu ze strany poskytovatele služby.
Veřejný cloud	Cloudová infrastruktura, kterou může volně využívat široká veřejnost.
Soukromý cloud	Cloudová infrastruktura určená pro výlučné užívání jedinou institucí.
Komunitní cloud	Cloudová infrastruktura určená pro výlučné užívání konkrétní komunitou institucí, včetně několika institucí v jediné skupině.
Hybridní cloud	Cloudová infrastruktura, která se skládá ze dvou či více různých cloudových infrastruktur.

² Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012.

³ Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES.

3. Provedení

Datum použitelnosti

5. Tato doporučení se použije ode dne 1. července 2018.

4. Doporučení ohledně zajištění cloudových služeb u externích poskytovatelů

4.1 Posouzení významnosti

1. Instituce externě zadávající činnost by měly před samotným externím zadáním posoudit, které činnosti lze považovat za významné. Instituce by měly provést toto posouzení významnosti činností na základě pokynu 1 písm. f) pokynů CEBS, a pokud jde o zajištění služeb zejména u externích poskytovatelů cloudových služeb, měly by zohlednit všechny tyto aspekty:
 - a) kritičnost a profil přirozeného rizika činností, jež mají být externě zadány, čili zda se jedná o činnosti kritické pro kontinuitu a životaschopnost provozu dané instituce a pro její závazky vůči zákazníkům;
 - b) přímý provozní dopad odstavek a s tím související právní rizika a rizika poškození dobré pověsti;
 - c) dopad, který by mohlo mít jakékoli narušení činnosti na vyhlídky příjmů dané instituce;
 - d) potenciální dopad, který by mohlo mít porušení důvěrnosti nebo selhání integrity dat na instituci a její zákazníky.

4.2 Povinnost patřičně informovat orgány dohledu

2. Instituce externě zadávající činnost by měly patřičně informovat příslušné orgány o významných činnostech, které mají zajistit externí poskytovatelé cloudových služeb. Instituce by tak měly jednat na základě bodu 4.3 pokynů CEBS a v každém případě by měly příslušným orgánům poskytnout tyto informace:
 - a) jméno poskytovatele cloudových služeb a případný název jeho mateřské společnosti;
 - b) popis činností a dat, jež mají být externě zadány;
 - c) země, ve které/kterých bude služba vykonávána (včetně umístění dat);
 - d) datum zahájení služby;
 - e) (případné) poslední datum obnovení smlouvy;
 - f) použitelné právní předpisy, jimiž se smlouva řídí;
 - g) datum vypršení platnosti služby nebo (případné) příští datum obnovení smlouvy.
3. S ohledem na informace poskytnuté v souladu s předchozím odstavcem může příslušný orgán požádat instituci externě zadávající činnost o doplňující informace k analýze rizik týkající se významných činností, které mají být externě zadány, jako například:

- a) zda má poskytovatel cloudové služby plán zachování kontinuity činnosti, který je vhodný pro služby poskytované institucí externě zadávající činnost;
 - b) zda má instituce externě zadávající činnost strategii odstoupení pro případ, že kterákoli ze stran činnost ukončí nebo že dojde k narušení zajišťování služeb poskytovatelem cloudových služeb;
 - c) zda si instituce externě zadávající činnost zachovává schopnosti a prostředky nezbytné k přiměřenému sledování externě zajišťovaných činností.
4. Instituce externě zadávající činnost by měla uchovávat aktualizovanou evidenci informací o všech svých významných i nevýznamných činnostech externě zadaných poskytovatelům cloudových služeb na úrovni institucí a skupin. Instituce externě zadávající činnost by měla na požádání zpřístupnit příslušnému orgánu kopii dohody o externím zajišťování činnosti a související informace zaznamenané v evidenci, bez ohledu na to, zda instituce posoudila činnost zajišťovanou externím poskytovatelem cloudových služeb jako významnou, či nikoliv.
5. V evidenci zmíněné v předchozím odstavci by měly být zahrnuty alespoň následující informace:
- a) informace uvedené v odst. 2 písm. a) až g), pokud nebyly dosud poskytnuty;
 - b) typ externího zadávání činnosti (model cloudových služeb a model zavedení cloudu, tj. veřejný/soukromý/hybridní/komunitní cloud);
 - c) strany přijímající cloudové služby podle dohody o externím zajišťování činnosti;
 - d) doklad o schválení externího zadání činnosti vedoucím orgánem nebo případně jeho pověřenými výbory;
 - e) jména všech případných subdodavatelů;
 - f) země, ve které je poskytovatel cloudových služeb nebo hlavní subdodavatel registrován;
 - g) zda byla externě zajišťovaná činnost posouzena jako významná (ano/ne);
 - h) datum posledního posouzení významnosti externě zajišťovaných činností provedeného dotyčnou institucí;
 - i) zda poskytovatel cloudových služeb nebo subdodavatel(é) podporují obchodní operace, které jsou z časového hlediska kritické (ano/ne);
 - j) posouzení nahraditelnosti poskytovatele cloudových služeb (zda je jednoduchá, složitá nebo nemožná);
 - k) určení případného náhradního poskytovatele služeb;
 - l) datum posledního posouzení rizik dohody o externím zajišťování činnosti nebo o subdodávkách.

4.3 Přístupové právo a právo na audit

Pro instituce

6. Na základě pokynu 8 bodu 2 písm. g) pokynů CEBS a za účelem externího zadávání cloudové činnosti by instituce externě zadávající činnost měly dále zajistit, aby měly uzavřenou písemnou dohodu s poskytovatelem cloudových služeb, ve které se posledně jmenovaný zavazuje, že:
- a) poskytne instituci, jakékoli třetí straně za tímto účelem institucí jmenované a statutárnímu auditorovi instituce úplný přístup do svých firemních prostor (do sídla a

provozních středisek), včetně celé škály zařízení, systémů, sítí a dat používaných v rámci poskytování externě zajišťovaných služeb (přístupové právo);

- b) udělí instituci, jakékoli třetí straně za tímto účelem institucí jmenované a statutárnímu auditorovi instituce neomezená práva inspekce a auditu související s externě zajišťovanými službami (právo na audit).
7. Smluvní ujednání by neměla ztěžovat či omezovat účinné uplatňování přístupového práva a práva na audit. Pokud by provádění auditů nebo používání některých postupů auditu mohlo vytvořit riziko pro prostředí jiného klienta, měly by být schváleny alternativní způsoby, jak zajistit podobnou míru jistoty požadovanou institucí.
8. Instituce externě zadávající činnost by měla uplatňovat svá práva na audit a na přístup na základě rizik. V případech, kdy instituce externě zadávající činnost nevyužívá své vlastní auditní zdroje, by měla zvážit, zda použije alespoň jeden z těchto nástrojů:
- a) Hromadné kontroly organizované společně s jinými klienty stejného poskytovatele cloudových služeb, které jsou vykonávány těmito klienty nebo třetí stranou jimi určenou, aby byly auditní zdroje využívány efektivněji a aby se snížilo organizační zatížení klientů i poskytovatele cloudových služeb.
 - b) Osvědčení vydané třetí stranou a zprávy o auditu podané třetí stranou nebo o vnitřním auditu zpřístupněné poskytovatelem cloudových služeb za předpokladu, že:
 - i. Instituce externě zadávající činnost zaručí, že do oblasti působnosti osvědčení nebo zprávy o auditu spadají systémy (tj. procesy, uplatňování, infrastruktura, datová centra atd.) a kontroly určené institucí externě zadávající činnost jako klíčové.
 - ii. Instituce externě zadávající činnost soustavně provádí důkladné posouzení obsahu osvědčení nebo zpráv o auditu a zejména zajistí, aby byly klíčové kontroly zahrnuty i v budoucích verzích zprávy o auditu, a ověří, že osvědčení nebo zpráva o auditu nejsou zastaralé.
 - iii. Instituce externě zadávající činnost je spokojená se způsobilostí strany, která provádí osvědčení či audit (např. pokud jde o střídání společnosti provádějící osvědčení či audit, o kvalifikaci, odborné znalosti, opakované provádění či ověření důkazních informací uvedených v auditorském spisu).
 - iv. Osvědčení jsou vydávána a audity prováděny v rozporu se všeobecně uznávanými standardy a zahrnují test provozní účelnosti zavedených klíčových kontrol.
 - v. Instituce externě zadávající činnost má smluvně stanovené právo požadovat rozšíření oblasti působnosti osvědčení nebo zpráv o auditu na některé podstatné systémy či kontroly. Počet a četnost těchto žádostí o úpravu oblasti působnosti by měly být rozumné a legitimní z hlediska řízení rizik.
9. Vzhledem k tomu, že cloudová řešení jsou po technické stránce značně složitá, instituce externě zadávající činnost by měla ověřit, že zaměstnanci provádějící audit – ať už interní auditoři či skupina auditorů jednající jejím jménem, nebo auditoři jmenovaní poskytovatelem cloudových

služeb – nebo případně zaměstnanci, kteří provádějí přezkoumání osvědčení vydaných třetí stranou nebo zpráv o auditu poskytovatele služeb, si osvojili náležité dovednosti a znalosti potřebné k provádění účinných a odpovídajících auditů či posouzení cloudových řešení.

Pro příslušné orgány

10. Na základě pokynu 8 bodu 2 písm. h) pokynů CEBS a za účelem externího zadávání cloudové činnosti by instituce externě zadávající činnost měly zajistit, že mají uzavřenou písemnou dohodu s poskytovatelem cloudových služeb, ve které se posledně jmenovaný zavazuje, že:

- a) poskytne příslušnému orgánu, který dohlíží na instituci externě zadávající činnost (nebo jakékoli třetí straně určené orgánem k tomuto účelu), úplný přístup do firemních prostor poskytovatele cloudových služeb (do sídla a operačních středisek), včetně celé škály zařízení, systémů, sítí a dat použitých v rámci poskytování služeb instituci externě zadávající činnost (přístupové právo);
- b) udělí příslušnému orgánu, který dohlíží na instituci externě zadávající činnost (nebo jakékoli třetí straně určené orgánem k tomuto účelu), neomezená práva inspekce a auditu související s externě zadávanými službami (právo na audit).

11. Instituce externě zadávající činnost by měla zajistit, aby smluvní ujednání nebránila příslušnému orgánu v provádění jeho kontrolních funkcí a cílů.

12. Informace, které příslušné orgány získají uplatněním práva na přístup a na audit, by měly podléhat požadavkům na zachování profesního tajemství a důvěrnosti uvedených v článku 53 a násl. směrnice 2013/36/EU (CRD IV). Příslušné orgány by se měly zdržet uzavírání jakýchkoli smluvních ujednání nebo prohlášení, která by jim mohla bránit v dodržování ustanovení právních předpisů Unie o důvěrnosti, profesním tajemství a výměně informací.

13. Na základě zjištění vyplývajících z auditu by měl příslušný orgán v případě nutnosti řešit veškeré zjištěné nedostatky tím, že uloží opatření přímo instituci externě zadávající činnost.

4.4 Podrobnosti o přístupovém právu

14. Dohoda uvedená v odstavcích 6 a 10 by měla zahrnovat tato ustanovení:

- a) Strana, která zamýšlí uplatnit své právo na přístup (instituce, příslušný orgán, auditor nebo třetí strana jednající jménem instituce nebo příslušného orgánu), by měla plánovanou kontrolu příslušného firemního prostoru oznámit předem v přiměřené lhůtě, není-li včasné předchozí oznámení nemožné z důvodu mimořádné situace nebo krize.
- b) Od poskytovatele cloudových služeb se požaduje, aby plně spolupracoval s příslušnými orgány, jakož i s institucí a jejím auditorem, v souvislosti s kontrolou na místě.

4.5 Zabezpečení dat a systémů

15. Jak je uvedeno v pokynu 8 bodě 2 písm. e) pokynů CEBS, smlouva o externím zajišťování činnosti by měla poskytovateli externě zajišťované služby ukládat povinnost zachovat důvěrnost informací předávaných finanční institucí. V souladu s pokynem 6 bodem 6 písm. e) pokynů CEBS by instituce měly naplnit ujednání, aby zaručily kontinuitu služeb, které zajišťují poskytovatelé externě zajišťovaných služeb. Na základě pokynu 8 bodu 2 písm. b) a pokynu 9 pokynů CEBS by měly být příslušné potřeby institucí externě zadávajících činnost s ohledem na kvalitu a výkon začleněny do písemných smluv o externím zajišťování činnosti a do dohod o úrovni poskytovaných služeb. Tyto bezpečnostní aspekty by rovněž měly být průběžně sledovány (pokyn 7).
16. Pro účely předchozího odstavce by instituce měla před externím zadáním činnosti a za účelem informování o příslušném rozhodnutí provést alespoň následující úkony:
- a) identifikovat a klasifikovat své činnosti, procesy a související data a systémy, pokud jde o citlivost a požadovanou ochranu;
 - b) provést důkladný výběr činností, procesů a souvisejících dat a systémů, u nichž se zvažuje, že budou externě zadány k řešení za použití cloud computingu, na základě rizika;
 - c) vymezit a zvolit vhodnou úroveň ochrany důvěrnosti dat, kontinuitu externě zajišťovaných činností a integritu a sledovatelnost dat a systémů v souvislosti se zamýšleným externím zadáním cloudových služeb. Instituce by rovněž měly zvážit případná zvláštní opatření zaměřená na přenášená data, data v paměti a uložená data, jako je použití šifrovacích technologií ve spojení s vhodnou klíčovou strukturou řízení.
17. Následně by instituce měly zajistit, že mají uzavřenou písemnou dohodu s poskytovatelem cloudových služeb, ve které se posledně jmenovaný mimo jiné zavazuje k povinnostem stanoveným v odst. 16 písm. c).
18. Instituce by měly průběžně sledovat výkon činností a bezpečnostních opatření v souladu s pokynem 7 pokynů CEBS, a to včetně mimořádných událostí, a v případě potřeby přezkoumat, zda externí zajišťování těchto činností vyhovuje předchozím odstavcům; jakákoli požadovaná nápravná opatření by měly přijmout urychleně.

4.6 Umístění a zpracování dat

19. Jak je uvedeno v pokynu 4 bodě 4 pokynů CEBS, instituce by měly věnovat zvýšenou pozornost při uzavírání a správě dohod o externím zajišťování činnosti uskutečněných mimo Evropský hospodářský prostor (EHP) z důvodu možných rizik v oblasti ochrany dat a rizik týkajících se účinného dohledu prováděného orgánem dohledu.
20. Instituce externě zadávající činnost by měla při externím zadávání činnosti v prostředí cloudu zaujmout přístup založený na posouzení míry rizika, co se týče zvažování umístění dat a zpracování dat. Posouzení by se mělo zaměřit na možné dopady rizik, včetně právních rizik a porušování předpisů, a omezení dohledu týkající se zemí, kde externě zadávané služby jsou nebo by mohly být poskytovány, a kde data jsou nebo by mohla být uložena. Posouzení by mělo zahrnovat úvahy ohledně širší politické a bezpečnostní stability dotyčných jurisdikcí, platné právní předpisy v těchto jurisdikcích (včetně zákonů o ochraně dat) a platná ustanovení týkající se prosazování práva v těchto jurisdikcích, včetně ustanovení insolvenčního práva, která by se použila v případě, že poskytovatel cloudových služeb nesplní požadavky. Instituce externě zadávající činnost by měla zajistit, aby se tato rizika udržovala v přijatelných mezích úměrných významnosti externě zadávané činnosti.

4.7 Řetězové externí zadávání činností

21. Jak je uvedeno v pokynu 10 pokynů CEBS, instituce by měly vzít na vědomí rizika spojená s „řetězovým“ externím zadáváním činností, kdy poskytovatel externě zadávaných služeb zadá část služby jiným poskytovatelům. Instituce externě zadávající činnost by měla souhlasit s řetězovým externím zadáváním činností pouze v případě, že subdodavatel rovněž splňuje existující závazek mezi institucí externě zadávající činnost a externím poskytovatelem zadaných služeb. Instituce externě zadávající činnost by navíc měla podniknout náležité kroky s cílem vypořádat se s rizikem jakékoli slabiny nebo selhání týkající se poskytování subdodavatelských činností, jež by mohly mít významný dopad na schopnost externího poskytovatele zadaných služeb plnit své povinnosti vyplývající z dohody o externím zajišťování činnosti.
22. Dohoda o externím zajišťování činnosti mezi institucí externě zadávající činnost a poskytovatelem cloudových služeb by měla vymezit všechny typy činností, které jsou vyloučeny z potenciálních subdodávek, a měla by uvádět, že poskytovatel cloudových služeb plně odpovídá za tyto služby, jež byly zadány subdodavatelům, a za dohled nad nimi.
23. Dohoda o externím zajišťování činnosti by rovněž měla zahrnovat závazek pro poskytovatele cloudových služeb, že bude instituci externě zadávající činnost informovat o všech plánovaných významných změnách ohledně subdodavatelů nebo subdodavatelských služeb uvedených v původní smlouvě, které by mohly ovlivnit schopnost poskytovatele služeb plnit své povinnosti vyplývající z dohody o externím zajišťování činnosti. Oznamovací lhůta pro tyto změny by měla být dohodnutá před uzavřením smlouvy, aby mohla instituce externě zadávající činnost vypracovat posouzení rizik plynoucích z dopadů navrhovaných změn předtím, než skutečná změna týkající se subdodavatelů či subdodavatelských služeb vstoupí v platnost.

24. V případě, že má poskytovatel cloudových služeb v plánu změny týkající se subdodavatele či subdodavatelských služeb, které by mohly mít nepříznivý dopad na posouzení rizik dohodnutých služeb, instituce externě zadávající činnost by měla mít právo dohodu vypovědět.
25. Instituce externě zadávající činnost by měla průběžně provádět přezkoumání a sledování celkového výkonu služby, bez ohledu na to, zda ji zajišťuje poskytovatel cloudových služeb, nebo jeho subdodavatelé.

4.8 Pohotovostní plány a strategie odstoupení

26. Jak je uvedeno v pokynu 6.1, pokynu 6 bodě 6 písm. e) a pokynu 8 bodě 2 písm. d) pokynů CEBS, instituce externě zadávající činnost by měla naplánovat a provádět opatření s cílem zajistit kontinuitu provozu v případě, že poskytování služeb externím poskytovatelem zadaných služeb pomine nebo se zhorší na nepřijatelnou úroveň. Tato ujednání by měla zahrnovat pohotovostní plánování a jasně definovanou strategii odstoupení. Smlouva o externím zajišťování činnosti by navíc měla zahrnovat ustanovení o ukončení a odstoupení od smlouvy, které umožňuje, aby činnosti zajišťované poskytovatelem externě zadané činnosti byly předány jinému poskytovateli externě zadaných služeb nebo aby byly znovu začleněny do instituce externě zadávající činnost.
27. Instituce externě zadávající činnost by rovněž měla zajistit, aby mohla případně vypovědět ujednání o externě zajišťovaných činnostech bez přílišného narušení poskytování služeb, bez nepříznivých dopadů na dodržování regulační úpravy a bez újmy na kontinuitě a kvalitě poskytování služeb klientům. Za účelem dosažení tohoto cíle by instituce externě zadávající činnost měla:
- a) vyvinout a zavést plány odstoupení, které jsou srozumitelné, zdokumentované a dostatečně otestované, je-li to na místě;
 - b) stanovit alternativní řešení a vyvinout plány přechodu, které umožní ukončit a převádět stávající činnosti a data od poskytovatele cloudových služeb na tato řešení řízeným a dostatečně prověřeným způsobem, a zároveň brát v potaz problémy s umístěním dat a zachování kontinuity provozu během fáze přechodu;
 - c) zajistit, aby dohoda o externím zajišťování činnosti zahrnovala povinnost poskytovatele cloudových služeb dostatečně podporovat instituci externě zadávající činnost v řádném předání činnosti jinému poskytovateli služeb nebo k přímému vedení institucí externě zadávající činnost v případě ukončení dohody o externím zajišťování činnosti.
28. Při vytváření strategií odstoupení by měla instituce externě zadávající činnost zvážit, zda přichází v úvahu:
- a) vyvinout klíčové ukazatele rizika za účelem identifikace nepřijatelné úrovně služby;

- b) provést analýzu dopadů přiměřenou externě zajišťovaným činnostem, aby bylo možné určit, jaké lidské a materiální zdroje by byly potřebné k provedení plánu odstoupení a jak dlouho by to trvalo;
- c) přidělit role a zodpovědnosti v rámci správy plánů odstoupení a přechodových činností;
- d) definovat kritéria úspěšnosti přechodu.

29. Instituce externě zadávající činnost by měla do svého průběžného sledování služeb a dohledu nad službami zajišťovanými poskytovatelem cloudových služeb zahrnout ukazatele, které mohou spustit plán odstoupení.