EBA/REC/2017/03

28/03/2018

Raccomandazioni

in materia di esternalizzazione a fornitori di servizi cloud

1. Conformità e obblighi di comunicazione

Status delle presenti raccomandazioni

1. Il presente documento contiene raccomandazioni emanate in applicazione dell'articolo 16 del regolamento (UE) n. 1093/2010[1]. Conformemente all'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti e gli enti finanziari compiono ogni sforzo per conformarsi alle raccomandazioni.

2. Le raccomandazioni definiscono la posizione dell'ABE in merito alle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione in un particolare settore. Le autorità competenti di cui all'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010 sono tenute a conformarsi a dette raccomandazioni integrandole opportunamente nelle rispettive prassi di vigilanza (per esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando le raccomandazioni sono dirette principalmente agli enti.

Obblighi di comunicazione

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti devono comunicare all'ABE entro il 28.05.2018 se sono conformi o se intendono conformarsi alle raccomandazioni in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna comunicazione da parte delle autorità competenti, queste sono ritenute dall'ABE non conformi. Le comunicazioni dovrebbero essere inviate trasmettendo il modulo disponibile sul sito web dell'ABE all'indirizzo compliance@eba.europa.eu con il riferimento "EBA/REC/2017/03" da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti. Ogni eventuale variazione dello status di conformità deve essere altresì comunicata all'ABE.

4. Le comunicazioni sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3.

[1] Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12).

2. Oggetto, ambito di applicazione e definizioni

Oggetto e ambito di applicazione

1. Le presenti raccomandazioni specificano ulteriormente le condizioni per l'esternalizzazione ai sensi degli orientamenti del CEBS in materia di esternalizzazione, del 14 dicembre 2006, e si applicano all'esternalizzazione a fornitori di servizi cloud da parte degli enti di cui all'articolo 4, paragrafo 1, punto 3), del regolamento (UE) n. 575/2013.

Destinatari

2. Le presenti raccomandazioni si rivolgono alle autorità competenti di cui all'articolo 4, paragrafo 2, punto i), del regolamento (UE) n. 1093/2010 e agli enti di cui all'articolo 4, paragrafo 1, punto 3), del regolamento (UE) n. 575/2013[2].

Definizioni

3. Salvo altrimenti specificato, i termini utilizzati e definiti nella direttiva 2013/36/UE[3] sui requisiti patrimoniali e negli orientamenti del CEBS assumono il medesimo significato nelle presenti raccomandazioni. Inoltre, ai fini delle presenti raccomandazioni si applicano le definizioni riportate di seguito.

Servizi cloud	Servizi forniti tramite cloud computing, ossia un modello che consente l'accesso in rete diffuso, conveniente e su richiesta a un gruppo condiviso di risorse informatiche configurabili (ad esempio reti, server, memorie, applicazioni e servizi), che possono essere forniti e messi a disposizione rapidamente con un minimo di attività gestionale o di interazione con il fornitore del servizio.
Cloud pubblico	Infrastruttura cloud disponibile per l'utilizzo da parte della generalità degli utenti.
Cloud privato	Infrastruttura cloud disponibile per l'utilizzo esclusivo da parte di un solo ente.
Cloud di comunità	Infrastruttura cloud disponibile per l'utilizzo esclusivo da parte di una specifica comunità di enti, compresa una pluralità di enti appartenenti a un unico gruppo.

[2] Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012.

[3] Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE.

Cloud ibrido	Infrastruttura cloud costituita da due o più infrastrutture cloud distinte.

3. Entrata in vigore

Data di applicazione

5. Le presenti raccomandazioni si applicano a partire dal 1º luglio 2018.

4. Raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud

4.1 Valutazione della rilevanza

1. Prima di esternalizzare le proprie attività, gli enti che esternalizzano dovrebbero valutare quali attività dovrebbero essere considerate rilevanti. Gli enti dovrebbero effettuare tale valutazione della rilevanza delle attività sulla base dell'Orientamento 1, lettera f), degli orientamenti del CEBS e, per quanto riguarda l'esternalizzazione in particolare a fornitori di servizi cloud, dovrebbero tenere conto di tutti i seguenti elementi:

    (a) la criticità e il profilo di rischio intrinseco delle attività da esternalizzare, ossia se sono attività critiche per la continuità operativa/sostenibilità economica dell'ente e i suoi obblighi nei confronti dei clienti;

    (b) l'impatto operativo diretto delle indisponibilità e i rischi giuridici e reputazionali connessi;

    (c) il possibile impatto di eventuali interruzioni dell'attività sulle prospettive economiche dell'ente;

    (d) il potenziale impatto di una violazione della riservatezza o di una perdita di integrità dei dati sull'ente e i suoi clienti.

4.2 Obbligo di informare adeguatamente le autorità di vigilanza

2. Gli enti che esternalizzano dovrebbero informare adeguatamente le autorità competenti circa le attività rilevanti che si intendono esternalizzare a fornitori di servizi cloud. A tal fine gli enti dovrebbero agire in conformità del paragrafo 4.3 degli orientamenti del CEBS e, in ogni caso, mettere a disposizione delle autorità competenti le seguenti informazioni:

    (a) il nome del fornitore di servizi cloud e della sua società madre (laddove esistente);
    (b) una descrizione delle attività e dei dati da esternalizzare;
    (c) il paese o i paesi in cui sarà svolto il servizio (inclusa la localizzazione dei dati);
    (d) la data d'inizio del servizio;
    (e) la data dell'ultimo rinnovo del contratto (se applicabile);
    (f) la legge applicabile che disciplina il contratto;
    (g) la data di scadenza del servizio o la data del prossimo rinnovo del contratto (se applicabile).

3. In aggiunta alle informazioni fornite ai sensi del precedente paragrafo, le autorità competenti possono chiedere all'ente che esternalizza ulteriori informazioni sulla sua analisi del rischio concernente le attività rilevanti che intende esternalizzare, ad esempio:

   (a) se il fornitore di servizi cloud dispone di un piano di continuità operativa che sia adeguato ai servizi forniti all'ente che esternalizza;
   (b) se l'ente che esternalizza dispone di una strategia di uscita in caso di recesso di una delle parti o di interruzione della fornitura dei servizi da parte del fornitore di servizi cloud;
   (c) se l'ente che esternalizza mantiene le capacità e le risorse necessarie per monitorare adeguatamente le attività esternalizzate.

4. L'ente che esternalizza dovrebbe tenere un registro aggiornato delle informazioni su tutte le proprie attività rilevanti e non rilevanti esternalizzate a fornitori di servizi cloud al livello di ente e di gruppo. L'ente che esternalizza dovrebbe mettere a disposizione dell'autorità competente, su richiesta, una copia dell'accordo di esternalizzazione e le relative informazioni riportate nel suddetto registro, indipendentemente dal fatto che l'ente abbia considerato rilevante l'attività esternalizzata a un fornitore di servizi cloud.

5. Il registro di cui al precedente paragrafo dovrebbe contenere almeno le seguenti informazioni:

   (a) le informazioni di cui al paragrafo 2, lettere da a) a g), se non ancora fornite;
   (b) il tipo di esternalizzazione (il modello per i servizi cloud e il modello di implementazione del cloud, ossia cloud pubblico/privato/ibrido/di comunità);
   (c) le parti che ricevono i servizi cloud in base all'accordo di esternalizzazione;
   (d) evidenze dell'autorizzazione a esternalizzare concessa dall'organo di gestione o dai suoi comitati delegati, se applicabile;
   (e) i nomi di eventuali subfornitori, se applicabile;
   (f) il paese in cui è registrato il fornitore di servizi cloud/il subfornitore principale;
   (g) se l'esternalizzazione è stata valutata come rilevante (sì/no);
   (h) la data dell'ultima valutazione della rilevanza delle attività esternalizzate effettuata dall'ente;
   (i) se il fornitore di servizi cloud/il subfornitore o i subfornitori supportano operazioni aziendali critiche in termini di tempo (sì/no);
   (j) una valutazione della sostituibilità del fornitore di servizi cloud (se è facile, difficile o impossibile sostituirlo);
   (k) l'indicazione di un fornitore di servizi alternativo, laddove possibile;
   (l) la data dell'ultima valutazione del rischio concernente l'accordo di esternalizzazione o di subappalto.

4.3 Diritti di accesso e di audit

Per gli enti

6. Sulla base dell'Orientamento 8, paragrafo 2, lettera g), degli Orientamenti del CEBS e ai fini dell'esternalizzazione tramite cloud, gli enti che esternalizzano dovrebbero accertarsi altresì di

porre in essere con il fornitore di servizi cloud un accordo scritto in cui il fornitore si impegna a:

(a) concedere all'ente, a un terzo nominato dall'ente a tal fine e al revisore legale dell'ente pieno accesso ai propri locali aziendali (uffici centrali e centri operativi), compresa l'intero insieme di dispositivi, sistemi, reti e dati utilizzati per la fornitura dei servizi esternalizzati (diritto di accesso);

(b) conferire all'ente, a un terzo nominato dall'ente a tal fine e al revisore legale dell'ente diritti illimitati di ispezione e audit in merito ai servizi esternalizzati (diritto di audit).

7. L'esercizio effettivo dei diritti di accesso e audit non dovrebbe essere impedito o limitato da accordi contrattuali. Qualora l'esecuzione degli audit o l'utilizzo di determinate tecniche di audit possano comportare un rischio per l'ambiente di un altro cliente, si dovrebbero concordare modalità alternative in grado di assicurare un livello di garanzia simile a quello richiesto dall'ente.

8. L'ente che esternalizza dovrebbe esercitare i propri diritti di audit e accesso secondo modalità basate sui rischi. Se l'ente che esternalizza non si avvale delle proprie risorse di audit, dovrebbe considerare l'utilizzo di almeno uno dei seguenti strumenti:

(a) audit congiunti organizzati insieme ad altri clienti dello stesso fornitore di servizi cloud ed eseguiti da tali clienti o da un terzo da essi nominato, al fine di utilizzare in modo più efficiente le risorse di audit e ridurre gli oneri organizzativi sia per i clienti sia per il fornitore di servizi cloud;

(b) certificazioni di terza parte e relazioni di terza parte o dell'audit interno messe a disposizione dal fornitore di servizi cloud, a condizione che:

i. l'ente che esternalizza si accerti che l'ambito della certificazione o della relazione di audit comprenda i sistemi (ossia i processi, le applicazioni, l'infrastruttura, i centri dati, ecc.) e i controlli che l'ente stesso ha individuato come essenziali;
ii. l'ente che esternalizza sottoponga a valutazione accurata e continua il contenuto delle certificazioni o delle relazioni di audit, accertandosi, in particolare, che i controlli essenziali siano compresi anche in versioni successive di una relazione di audit, e verifichi che la certificazione o la relazione di audit non siano obsolete;
iii. l'ente che esternalizza sia soddisfatto della competenza del soggetto che esegue la certificazione o l'audit (per quanto riguarda, ad esempio, la avvicendamento delle società che eseguono la certificazione o l'audit, le qualifiche, le competenze, la riesecuzione/verifica delle evidenze nel fascicolo di audit considerato);
iv. le certificazioni siano rilasciate e gli audit siano eseguiti sulla base di norme ampiamente riconosciute, e sia effettuata anche una verifica dell'efficacia operativa dei controlli essenziali in atto;

v. l'ente che esternalizza abbia il diritto contrattuale di chiedere l'ampliamento dell'ambito delle certificazioni o delle relazioni di audit per includervi taluni sistemi e/o controlli rilevanti; il numero e la frequenza di tali richieste di modifica dell'ambito dovrebbero essere ragionevoli e giustificate in un'ottica di gestione dei rischi.

9. In considerazione dell'elevata complessità tecnica delle soluzioni cloud, l'ente che esternalizza dovrebbe verificare che il personale che esegue l'audit – ossia i suoi revisori interni o il gruppo di revisori che opera per suo conto, o i revisori nominati dal fornitore di servizi cloud – o, se del caso, il personale che rivede la certificazione di terza parte o le relazioni di audit del fornitore di servizi abbiano acquisito le giuste capacità e conoscenze e siano pertanto in grado di eseguire audit e/o valutazioni efficaci e pertinenti delle soluzioni cloud.

Per le autorità competenti

10. Sulla base dell'Orientamento 8, paragrafo 2, lettera h), degli Orientamenti del CEBS e ai fini dell'esternalizzazione tramite cloud, gli enti che esternalizzano dovrebbero accertarsi di porre in essere con il fornitore di servizi cloud un accordo scritto in cui il fornitore si impegna a:

(a) concedere all'autorità competente preposta alla vigilianza dell'ente che esternalizza (o a un terzo nominato a tal fine dall'autorità in questione) pieno accesso ai propri locali aziendali (uffici centrali e centri operativi), compresa l'intero insieme di dispositivi, sistemi, reti e dati utilizzati per la fornitura dei servizi all'ente che esternalizza (diritto di accesso);

(b) conferire all'autorità competente preposta alla vigilianza dell'ente che esternalizza (o a un terzo nominato a tal fine dall'autorità in questione) diritti illimitati di ispezione e audit in merito ai servizi esternalizzati (diritto di audit).

11. L'ente che esternalizza dovrebbe accertarsi che gli accordi contrattuali non impediscano alla sua autorità competente di svolgere le proprie funzioni di vigilanza e conseguire i relativi obiettivi.

12. Le informazioni che le autorità competenti ottengono nell'esercizio dei propri diritti di accesso e audit dovrebbero essere soggette agli obblighi in materia di segreto professionale e riservatezza di cui agli articoli 53 e seguenti della direttiva 2013/36/UE (CRD IV). Le autorità competenti dovrebbero astenersi da qualsiasi tipo di accordo contrattuale o dichiarazione tali da impedire loro di rispettare le disposizioni del diritto dell'Unione in materia di riservatezza, segreto professionale e scambio di informazioni.

13. Sulla base delle risultanze dei propri audit, l'autorità competente dovrebbe prendere in esame le eventuali carenze individuate, se necessario imponendo misure direttamente all'ente che esternalizza.

4.4 In particolare per il diritto di accesso

14. L'accordo di cui ai paragrafi 6 e 10 dovrebbe comprendere le seguenti disposizioni:

(a) prima di compiere una visita in loco pianificata, la parte che intende esercitare il diritto di accesso (ente, autorità competente, revisore o terzo che opera per conto dell'ente o dell'autorità competente) dovrebbe notificare con congruo anticipo la visita in loco presso un locale aziendale pertinente, a meno che tale notifica preliminare sia impossibile a causa di una situazione di emergenza o di crisi;

(b) il fornitore di servizi cloud è tenuto a collaborare pienamente con le relative autorità competenti nonché con l'ente e i suoi revisori in riferimento alla visita in loco.

4.5 Sicurezza dei dati e dei sistemi

15. Come stabilito dall'orientamento 8, paragrafo 2, lettera e), degli Orientamenti del CEBS, il contratto di esternalizzazione dovrebbe impegnare il fornitore di servizi di esternalizzazione a tutelare la riservatezza delle informazioni trasmesse dall'istituto finanziario. A norma dell'Orientamento 6, paragrafo 6, lettera e), degli Orientamenti del CEBS, gli enti dovrebbero applicare accordi volti a garantire la continuità dei servizi erogati dai fornitori di servizi di esternalizzazione. Sulla base dell'Orientamento 8, paragrafo 2, lettera b), e dell'Orientamento 9 degli Orientamenti del CEBS, le esigenze di qualità e prestazione degli enti che esternalizzano dovrebbero essere tenute in considerazione nei contratti scritti di esternalizzazione e negli accordi sui livelli del servizio. Inoltre, questi aspetti relativi alla sicurezza dovrebbero essere sottoposti a monitoraggio continuo (Orientamento 7).

16. Ai fini del precedente paragrafo, l'ente dovrebbe eseguire almeno quanto segue, prima di esternalizzare e allo scopo di adottare la decisione adeguata in modo informato:

(a) individuare e classificare le proprie attività, i processi e i relativi dati e sistemi in termini di sensibilità e delle protezioni necessarie;

(b) effettuare un'approfondita selezione basata sui rischi delle attività, dei processi e dei relativi dati e sistemi che sono presi in considerazione ai fini dell'esternalizzazione tramite una soluzione di cloud computing;

(c) definire e stabilire un adeguato livello di protezione della riservatezza dei dati, della continuità delle attività esternalizzate nonché dell'integrità e tracciabilità dei dati e dei sistemi nel contesto della prevista esternalizzazione tramite cloud. Gli enti dovrebbero altresì prendere in considerazione, laddove necessario, misure specifiche per i dati in transito, i dati memorizzati e i dati archiviati, come l'utilizzo di tecniche crittografiche unite a un'adeguata architettura di gestione delle chiavi di crittografia.

17. Successivamente gli enti dovrebbero accertarsi di porre in essere con il fornitore di servizi cloud accordi scritti che contemplino a carico di quest'ultimo, tra l'altro, gli obblighi di cui al paragrafo 16, lettera c).

18. Gli enti dovrebbero sottoporre a monitoraggio continuo l'esecuzione delle attività e delle misure di sicurezza in conformità dell'Orientamento 7 degli Orientamenti del CEBS, compresi gli incidenti, nonché riesaminare, se del caso, la conformità dell'esternalizzazione delle attività ai precedenti paragrafi e adottare prontamente eventuali misure correttive necessarie.

4.6 Localizzazione dei dati e trattamento dei dati

19. Come stabilito nell'Orientamento 4, paragrafo 4, degli orientamenti del CEBS, gli enti dovrebbero prestare particolare attenzione quando concludono e gestiscono accordi di esternalizzazione al di fuori del SEE a causa di possibili rischi per la protezione dei dati e per una vigilanza efficace da parte dell'autorità di vigilanza.

20. Quando esternalizza in un ambiente cloud, l'ente che esternalizza dovrebbe valutare la localizzazione dei dati e il loro trattamento secondo un approccio basato sui rischi. Tale valutazione dovrebbe riguardare gli impatti dei rischi potenziali, compresi i rischi giuridici e le questioni di conformità, nonché eventuali limitazioni alla supervisione connesse ai paesi in cui sono forniti o è probabile che siano forniti i servizi esternalizzati e in cui sono conservati o è probabile che siano conservati i dati. La valutazione dovrebbe comprendere considerazioni sulla stabilità generale della situazione politica e della sicurezza nelle giurisdizioni in questione, nonché sulle leggi (comprese quelle in materia di protezione dei dati) e sulle norme di attuazione vigenti in tali giurisdizioni, incluse le disposizioni del diritto fallimentare applicabili in caso di fallimento del fornitore di servizi cloud. L'ente che esternalizza dovrebbe accertarsi che i suddetti rischi siano mantenuti entro limiti accettabili e commisurati alla rilevanza dell'attività esternalizzata.

4.7 Esternalizzazione «a catena»

21. Come stabilito nell'orientamento 10 degli orientamenti del CEBS, gli enti dovrebbero tenere conto dei rischi connessi all'esternalizzazione «a catena», ossia quando il fornitore di servizi di esternalizzazione subappalta elementi del servizio ad altri fornitori. L'ente che esternalizza dovrebbe acconsentire a un'esternalizzazione «a catena» soltanto se anche il subfornitore adempirà pienamente agli obblighi esistenti tra l'ente stesso e il fornitore di servizi di esternalizzazione. Inoltre, l'ente che esternalizza dovrebbe adottare provvedimenti adeguati per affrontare il rischio di carenze od omissioni nell'esecuzione delle attività subappaltate che siano tali da incidere significativamente sulla capacità del fornitore di servizi di esternalizzazione di ottemperare alle proprie responsabilità quali previste dall'accordo di esternalizzazione.

22. L'accordo di esternalizzazione tra l'ente che esternalizza e il fornitore di servizi cloud dovrebbe specificare i tipi di attività che sono esclusi da un eventuale subappalto, nonché precisare che il fornitore di servizi cloud rimane pienamente responsabile per i servizi che ha subappaltato e per la loro supervisione.

23. L'accordo di esternalizzazione dovrebbe altresì contemplare l'obbligo del fornitore di servizi cloud di informare l'ente che esternalizza di eventuali modifiche sostanziali dei subappaltatori o dei servizi subappaltati citati nell'accordo iniziale che siano state pianificate e possano incidere sulla capacità del fornitore di servizi di ottemperare alle proprie responsabilità quali previste dall'accordo di esternalizzazione. Il periodo di notifica di tali modifiche dovrebbe essere prestabilito contrattualmente, per consentire all'ente che esternalizza di effettuare una

valutazione dei rischi relativa agli effetti delle modifiche proposte dei subappaltatori o dei servizi subappaltati prima che le stesse siano attuate.

24. Qualora un fornitore di servizi cloud intenda apportare a un subfornitore o ai servizi subappaltati modifiche tali da incidere negativamente sulla valutazione dei rischi dei servizi concordati, l'ente che esternalizza dovrebbe avere il diritto di recedere dal contratto.

25. L'ente che esternalizza dovrebbe sottoporre a riesame e monitoraggio continui l'esecuzione del servizio nel suo complesso, indipendentemente dal fatto che esso sia erogato dal fornitore di servizi cloud o dai suoi subfornitori.

4.8 Piani di emergenza e strategie di uscita

26. Come stabilito nell'orientamento 6.1, nell'orientamento 6, paragrafo 6, lettera e), e nell'orientamento 8, paragrafo 2, lettera d), degli Orientamenti del CEBS, l'ente che esternalizza dovrebbe pianificare e attuare provvedimenti atti a garantire la continuità operativa della sua azienda anche in caso di interruzione o inaccettabile deterioramento dell'erogazione dei servizi da parte di un fornitore di servizi esternalizzati. Tali provvedimenti dovrebbero comprendere piani di emergenza e una strategia di uscita chiaramente definita. Inoltre, il contratto di esternalizzazione dovrebbe contemplare una clausola di recesso e gestione dell'uscita che consenta il trasferimento delle attività erogate dal fornitore di servizi di esternalizzazione a un altro fornitore di tali servizi ovvero la reinternalizzazione delle attività nell'ente che esternalizza.

27. L'ente che esternalizza dovrebbe accertarsi anche di avere la possibilità, laddove necessario, di recedere da accordi di esternalizzazione tramite cloud senza che ciò comporti un'indebita interruzione della sua erogazione di servizi o pregiudichi la sua conformità al regime normativo oppure la continuità e qualità della sua erogazione di servizi ai clienti. A tal fine l'ente che esternalizza dovrebbe:

    (a) elaborare e attuare piani di uscita che siano complessivi, documentati e sufficientemente sperimentati, se del caso;

    (b) individuare soluzioni alternative ed elaborare piani di transizione che gli consentano di rimuovere e trasferire attività e dati esistenti dal fornitore di servizi cloud a tali soluzioni in modo controllato e sufficientemente sperimentato, tenendo conto dei problemi connessi alla localizzazione dei dati e del mantenimento della continuità operativa durante la fase di transizione;

    (c) accertarsi che l'accordo di esternalizzazione contempli l'obbligo a carico del fornitore di servizi cloud di sostenere adeguatamente l'ente che esternalizza, al fine di garantire, in caso di recesso dall'accordo di esternalizzazione, un trasferimento ordinato delle attività a un altro fornitore di servizi o alla gestione diretta da parte dell'ente che esternalizza.

28. Nell'elaborazione delle strategie di uscita, l'ente che esternalizza dovrebbe considerare quanto segue:

    (a) definire indicatori chiave di rischio per identificare un livello inaccettabile del servizio;

    (b) effettuare un'analisi d'impatto aziendale commisurata alle attività esternalizzate, al fine di individuare le risorse umane e materiali necessarie per l'eventuale attuazione del piano di uscita e calcolare le relative tempistiche;

    (c) attribuire ruoli e responsabilità per la gestione dei piani di uscita e delle attività di transizione;

    (d) definire i criteri di successo della transizione.

29. L'ente che esternalizza dovrebbe includere nel monitoraggio continuo del servizio e nella supervisione dei servizi erogati dal fornitore di servizi cloud gli indicatori che possono innescare l'avvio del piano di uscita.