EBA/GL/2019/02

25 febbraio 2019

Orientamenti in materia di esternalizzazione

1. Conformità e obblighi di comunicazione

Status giuridico dei presenti orientamenti

1. Il presente documento contiene gli orientamenti emanati 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 agli orientamenti.

2. Gli orientamenti 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 cui si applicano gli orientamenti sono tenute a conformarsi ad essi integrandoli opportunamente nelle rispettive prassi (ad esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti sono diretti principalmente agli enti.

Obblighi di notifica

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti devono notificare all'ABE entro il ([gg.mm.aaaa)] se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna notifica da parte delle autorità competenti, queste sono ritenute dall'ABE non conformi. Le notifiche dovrebbero essere inviate trasmettendo il modulo disponibile sul sito web dell'ABE all'indirizzo compliance@eba.europa.eu con il riferimento «ABE/GL/2019/02» 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 notifiche 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

5. I presenti orientamenti specificano i dispositivi di governance interna, tra cui una rigorosa gestione dei rischi, che gli enti, gli istituti di pagamento e gli istituti di moneta elettronica dovrebbero attuare quando esternalizzano le proprie funzioni, in particolare in caso di esternalizzazione di funzioni essenziali o importanti.

6. Gli orientamenti specificano in che modo i dispositivi di governance di cui al paragrafo precedente dovrebbero essere rivisti e monitorati dalle autorità competenti, nel contesto dell'articolo 97 della direttiva 2013/36/UE[2], processo di revisione e valutazione prudenziale (SREP), dell'articolo 9, paragrafo 3, della direttiva (UE) 2015/2366 [3] e dell'articolo 5, paragrafo 5, della direttiva 2009/110/CE[4], per adempiere al loro dovere di verificare che i soggetti destinatari dei presenti orientamenti rispettino nel continuo le condizioni della loro autorizzazione.

Destinatari

7. I presenti orientamenti sono indirizzati alle autorità competenti di cui all'articolo 4, paragrafo 1, punto 40, del regolamento (UE) n. 575/2013[5], inclusa la Banca centrale europea per quanto riguarda le questioni relative ai compiti ad essa conferiti dal regolamento (UE) n. 1024/2013[6], agli enti di cui all'articolo 4, paragrafo 1, punto 3, del regolamento (UE) n. 575/2013, agli istituti di pagamento di cui all'articolo 4, paragrafo 4, della direttiva (UE) 2015/2366 e agli istituti di moneta elettronica di cui all'articolo 2, paragrafo 1, della direttiva 2009/110/CE. I prestatori di servizi di informazione sui conti che forniscono solo il servizio di cui all'allegato I, punto 8, della direttiva (UE) 2015/2366 non sono inclusi nell'ambito di applicazione dei presenti orientamenti, conformemente all'articolo 33 di detta direttiva.

---

[2] 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.

[3] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

[4] Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE.

[5] 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 (GU L 176 del 27.6.2013, pag. 1).

[6] Regolamento (UE) n. 1024/2013 del Consiglio, del 15 ottobre 2013, che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi.

8. Ai fini dei presenti orientamenti, ogni riferimento agli «istituti di pagamento» include gli «istituti di moneta elettronica» e ogni riferimento ai «servizi di pagamento» include l'«emissione di moneta elettronica».

Ambito di applicazione

9. Fatta salva l'applicazione della direttiva 2014/65/UE [7] e del regolamento delegato (UE) 2017/565[8] della Commissione (che contiene obblighi in materia di esternalizzazione da parte degli enti che forniscono servizi di investimento e svolgono attività di investimento), nonché dei relativi orientamenti emanati dall'Autorità europea degli strumenti finanziari e dei mercati (ESMA) in materia di servizi e attività di investimento, gli enti di cui all'articolo 3, paragrafo 1, punto 3, della direttiva 2013/36/UE dovrebbero conformarsi ai presenti orientamenti su base individuale, subconsolidata e consolidata. Le autorità competenti possono concedere una deroga all'applicazione su base individuale a norma dell'articolo 21 o dell'articolo 109, paragrafo 1, della direttiva 2013/36/UE in combinato disposto con l'articolo 7 del regolamento (UE) n. 575/2013. Gli enti soggetti alla direttiva 2013/36/UE dovrebbero conformarsi a tale direttiva e ai presenti orientamenti su base consolidata e subconsolidata, come disposto dall'articolo 21 e dagli articoli da 108 a 110 della direttiva 2013/36/UE.

10. Fatti salvi l'articolo 8, paragrafo 3, della direttiva (UE) 2015/2366 e l'articolo 5, paragrafo 7, della direttiva 2009/110/CE, gli istituti di pagamento e gli istituti di moneta elettronica dovrebbero conformarsi ai presenti orientamenti su base individuale.

11. Le autorità competenti responsabili della vigilanza degli enti, degli istituti di pagamento e degli istituti di moneta elettronica dovrebbero conformarsi ai presenti orientamenti.

Definizioni

12. Se non diversamente specificato, i termini utilizzati e definiti nella direttiva 2013/36/UE, nel regolamento (UE) n. 575/2013, nella direttiva 2009/110/CE, nella direttiva (UE) 2015/2366 e negli orientamenti dell'ABE sulla governance interna [9] hanno il medesimo significato nei presenti orientamenti. Ai fini dei presenti orientamenti, si applicano inoltre le definizioni riportate di seguito:

Esternalizzazione	Un accordo di qualsiasi forma tra un ente, un istituto di pagamento o un istituto di moneta elettronica e un fornitore di servizi in base al quale quest'ultimo svolge un processo, un

[7] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).

[8] Regolamento delegato (UE) 2017/565 della Commissione, del 25 aprile 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda i requisiti organizzativi e le condizioni di esercizio dell'attività delle imprese di investimento e le definizioni di taluni termini ai fini di detta direttiva (GU L 87 del 31.3.2017, pag. 1).

[9] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

	servizio o un'attività che sarebbe altrimenti svolto/a dall'ente, dall'istituto di pagamento o dall'istituto di moneta elettronica stesso.
Funzione	Qualsiasi processo, servizio o attività.
Funzione essenziale o importante[10]	Qualsiasi funzione considerata essenziale o importante, come specificato nella sezione 4 dei presenti orientamenti.
Subesternalizzazione	Una situazione in cui il fornitore di servizi nell'ambito di un accordo di esternalizzazione trasferisce ulteriormente una funzione esternalizzata a un altro fornitore di servizi[11].
Fornitore di servizi	Un soggetto terzo che svolge in tutto o in parte un processo, un servizio o un'attività esternalizzata nell'ambito di un accordo di esternalizzazione.
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 elettroniche configurabili (ad esempio reti, server, memorie, applicazioni e servizi), che possono essere forniti e messi a disposizione rapidamente con minimo impegno gestionale o 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 o istituto di pagamento.
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.
Cloud ibrido	Infrastruttura cloud costituita da due o più infrastrutture cloud distinte.
Organo di amministrazione	L'organo o gli organi di un ente o di un istituto di pagamento, designati conformemente al diritto nazionale, cui è conferito il potere di stabilire gli indirizzi strategici, gli obiettivi e la direzione generale dell'ente o dell'istituto di pagamento, che supervisionano e monitorano le decisioni della dirigenza e che comprendono le persone che dirigono di fatto l'attività dell'ente o

[10] La locuzione «funzione essenziale o importante» si basa sull'espressione utilizzata nella direttiva 2014/65/UE (MiFID II) e nel regolamento delegato (UE) 2017/565 della Commissione che integra la MiFID II, e viene impiegata solo a fini di esternalizzazione; non è collegata alla definizione di «funzioni essenziali» ai fini del quadro di risanamento e risoluzione delle crisi di cui all'articolo 2, paragrafo 1, punto 35, della direttiva 2014/59/UE (BRRD).

[11] Ai fini della valutazione si applicano le disposizioni di cui alla sezione 3; in altri documenti dell'ABE la subesternalizzazione è indicata anche come «esternalizzazione a catena».

	dell'istituto di pagamento e gli amministratori e le persone responsabili della gestione dell'ente o dell'istituto di pagamento.

3. Attuazione

Data di applicazione

13. Ad eccezione del paragrafo 63, lettera b), i presenti orientamenti si applicano dal 30 settembre 2019 a tutti gli accordi di esternalizzazione conclusi, rivisti o modificati a partire da tale data. Il paragrafo 63, lettera b), si applica a partire dal 31 dicembre 2021.

14. Gli enti e gli istituti di pagamento dovrebbero rivedere e modificare di conseguenza gli accordi di esternalizzazione esistenti al fine di assicurare che siano conformi ai presenti orientamenti.

15. Qualora la revisione degli accordi di esternalizzazione di funzioni essenziali o importanti non sia concluso entro il 31 dicembre 2021, gli enti e gli istituti di pagamento dovrebbero informare di tale fatto la propria autorità competente, segnalando altresì le misure previste per completare la revisione o l'eventuale strategia di uscita.

Disposizioni transitorie

16. Gli enti e gli istituti di pagamento dovrebbero completare la documentazione di tutti gli accordi di esternalizzazione esistenti, ad eccezione degli accordi di esternalizzazione a fornitori di servizi cloud, in linea con i presenti orientamenti dopo la prima data di rinnovo di ciascun accordo di esternalizzazione esistente e comunque entro il 31 dicembre 2021.

Abrogazione

17. Gli orientamenti del comitato delle autorità europee di vigilanza bancaria (CEBS) in materia di esternalizzazione del 14 dicembre 2006 e le raccomandazioni dell'ABE in materia di esternalizzazione a fornitori di servizi cloud[12] sono abrogati con effetto dal 30 settembre 2019.

[12] Raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud (EBA/REC/2017/03).

4. Orientamenti in materia di esternalizzazione

Titolo I. Proporzionalità: applicazione a livello di gruppo e sistemi di tutela istituzionale

1 Proporzionalità

18. Nel rispettare o vigilare sul rispetto dei presenti orientamenti, gli enti, gli istituti di pagamento e le autorità competenti dovrebbero tenere conto del principio di proporzionalità. Tale principio mira ad assicurare che i dispositivi di governance, compresi quelli relativi all'esternalizzazione, siano coerenti con il profilo di rischio individuale, con la natura e il modello di business dell'ente o dell'istituto di pagamento nonché con la portata e la complessità delle loro attività, ai fini dell'effettivo conseguimento degli obiettivi previsti dagli obblighi normativi.

19. Nell'applicare quanto emanato nei presenti orientamenti, gli enti e gli istituti di pagamento dovrebbero tenere in considerazione la complessità delle funzioni esternalizzate, i rischi derivanti dall'accordo di esternalizzazione, l'essenzialità o l'importanza della funzione esternalizzata e l'impatto potenziale dell'esternalizzazione sulla continuità delle loro attività.

20. Nell'applicare il principio di proporzionalità, gli enti, gli istituti di pagamento[13] e le autorità competenti dovrebbero tenere conto dei criteri di cui al titolo I degli orientamenti dell'ABE sulla governance interna, in linea con l'articolo 74, paragrafo 2, della direttiva 2013/36/UE.

2 Esternalizzazione da parte di gruppi e di enti che sono membri di un sistema di tutela istituzionale

21. Conformemente all'articolo 109, paragrafo 2, della direttiva 2013/36/UE, i presenti orientamenti dovrebbero applicarsi anche a livello subconsolidato e consolidato, tenendo conto del perimetro di consolidamento prudenziale[14]. A tal fine, le imprese madri dell'UE o l'impresa madre di uno Stato membro dovrebbero assicurare che i dispositivi, i processi e i meccanismi di governance delle loro filiazioni, inclusi gli istituti di pagamento, siano coerenti,

[13] Gli istituti di pagamento dovrebbero inoltre fare riferimento agli orientamenti dell'ABE sulle informazioni che devono essere fornite per ottenere l'autorizzazione degli istituti di pagamento e degli istituti di moneta elettronica, nonché per la registrazione dei prestatori di servizi di informazione sui conti ai sensi della PSD2, disponibili sul sito web dell'ABE al seguente link: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

[14] Per informazioni sul perimetro di consolidamento si rimanda all'articolo 4, paragrafo 1, punti 47) e 48), del regolamento (UE) n. 575/2013.

ben integrati e adeguati per assicurare l'effettiva applicazione dei presenti orientamenti a tutti i livelli.

22. Gli enti e gli istituti di pagamento, ai sensi del paragrafo 21, e gli enti che, in quanto membri di un sistema di tutela istituzionale, utilizzano dispositivi di governance stabiliti a livello centrale, dovrebbero rispettare quanto segue:

    a. se tali enti o istituti di pagamento hanno concluso accordi di esternalizzazione con fornitori di servizi nell'ambito del gruppo o del sistema di tutela istituzionale[15], l'organo di amministrazione di tali enti o istituti di pagamento mantiene, anche per tali accordi di esternalizzazione, la piena responsabilità del rispetto di tutti gli obblighi normativi e dell'effettiva applicazione dei presenti orientamenti;

    b. se tali enti o istituti di pagamento esternalizzano i compiti operativi delle funzioni di controllo interno a un fornitore di servizi nell'ambito del gruppo o del sistema di tutela istituzionale, per il monitoraggio e l'audit degli accordi di esternalizzazione, gli enti dovrebbero assicurare che, anche per tali accordi di esternalizzazione, i suddetti compiti operativi siano effettivamente eseguiti, anche mediante la ricezione di apposite relazioni.

23. In aggiunta al paragrafo 22, gli enti e gli istituti di pagamento appartenenti a un gruppo per il quale non sono state concesse deroghe a norma dell'articolo 109 della direttiva 2013/36/UE e dell'articolo 7 del regolamento (UE) n. 575/2013, gli enti che sono un organismo centrale o che sono affiliati permanentemente a un organismo centrale per il quale non sono state concesse deroghe a norma dell'articolo 21 della direttiva 2013/36/UE o gli enti che sono membri di un sistema di tutela istituzionale dovrebbero tenere conto di quanto segue:

    a. nel caso in cui il monitoraggio operativo dell'esternalizzazione sia centralizzato (ad esempio nell'ambito di un accordo quadro per il monitoraggio dei contratti di esternalizzazione), gli enti e gli istituti di pagamento dovrebbero assicurare che, almeno per le funzioni essenziali o importanti esternalizzate, siano possibili il monitoraggio indipendente sul fornitore di servizi e l'adeguato controllo da parte di ciascun ente o istituto di pagamento, anche ricevendo, almeno una volta all'anno e su richiesta della funzione centralizzata di monitoraggio, relazioni che includano quanto meno una sintesi della valutazione dei rischi e del monitoraggio sulla performance del fornitore di servizi. Inoltre, gli enti e gli istituti di pagamento dovrebbero ricevere dalla funzione centralizzata di monitoraggio una sintesi delle relazioni di audit relative all'esternalizzazione delle funzioni essenziali o importanti e, su richiesta, la relazione di audit integrale;

    b. gli enti e gli istituti di pagamento dovrebbero assicurare che l'organo di amministrazione sia debitamente informato in merito alle modifiche pianificate

[15] Ai sensi dell'articolo 113, paragrafo 7, del regolamento CRR, per regime di tutela istituzionale si intende un accordo di responsabilità contrattuale o previsto dalla legge che tutela gli enti che aderiscono al sistema stesso e, in particolare, garantisce la loro liquidità e la loro solvibilità per evitare il fallimento ove necessario.

riguardanti i fornitori di servizi soggetti a monitoraggio centralizzato e all'impatto potenziale di tali modifiche sulle funzioni essenziali o importanti fornite, compresa una sintesi dell'analisi dei rischi, tra cui i rischi legali, il rispetto degli obblighi normativi e l'impatto sui livelli di servizio, al fine di poter valutare l'impatto delle modifiche in questione;

c. nel caso in cui gli enti e gli istituti di pagamento nell'ambito del gruppo, gli enti affiliati a un organismo centrale o gli enti che fanno parte di un sistema di tutela istituzionale facciano ricorso a una valutazione preventiva centralizzata dell'esternalizzazione prima di stipulare l'accordo, di cui alla sezione 12, ogni ente e istituto di pagamento dovrebbe ricevere una sintesi della valutazione e assicurare che essa tenga conto della propria struttura e dei rischi specifici nell'ambito del processo decisionale;

d. se il registro di tutti gli accordi di esternalizzazione esistenti, come indicato alla sezione 11, è istituito e tenuto a livello centralizzato nell'ambito di un gruppo o di un sistema di tutela istituzionale, le autorità competenti, tutti gli enti e gli istituti di pagamento dovrebbero poter ottenere il proprio registro individuale senza indebiti ritardi. Tale registro dovrebbe includere tutti gli accordi di esternalizzazione, compresi quelli conclusi con fornitori di servizi all'interno del gruppo o del sistema di tutela istituzionale;

e. se tali enti e istituti di pagamento si avvalgono, per una funzione essenziale o importante, di un piano di uscita (exit plan) stabilito a livello di gruppo, di sistema di tutela istituzionale o dall'organismo centrale, tutti gli enti e gli istituti di pagamento dovrebbero ricevere una sintesi del piano e accertarsi che il piano possa essere effettivamente attuato.

24. Qualora siano state concesse deroghe ai sensi dell'articolo 21 della direttiva 2013/36/UE o dell'articolo 109, paragrafo 1, della direttiva 2013/36/UE in combinato disposto con l'articolo 7 del regolamento (UE) n. 575/2013, quanto emanato dai presenti orientamenti dovrebbe essere applicato dall'impresa madre in uno Stato membro per se stessa e per le sue filiazioni o dall'organismo centrale e dagli enti ad esso affiliati nel loro complesso.

25. Gli enti e gli istituti di pagamento che sono filiazioni di un'impresa madre nell'UE o di un'impresa madre in uno Stato membro a cui non sono state concesse deroghe a norma dell'articolo 21 della direttiva 2013/36/UE o dell'articolo 109, paragrafo 1, della direttiva 2013/36/UE in combinato disposto con l'articolo 7 del regolamento (UE) n. 575/2013 dovrebbero assicurare il rispetto dei presenti orientamenti a livello individuale.

Titolo II. Valutazione degli accordi di esternalizzazione

3 Esternalizzazione

26. Gli enti e gli istituti di pagamento dovrebbero stabilire se un accordo con un soggetto terzo rientra nella definizione di esternalizzazione. Nell'ambito di tale valutazione si dovrebbe considerare se la funzione (o parte di essa) esternalizzata a un fornitore di servizi è eseguita su base ricorrente o continuativa dal fornitore di servizi stesso e se tale funzione (o parte di essa) rientrerebbe in genere nell'ambito delle funzioni che sarebbero o potrebbero realisticamente essere svolte da enti o istituti di pagamento, anche qualora l'ente o l'istituto di pagamento in questione non abbia svolto tale funzione in passato.

27. Se un accordo con un fornitore di servizi ha come oggetto molteplici funzioni, gli enti e gli istituti di pagamento dovrebbero considerare tutti gli aspetti dell'accordo nella loro valutazione, per esempio se il servizio prestato comprende la fornitura di hardware per la conservazione dei dati e il backup dei dati, entrambi aspetti che dovrebbero essere considerati congiuntamente.

28. In linea di principio, gli enti e gli istituti di pagamento non dovrebbero considerare come esternalizzazione:

    a. una funzione che a norma di legge deve essere svolta da un fornitore di servizi, ad esempio la revisione legale dei conti;

    b. i servizi di informazione sui mercati (ad esempio la fornitura di dati da parte di Bloomberg, Moody's, Standard & Poor's, Fitch);

    c. le infrastrutture di rete globali (ad esempio Visa, MasterCard);

    d. gli accordi di compensazione e regolamento tra organismi di compensazione, controparti centrali e istituti di regolamento e loro membri;

    e. le infrastrutture globali di messaggistica finanziaria soggette alla vigilanza delle pertinenti autorità;

    f. i servizi bancari di corrispondenza;

    g. l'acquisizione di servizi che altrimenti non sarebbero intrapresi dall'ente o dall'istituto di pagamento (ad esempio, la consulenza di un architetto, pareri legali e rappresentanza legale di fronte a un tribunale e a organi amministrativi, servizi di pulizia, giardinaggio e manutenzione dei locali dell'ente o dell'istituto di pagamento, servizi medici, manutenzione di automobili aziendali, servizi di ristorazione, servizi di distribuzione automatica, servizi amministrativi, servizi di business travel, servizi postali, servizi di receptionist, segreteria e centralino), beni (ad esempio, tessere di plastica, lettori di carte, forniture per ufficio, personal computer, mobilio) o servizi di pubblica utilità (ad esempio, forniture di elettricità, gas, acqua, telefonia).

4 Funzioni essenziali o importanti

29. Gli enti e gli istituti di pagamento dovrebbero sempre considerare una funzione come essenziale o importante nelle seguenti situazioni[16]:

    a. se un'anomalia nella sua esecuzione o la sua mancata esecuzione comprometterebbero gravemente:

        i. il rispetto nel continuo delle condizioni della loro autorizzazione o degli altri obblighi previsti dalla direttiva 2013/36/UE, dal regolamento (UE) n. 575/2013, dalla direttiva 2014/65/UE, dalla direttiva (UE) 2015/2366 e dalla direttiva 2009/110/CE e dei loro obblighi normativi;

        ii. i risultati finanziari; o

        iii. la solidità o la continuità delle attività bancarie o dei servizi di pagamento svolti;

    b. quando sono esternalizzati compiti operativi delle funzioni di controllo interno, a meno che la valutazione non stabilisca che la mancata esecuzione della funzione esternalizzata o un'esecuzione inadeguata della stessa non avrebbe un impatto negativo sull'efficacia della funzione di controllo interno;

    c. quando intendono esternalizzare le funzioni relative ad attività bancarie o a servizi di pagamento in misura tale da richiedere l'autorizzazione[17] di un'autorità competente, come indicato nella sezione 12.1.

30. Nel caso degli enti, si dovrebbe prestare particolare attenzione alla valutazione dell'essenzialità o dell'importanza delle funzioni se l'esternalizzazione riguarda funzioni relative alle principali linee di business e alle funzioni essenziali quali definite all'articolo 2, paragrafo 1, punto 35), e all'articolo 2, paragrafo 1, punto 36), della direttiva 2014/59/UE[18] e individuate dagli enti sulla base dei criteri di cui agli articoli 6 e 7 del regolamento delegato (UE) 2016/778 della Commissione[19]. Le funzioni che sono necessarie allo svolgimento delle attività delle principali linee di business o delle funzioni essenziali dovrebbero essere considerate funzioni essenziali o

[16] Cfr. anche l'articolo 30 del regolamento delegato (UE) 2017/565 della Commissione, del 25 aprile 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda i requisiti organizzativi e le condizioni di esercizio dell'attività delle imprese di investimento e le definizioni di taluni termini ai fini di detta direttiva.

[17] Cfr. le attività elencate nell'allegato I della direttiva 2013/36/UE.

[18] Direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento e che modifica la direttiva 82/891/CEE del Consiglio, e le direttive 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e i regolamenti (UE) n. 1093/2010 e (UE) n. 648/2012 del Parlamento europeo e del Consiglio (BRRD) (GU L 173 del 12.6.2014, pag. 190).

[19] Regolamento delegato (UE) 2016/778 della Commissione, del 2 febbraio 2016, che integra la direttiva 2014/59/UE del Parlamento europeo e del Consiglio per quanto riguarda le circostanze e le modalità secondo le quali il pagamento dei contributi straordinari ex post può essere parzialmente o integralmente rinviato, e i criteri per l'individuazione delle attività, dei servizi e delle operazioni per quanto concerne le funzioni essenziali e per l'individuazione delle linee di business e dei servizi connessi per quanto attiene alle linee di business principali (GU L 131 del 20.5.2016, pag. 41).

importanti ai fini dei presenti orientamenti, a meno che la valutazione dell'ente non stabilisca che la mancata esecuzione della funzione esternalizzata o un'esecuzione inadeguata della stessa non avrebbe un impatto negativo sulla continuità operativa della linea di business principale o della funzione essenziale.

31. Nel valutare se un accordo di esternalizzazione riguarda una funzione essenziale o importante, gli enti e gli istituti di pagamento dovrebbero considerare, insieme all'esito della valutazione del rischio di cui alla sezione 12.2, almeno i seguenti fattori:

    a. se l'accordo di esternalizzazione è direttamente collegato alla prestazione di attività bancarie o di servizi di pagamento[20] per i quali gli enti o gli istituti di pagamento sono autorizzati;

    b. il potenziale impatto che un'interruzione nell'esecuzione della funzione esternalizzata o la mancata prestazione del servizio ai livelli di servizio concordati su base continuativa da parte del fornitore di servizi potrebbe avere su:

        i. la propria solidità e sostenibilità finanziaria a breve e a lungo termine, compresi, se del caso, gli attivi, il capitale, i costi, le fonti di finanziamento (funding), la liquidità, i profitti e le perdite;

        ii. la propria continuità e solidità operativa;

        iii. i rischi operativi, compresi i rischi di condotta, i rischi legati alle tecnologie dell'informazione e della comunicazione («information and communication technologies, ICT») e i rischi legali;

        iv. i rischi reputazionali;

        v. ove opportuno, la pianificazione del risanamento e della risoluzione delle crisi, la possibilità di risoluzione (resolvability) e la continuità operativa in una situazione di intervento precoce, risanamento o risoluzione;

    c. l'impatto potenziale dell'accordo di esternalizzazione sulla propria capacità di:

        i. individuare, monitorare e gestire tutti i rischi;

        ii. rispettare tutte le previsioni di legge e tutti gli obblighi normativi;

        iii. condurre opportune verifiche di audit sulla funzione esternalizzata;

    d. l'impatto potenziale sui servizi forniti ai propri clienti;

    e. tutti gli accordi di esternalizzazione, l'esposizione complessiva dell'ente o dell'istituto di pagamento nei confronti dello stesso fornitore di servizi e il potenziale impatto cumulativo degli accordi di esternalizzazione nella medesima area operativa;

[20] Cfr. le attività elencate nell'allegato I della direttiva 2013/36/UE.

f. le dimensioni e la complessità di qualsiasi area operativa interessata;

g. la possibilità di ampliare (scale up) l'accordo di esternalizzazione proposto senza sostituire o rivedere l'accordo sottostante;

h. la possibilità di trasferire l'accordo di esternalizzazione proposto a un altro fornitore di servizi, se necessario o auspicabile, sia contrattualmente sia nella pratica, compresi i rischi stimati, gli ostacoli alla continuità operativa, i costi e le tempistiche di esecuzione («sostituibilità»);

i. la capacità di reintegrare la funzione esternalizzata all'interno dell'ente o dell'istituto di pagamento, se necessario o auspicabile;

j. la protezione dei dati e l'impatto potenziale di una violazione dell'obbligo di riservatezza o della mancata disponibilità e integrità dei dati relativi all'ente o all'istituto di pagamento e ai suoi clienti, compreso tra l'altro il rispetto del regolamento (UE) 2016/679[21].

[21] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Titolo III. Quadro di governance

5 Solidi dispositivi di governance e rischio derivante da terzi

32. Nell'ambito del sistema generale dei controlli interni[22], compresi i meccanismi di controllo interno[23], gli enti e gli istituti di pagamento dovrebbero disporre di un sistema olistico di gestione dei rischi a livello dell'intero ente che si estenda a tutte le linee di business e unità interne. Nell'ambito di tale sistema, gli enti e gli istituti di pagamento dovrebbero individuare e gestire tutti i loro rischi, compresi quelli derivanti da accordi con terzi. Il sistema di gestione dei rischi dovrebbe inoltre consentire agli enti e agli istituti di pagamento di prendere decisioni informate sull'assunzione dei rischi e assicurare che le misure di gestione dei rischi siano correttamente attuate, anche per quanto riguarda i rischi informatici[24].

33. Tenendo conto del principio di proporzionalità di cui alla sezione 1, gli enti e gli istituti di pagamento dovrebbero individuare, valutare, monitorare e gestire tutti i rischi derivanti da accordi con terzi ai quali sono o potrebbero essere esposti, indipendentemente dal fatto che tali accordi siano accordi di esternalizzazione. I rischi, in particolare quelli operativi, di tutti gli accordi con terzi, compresi quelli di cui ai paragrafi 26 e 28, dovrebbero essere valutati in linea con la sezione 12.2.

34. Gli enti e gli istituti di pagamento dovrebbero assicurare il rispetto di tutti gli obblighi previsti dal regolamento (UE) 2016/679, anche per quanto riguarda gli accordi con terzi e gli accordi di esternalizzazione.

6 Solidi dispositivi di governance ed esternalizzazione

35. L'esternalizzazione di funzioni non può comportare la delega delle responsabilità dell'organo di amministrazione. Gli enti e gli istituti di pagamento restano pienamente responsabili del rispetto di tutti i loro obblighi normativi, compresa la capacità di vigilare sull'esternalizzazione di funzioni essenziali o importanti.

36. L'organo di amministrazione è in ogni momento pienamente responsabile almeno:

    a. di assicurare che l'ente o l'istituto di pagamento soddisfi costantemente le condizioni che è tenuto a rispettare per mantenere l'autorizzazione, comprese eventuali condizioni imposte dall'autorità competente;

    b. dell'organizzazione interna dell'ente o dell'istituto di pagamento;

---

[22] Gli enti dovrebbero fare riferimento al titolo V degli orientamenti dell'ABE sulla governance interna.

[23] Si rimanda anche all'articolo 11 della direttiva 2015/2366 (PSD2).

[24] Cfr. anche gli orientamenti dell'ABE sulla gestione dei rischi delle TIC e della sicurezza (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) e gli elementi fondamentali del G7 per la gestione dei rischi informatici legati a terzi nel settore finanziario (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

c. di individuare, valutare e gestire i conflitti di interesse;

d. di definire le strategie e le politiche dell'ente o dell'istituto di pagamento (ad esempio, il modello di business, la propensione al rischio, il quadro di gestione dei rischi);

e. di vigilare sulla gestione quotidiana dell'ente o dell'istituto di pagamento, compresa la gestione di tutti i rischi associati all'esternalizzazione;

f. di svolgere il ruolo di supervisione dell'organo di amministrazione nella sua funzione di supervisione strategica, compresi il monitoraggio e il controllo sul processo decisionale dell'amministrazione.

37. L'esternalizzazione non dovrebbe abbassare i requisiti di idoneità applicati ai membri dell'organo di amministrazione di un ente, ai direttori e alle persone responsabili della gestione dell'istituto di pagamento e il personale che riveste ruoli chiave. Gli enti e gli istituti di pagamento dovrebbero avere competenze adeguate e risorse sufficienti e debitamente qualificate per assicurare un'adeguata gestione e supervisione degli accordi di esternalizzazione.

38. Gli enti e gli istituti di pagamento dovrebbero:

a. attribuire in modo chiaro le responsabilità per le attività di documentazione, gestione e controllo degli accordi di esternalizzazione;

b. stanziare risorse sufficienti per assicurare il rispetto di tutte le previsioni di legge e di tutti gli obblighi normativi, compresi i presenti orientamenti e la documentazione e il monitoraggio di tutti gli accordi di esternalizzazione;

c. tenendo conto della sezione 1 dei presenti orientamenti, istituire una funzione di esternalizzazione o designare un membro del personale di grado superiore (senior staff member) che risponda direttamente all'organo di amministrazione (ad esempio, una persona che riveste un ruolo chiave nell'ambito di una funzione di controllo) e che sia responsabile della gestione e supervisione dei rischi connessi agli accordi di esternalizzazione nell'ambito del sistema dei controlli interni dell'ente e della supervisione della documentazione degli accordi di esternalizzazione. Gli enti o gli istituti di pagamento di piccole dimensioni e minore complessità dovrebbero almeno assicurare una chiara divisione dei compiti e delle responsabilità relative alla gestione e al controllo degli accordi di esternalizzazione, e possono assegnare questa funzione in materia di esternalizzazione a un membro dell'organo di amministrazione dell'ente o dell'istituto di pagamento.

39. Gli enti e gli istituti di pagamento dovrebbero mantenere in ogni momento un'operatività sostanziale, evitando di diventare cosiddette «empty shells» o «letter-box entities». A tal fine essi dovrebbero:

a. soddisfare in ogni momento tutte le condizioni della loro autorizzazione[25], tra cui assicurare che l'organo di amministrazione eserciti effettivamente le responsabilità di cui al paragrafo 36 dei presenti orientamenti;

b. mantenere una struttura e un quadro organizzativo chiari e trasparenti, che consentano loro di assicurare il rispetto delle previsioni di legge e degli obblighi normativi;

c. se i compiti operativi delle funzioni di controllo interno sono esternalizzati (ad esempio, in caso di esternalizzazione infragruppo o di esternalizzazione nell'ambito di sistemi di tutela istituzionale), esercitare un controllo adeguato ed essere in grado di gestire i rischi generati dall'esternalizzazione di funzioni essenziali o importanti;

d. disporre di risorse e abilità sufficienti per assicurare l'osservanza delle lettere da a) a c).

40. In caso di esternalizzazione, gli enti e gli istituti di pagamento dovrebbero almeno assicurare di:

a. poter prendere e attuare decisioni in relazione alle proprie attività operative e alle funzioni essenziali o importanti, incluse quelle esternalizzate;

b. mantenere l'ordinato svolgimento delle proprie attività e dei servizi bancari e di pagamento che forniscono;

c. individuare, valutare, gestire e attenuare in maniera adeguata i rischi connessi agli accordi di esternalizzazione esistenti e a quelli futuri, compresi i rischi ICT e quelli legati alla tecnologia finanziaria (fintech);

d. porre in essere disposizioni adeguate in materia di riservatezza dei dati e di altre informazioni;

e. mantenere un adeguato flusso di informazioni con i fornitori di servizi;

f. poter intraprendere in tempi adeguati almeno una delle seguenti azioni con riferimento all'esternalizzazione di funzioni essenziali o importanti:

    i. trasferire la funzione a fornitori di servizi alternativi;

[25] Cfr. anche le norme tecniche di regolamentazione (RTS) di cui all'articolo 8, paragrafo 2, della direttiva 2013/36/UE sulle informazioni da fornire alle autorità competenti nella domanda di autorizzazione degli enti creditizi, e le norme tecniche di attuazione (ITS) di cui all'articolo 8, paragrafo 3, della direttiva 2013/36/UE relative ai moduli standard, modelli e procedure per la presentazione delle informazioni richieste per l'autorizzazione degli enti creditizi (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

Per gli istituti di pagamento, si prega di fare riferimento agli orientamenti dell'ABE sulle informazioni che devono essere fornite per ottenere l'autorizzazione degli istituti di pagamento e degli istituti di moneta elettronica, nonché per la registrazione dei prestatori di servizi di informazione sui conti ai sensi della direttiva (UE) 2015/2366 (PSD2) (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

ii. reintegrare la funzione; oppure

iii. interrompere le attività operative che dipendono dalla funzione.

g. attuare misure adeguate e trattare i dati in conformità del regolamento (UE) 2016/679 nel caso in cui i dati personali siano trattati da fornitori di servizi situati nell'UE e/o in paesi terzi.

7 Politica di esternalizzazione

41. L'organo di amministrazione di un ente o istituto di pagamento[26] che ha in essere o che prevede di concludere accordi di esternalizzazione dovrebbe approvare, rivedere e aggiornare periodicamente una politica di esternalizzazione redatta in forma scritta e assicurarne l'attuazione, ove opportuno, a livello individuale, subconsolidato e consolidato. Per gli enti, la politica di esternalizzazione dovrebbe essere conforme alla sezione 8 degli orientamenti dell'ABE sulla governance interna e, in particolare, dovrebbe tenere conto dei requisiti di cui alla sezione 18 (nuovi prodotti e modifiche significative) di tali orientamenti. Anche gli istituti di pagamento possono armonizzare le proprie politiche con le sezioni 8 e 18 degli orientamenti dell'ABE sulla governance interna.

42. La politica dovrebbe includere le fasi principali del ciclo di vita degli accordi di esternalizzazione e definire i principi, le responsabilità e i processi in relazione all'esternalizzazione. In particolare, la politica dovrebbe riguardare almeno:

a. le responsabilità dell'organo di amministrazione in linea con il paragrafo 36, compreso il suo coinvolgimento, se del caso, nel processo decisionale relativo all'esternalizzazione di funzioni essenziali o importanti;

b. il coinvolgimento delle linee di business, delle funzioni di controllo interno e di altri soggetti con riferimento agli accordi di esternalizzazione;

c. la pianificazione degli accordi di esternalizzazione, che include:

i. la definizione dei requisiti operativi relativi agli accordi di esternalizzazione;

ii. i criteri, compresi quelli di cui alla sezione 4, e i processi per l'individuazione delle funzioni essenziali o importanti;

iii. l'individuazione, la valutazione e la gestione dei rischi conformemente alla sezione 12.2;

[26] Cfr. anche gli orientamenti dell'ABE sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva PSD2, disponibili all'indirizzo: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

iv. i controlli di due diligence sui potenziali fornitori di servizi, comprese le misure di cui alla sezione 12.3;

v. le procedure per l'individuazione, la valutazione, la gestione e l'attenuazione dei potenziali conflitti di interesse, conformemente alla sezione 8;

vi. la pianificazione della continuità operativa in linea con quanto indicato nella sezione 9;

vii. il processo di approvazione di nuovi accordi di esternalizzazione;

d. l'attuazione, il monitoraggio e la gestione degli accordi di esternalizzazione, compresi:

i. la continua valutazione della performance del fornitore di servizi in linea con la sezione 14;

ii. le procedure di notifica e di reazione alle modifiche riguardanti un accordo di esternalizzazione o un fornitore di servizi (ad esempio, la sua posizione finanziaria, la sua struttura organizzativa o proprietaria, la subesternalizzazione);

iii. la revisione e verifiche di audit indipendenti sulla conformità alle alle previsioni di legge, agli obblighi normativi e alle politiche;

iv. i processi di rinnovo;

e. la documentazione e la tenuta dei registri, in considerazione dei requisiti di cui alla sezione 11;

f. le strategie di uscita (exit strategies) e i processi per porre termine all'accordo, compresa la richiesta di un piano di uscita (exit plan) documentato per ogni funzione essenziale o importante da esternalizzare, qualora tale uscita sia considerata praticabile alla luce delle possibili interruzioni del servizio o della cessazione inattesa di un accordo di esternalizzazione.

43. La politica di esternalizzazione dovrebbe distinguere tra:

a. l'esternalizzazione di funzioni essenziali o importanti e altri accordi di esternalizzazione;

b. l'esternalizzazione a fornitori di servizi autorizzati da un'autorità competente e a fornitori di servizi che non lo sono;

c. gli accordi di esternalizzazione infragruppo, gli accordi di esternalizzazione nell'ambito dello stesso sistema di tutela istituzionale (comprese le entità interamente controllate individualmente o collettivamente da enti nell'ambito del sistema di tutela istituzionale) e l'esternalizzazione a entità al di fuori del gruppo;

d. l'esternalizzazione a fornitori di servizi stabiliti in uno Stato membro e a fornitori di servizi stabiliti in paesi terzi.

44. Gli enti e gli istituti di pagamento dovrebbero assicurare che la politica contempli l'individuazione dei seguenti effetti potenziali degli accordi di esternalizzazione di funzioni essenziali o importanti e che questi siano presi in considerazione nel processo decisionale:

a. il proprio profilo di rischio;

b. la capacità di supervisionare il fornitore di servizi e di gestire i rischi;

c. le misure di continuità operativa;

d. lo svolgimento delle loro attività operative.

8 Conflitti di interesse

45. Gli enti, in linea con il titolo IV, sezione 11, degli orientamenti dell'ABE sulla governance interna[27], e gli istituti di pagamento dovrebbero individuare, valutare e gestire i conflitti di interesse inerenti dai propri accordi di esternalizzazione.

46. Se l'esternalizzazione dà adito a conflitti di interesse rilevanti, anche tra entità appartenenti allo stesso gruppo o allo stesso sistema di tutela istituzionale, gli enti e gli istituti di pagamento devono adottare misure adeguate per la gestione di tali conflitti.

47. Se le funzioni sono eseguite da un fornitore di servizi appartenente a un gruppo o che è membro di un sistema di tutela istituzionale o è controllato dall'ente, dall'istituto di pagamento, dal gruppo o dagli enti affiliati a un sistema di tutela istituzionale, le condizioni del servizio esternalizzato, anche quelle di natura finanziaria, dovrebbero essere fissate in base a normali condizioni di mercato. Tuttavia, nell'ambito della tariffazione dei servizi (pricing), possono essere prese in considerazione le sinergie derivanti dalla prestazione degli stessi servizi o di servizi simili a più enti all'interno di uno stesso gruppo o sistema di tutela istituzionale, a condizione che il fornitore di servizi sia in grado di operare sul mercato in maniera redditizia autonomamente; all'interno di un gruppo ciò dovrebbe avvenire indipendentemente dal dissesto di qualsiasi altra entità del gruppo.

9 Piani di continuità operativa

48. Gli enti, in linea con gli obblighi di cui all'articolo 85, paragrafo 2, della direttiva 2013/36/UE e con i requisiti del titolo VI degli orientamenti dell'ABE sulla governance interna[28], e gli istituti di pagamento dovrebbero approntare, mantenere e testare periodicamente adeguati piani di continuità operativa per quanto riguarda le funzioni essenziali o importanti esternalizzate. Gli

[27] Anche gli istituti di pagamento possono armonizzare le proprie politiche con tali orientamenti.

[28] Disponibili all'indirizzo: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

enti e gli istituti di pagamento appartenenti a un gruppo o a un sistema di tutela istituzionale possono avvalersi di piani di continuità operativa stabiliti a livello centralizzato per quanto riguarda le loro funzioni esternalizzate.

49. Nei piani di continuità operativa dovrebbe essere presa in considerazione l'evenienza che la qualità dell'esecuzione della funzione essenziale o importante esternalizzata possa deteriorarsi fino a un livello inaccettabile o che essa venga meno. Tali piani dovrebbero anche tenere conto dell'impatto potenziale dell'insolvenza o di altre inadempienze dei fornitori di servizi e, se opportuno, dei rischi politici nel paese del fornitore di servizi.

10 Funzione di audit interno

50. Le attività della funzione di audit interno[29] dovrebbero comprendere, secondo un approccio basato sul rischio, la revisione indipendente delle attività esternalizzate. Il piano [30] e il programma di audit dovrebbero includere, in particolare, gli accordi di esternalizzazione di funzioni essenziali o importanti.

51. Per quanto riguarda il processo di esternalizzazione, la funzione di audit interno dovrebbe almeno accertare:

    a. che il quadro di riferimento dell'ente o dell'istituto di pagamento per l'esternalizzazione, compresa la politica di esternalizzazione, sia attuato correttamente ed efficacemente e sia in linea con le leggi e la normativa applicabili, con la strategia di rischio e con le decisioni dell'organo di amministrazione;

    b. l'adeguatezza, la qualità e l'efficacia della valutazione dell'essenzialità o dell'importanza delle funzioni;

    c. l'adeguatezza, la qualità e l'efficacia della valutazione dei rischi per gli accordi di esternalizzazione, e che i rischi rimangano in linea con la strategia di rischio dell'ente;

    d. l'adeguato coinvolgimento degli organi aziendali;

    e. l'adeguato monitoraggio e la corretta gestione degli accordi di esternalizzazione.

11 Requisiti in materia di documentazione

52. Nell'ambito del proprio sistema di gestione dei rischi, gli enti e gli istituti di pagamento dovrebbero tenere un registro aggiornato delle informazioni concernenti tutti gli accordi di esternalizzazione a livello dell'ente e, ove applicabile, a livello consolidato e subconsolidato, come indicato nella sezione 2, e dovrebbero documentare adeguatamente tutti gli accordi di esternalizzazione in essere, distinguendo tra esternalizzazione di funzioni essenziali o importanti e altri accordi di esternalizzazione. Nel rispetto del diritto nazionale, gli enti dovrebbero conservare nel registro la documentazione riguardante gli accordi di esternalizzazione cessati e la documentazione di supporto per un periodo di tempo adeguato.

---

[29] Per quanto riguarda le responsabilità della funzione di audit interno, gli enti dovrebbero fare riferimento alla sezione 22 degli orientamenti dell'ABE sulla governance interna (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-) e gli istituti di pagamento dovrebbero fare riferimento all'orientamento 5 degli orientamenti dell'ABE sull'autorizzazione degli istituti di pagamento (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

[30] Cfr. anche gli orientamenti dell'ABE sulle procedure e sulle metodologie comuni per il processo di revisione e valutazione prudenziale (SREP): https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing

53. Tenendo conto del titolo I e delle condizioni di cui al paragrafo 23, lettera d), dei presenti orientamenti, per gli enti e gli istituti di pagamento appartenenti a un gruppo, gli enti permanentemente affiliati a un organismo centrale o gli enti aderenti a uno stesso sistema di tutela istituzionale il registro può essere tenuto a livello centralizzato.

54. Il registro dovrebbe includere almeno le seguenti informazioni per tutti gli accordi di esternalizzazione esistenti:

    a. un numero di riferimento per ciascun accordo di esternalizzazione;

    b. la data di inizio e, se applicabile, la successiva data di rinnovo del contratto, la data di scadenza e/o i termini di preavviso per il fornitore di servizi e per l'ente o l'istituto di pagamento;

    c. una breve descrizione della funzione esternalizzata, compresi i dati esternalizzati, specificando se sono stati trasferiti dati personali (ad esempio, indicando un «sì» o un «no» in un campo separato) o se il loro trattamento è stato esternalizzato a un fornitore di servizi;

    d. una categoria assegnata dall'ente o dall'istituto di pagamento che rifletta la natura della funzione come descritto alla lettera c) [ad esempio, tecnologia dell'informazione (IT), funzione di controllo], che dovrebbe facilitare l'individuazione delle diverse tipologie di accordi;

    e. il nome del fornitore di servizi, il numero di registrazione dell'impresa, l'identificativo della persona giuridica (se disponibile), l'indirizzo della sede legale e altri recapiti rilevanti, nonché il nome dell'impresa madre, se presente;

    f. il paese o i paesi in cui sarà prestato il servizio, incluso il luogo (paese o regione) in cui si trovano i dati;

    g. un campo («sì/no») per indicare se la funzione esternalizzata è considerata essenziale o importante, inclusa, se pertinente, una breve sintesi dei motivi per cui la funzione esternalizzata è considerata essenziale o importante;

    h. in caso di esternalizzazione a un fornitore di servizi cloud, i modelli di servizi cloud e di implementazione del cloud, ossia pubblico/privato/ibrido/di comunità, nonché la natura specifica dei dati da conservare e i luoghi (paesi o regioni) in cui tali dati saranno conservati;

    i. la data dell'ultima valutazione dell'essenzialità o dell'importanza della funzione esternalizzata.

55. Per l'esternalizzazione di funzioni essenziali o importanti, il registro dovrebbe includere almeno le seguenti informazioni aggiuntive:

a. gli enti, gli istituti di pagamento e le altre imprese incluse nel perimetro di consolidamento prudenziale o nel sistema di tutela istituzionale, a seconda del caso, che si avvalgono dell'esternalizzazione;

b. un campo per indicare se il fornitore o il subfornitore di servizi appartiene al gruppo o è membro del sistema di tutela istituzionale o è controllato dagli enti o dagli istituti di pagamento facenti parte del gruppo o ancora è controllato dai membri di un sistema di tutela istituzionale;

c. la data dell'ultima valutazione dei rischi e una breve sintesi dei principali risultati;

d. l'individuo o l'organo decisionale (ad esempio, l'organo di amministrazione) dell'ente o dell'istituto di pagamento che ha approvato l'accordo di esternalizzazione;

e. la normativa che disciplina il contratto di esternalizzazione;

f. le date delle ultime verifiche di audit e di quelle eventualmente in programma;

g. ove opportuno, i nomi di eventuali subcontraenti cui sono affidate parti sostanziali di una funzione essenziale o importante, compresi il paese in cui i subcontraenti sono registrati, il luogo in cui sarà prestato il servizio e, a seconda dei casi, il luogo (paese o regione) in cui i dati saranno conservati;

h. il risultato della valutazione della sostituibilità del fornitore di servizi (facile, difficile o impossibile), della possibilità di reintegrare una funzione essenziale o importante all'interno dell'ente o dell'istituto di pagamento o dell'impatto dell'interruzione della funzione essenziale o importante;

i. l'identificazione di fornitori di servizi alternativi tenuto conto della lettera h);

j. un campo che indichi se la funzione essenziale o importante esternalizzata supporta attività operative che sono critiche in termini di tempo;

k. la stima del costo finanziario annuo (budget cost).

56. Gli enti e gli istituti di pagamento dovrebbero, su richiesta, mettere a disposizione dell'autorità competente il registro completo di tutti gli accordi di esternalizzazione in corso[31] o sezioni specificate di esso, come le informazioni su tutti gli accordi di esternalizzazione che rientrano in una delle categorie di cui al paragrafo 54, lettera d), dei presenti orientamenti (ad esempio tutti gli accordi di esternalizzazione relativi ai servizi informatici). Gli enti e gli istituti di pagamento dovrebbero fornire queste informazioni in un formato elettronico leggibile (ad esempio, un formato di database comunemente utilizzato, valori separati da virgole).

[31] Cfr. anche gli orientamenti dell'ABE sulle procedure e sulle metodologie comuni per il processo di revisione e valutazione prudenziale (SREP), disponibili all'indirizzo: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

57. Gli enti e gli istituti di pagamento dovrebbero, su richiesta, mettere a disposizione dell'autorità competente tutte le informazioni necessarie per consentirle di esercitare un'efficace vigilanza sull'ente o sull'istituto di pagamento, fornendo anche, se necessario, una copia dell'accordo di esternalizzazione.

58. Fatto salvo l'articolo 19, paragrafo 6, della direttiva (UE) 2015/2366, gli enti e gli istituti di pagamento dovrebbero informare adeguatamente, in modo tempestivo, le autorità competenti o avviare con queste un dialogo di vigilanza quando pianificano l'esternalizzazione di funzioni essenziali o importanti e/o quando una funzione esternalizzata è diventata essenziale o importante, comunicando almeno le informazioni di cui al paragrafo 54.

59. Gli enti e gli istituti di pagamento [32] dovrebbero informare tempestivamente le autorità competenti in merito a modifiche rilevanti e/o eventi gravi riguardanti i propri accordi di esternalizzazione che potrebbero avere un impatto significativo sulla continuità delle attività operative dell'ente o dell'istituto di pagamento.

60. Gli enti e gli istituti di pagamento dovrebbero documentare adeguatamente le valutazioni effettuate ai sensi del titolo IV e i risultati del continuo monitoraggio svolto (ad esempio, la performance del fornitore di servizi, il rispetto dei livelli di servizio concordati, altri obblighi contrattuali e normativi, gli aggiornamenti della valutazione dei rischi).

Titolo IV. Processo di esternalizzazione

12 Analisi preventiva dell'esternalizzazione

61. Prima di concludere un accordo di esternalizzazione, gli enti e gli istituti di pagamento dovrebbero:

    a. valutare se l'accordo di esternalizzazione riguarda una funzione essenziale o importante, come indicato al titolo II;

    b. valutare se le condizioni di vigilanza per l'esternalizzazione di cui alla sezione 12.1 siano soddisfatte;

    c. individuare e valutare tutti i rischi dell'accordo di esternalizzazione conformemente alla sezione 12.2;

    d. effettuare un'adeguata due diligence sul potenziale fornitore di servizi conformemente alla sezione 12.3;

    e. individuare e valutare i conflitti di interesse che l'esternalizzazione può generare, in linea con la sezione 8.

[32] Cfr. anche gli orientamenti dell'ABE in materia di segnalazione dei gravi incidenti ai sensi della direttiva PSD2, disponibili all'indirizzo: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

12.1 Condizioni di vigilanza per l'esternalizzazione

62. Gli enti e gli istituti di pagamento dovrebbero assicurare che l'esternalizzazione di funzioni relative alle attività bancarie[33] o ai servizi di pagamento, nella misura in cui la performance di tali funzioni richiede l'autorizzazione o la registrazione da parte di un'autorità competente nello Stato membro in cui essi sono autorizzati, a un fornitore di servizi situato nello stesso o in un altro Stato membro, avvenga solo se è soddisfatta una delle seguenti condizioni:

    a. il fornitore di servizi è registrato o autorizzato da un'autorità competente a svolgere tali attività bancarie o servizi di pagamento; oppure

    b. il fornitore di servizi è altrimenti autorizzato a svolgere tali attività bancarie o servizi di pagamento conformemente alla normativa nazionale applicabile in materia.

63. Gli enti e gli istituti di pagamento dovrebbero assicurare che l'esternalizzazione di funzioni relative alle attività bancarie o ai servizi di pagamento, nella misura in cui lo svolgimento di tali funzioni richiede l'autorizzazione o la registrazione da parte di un'autorità competente nello Stato membro in cui essi sono autorizzati, a un fornitore di servizi situato in un paese terzo, avvenga solo se sono soddisfatte le seguenti condizioni:

    a. il fornitore di servizi è registrato o autorizzato a svolgere tale attività bancaria o servizio di pagamento nel paese terzo ed è soggetto alla vigilanza di un'autorità competente di tale paese terzo (denominata «autorità di vigilanza»);

    b. esiste un apposito accordo di cooperazione, ad esempio sotto forma di memorandum of understanding o di accordo a livello di collegio, tra le autorità competenti responsabili della vigilanza dell'ente e le autorità di vigilanza responsabili della vigilanza del fornitore di servizi;

    c. l'accordo di cooperazione di cui alla lettera b) dovrebbe assicurare che le autorità competenti siano almeno in grado di:

        i. ottenere, su richiesta, le informazioni necessarie allo svolgimento dei propri compiti di vigilanza ai sensi della direttiva 2013/36/UE, del regolamento (UE) n. 575/2013, della direttiva (UE) 2015/2366 e della direttiva 2009/110/CE;

        ii. avere accesso a tutti i dati, documenti, locali o membri del personale del paese terzo che rilevano per l'esercizio dei loro poteri di vigilanza;

        iii. ricevere, nel più breve tempo possibile, informazioni dall'autorità di vigilanza del paese terzo per indagare su presunte violazioni degli obblighi previsti dalla direttiva 2013/36/UE, dal regolamento (UE) n. 575/2013, dalla direttiva (UE) 2015/2366 e dalla direttiva 2009/110/CE;

[33] Cfr. l'articolo 9 della direttiva sui requisiti patrimoniali (CRD) per quanto riguarda il divieto per persone o imprese diverse dagli enti creditizi di accettare depositi o altri fondi rimborsabili dal pubblico.

iv. cooperare con le autorità di vigilanza competenti del paese terzo per l'applicazione della legge in caso di violazione degli obblighi normativi applicabili e del diritto nazionale dello Stato membro. La cooperazione dovrebbe comprendere, a titolo non esaustivo, l'ottenimento, non appena possibile, dalle autorità di vigilanza del paese terzo delle informazioni sulle potenziali violazioni degli obblighi normativi applicabili.

12.2 Valutazione dei rischi degli accordi di esternalizzazione

64. Gli enti e gli istituti di pagamento dovrebbero valutare l'impatto potenziale degli accordi di esternalizzazione in termini di rischio operativo, tenere conto dei risultati di tale valutazione quando decidono se esternalizzare la funzione a un fornitore di servizi e adottare misure adeguate per evitare ulteriori rischi operativi indebiti prima di procedere alla stipula degli accordi di esternalizzazione.

65. La valutazione dovrebbe includere, a seconda dei casi, scenari di possibili eventi di rischio, compresi quelli che comportano un rischio operativo di elevata gravità. Nell'ambito dell'analisi degli scenari, gli enti e gli istituti di pagamento dovrebbero valutare l'impatto potenziale di una mancata o inadeguata prestazione dei servizi, compresi i rischi derivanti da processi, sistemi, persone o eventi esterni. Tenendo conto del principio di proporzionalità di cui alla sezione 1, gli enti e gli istituti di pagamento dovrebbero documentare l'analisi effettuata e i relativi risultati e stimare in che misura l'accordo di esternalizzazione aumenterebbe o ridurrebbe il proprio rischio operativo. In considerazione del titolo I, gli enti e gli istituti di pagamento di minori dimensioni e complessità possono avvalersi di metodi qualitativi di valutazione del rischio, mentre gli enti di maggiori dimensioni o complessità dovrebbero adottare un metodo più sofisticato, che includa, se disponibile, l'uso di dati sulle perdite interne ed esterne nell'analisi degli scenari.

66. Nell'ambito della valutazione dei rischi, gli enti e gli istituti di pagamento dovrebbero anche considerare i benefici e i costi attesi dell'accordo di esternalizzazione proposto, anche valutando gli eventuali rischi che possono essere ridotti o gestiti più efficacemente a fronte dei rischi che possono derivare dall'accordo di esternalizzazione proposto, tenendo conto almeno di quanto segue:

    a. rischi di concentrazione, compresi quelli derivanti:

        i. dall'esternalizzazione a un fornitore di servizi prevalente e non facilmente sostituibile;

        ii. da molteplici accordi di esternalizzazione con lo stesso fornitore di servizi o con fornitori di servizi strettamente connessi;

    b. dai rischi aggregati derivanti dall'esternalizzazione di diverse funzioni al livello dell'ente o dell'istituto di pagamento e, nel caso di gruppi di enti o di sistemi di tutela istituzionale, i rischi aggregati a livello consolidato o del sistema di tutela istituzionale;

c. nel caso di enti significativi, dal rischio di intervento («step-in risk»), ossia il rischio che potrebbe derivare dalla necessità di fornire sostegno finanziario a un fornitore di servizi in difficoltà o di subentrargli nelle sue attività operative;

d. dalle misure attuate dall'ente o dall'istituto di pagamento e dal fornitore di servizi per la gestione e attenuazione dei rischi.

67. Se l'accordo di esternalizzazione prevede la possibilità che il fornitore di servizi subesternalizzi funzioni essenziali o importanti ad altri fornitori di servizi, gli enti e gli istituti di pagamento dovrebbero tener conto di quanto segue:

    a. i rischi associati alla subesternalizzazione, compresi i rischi aggiuntivi che possono sorgere se il subcontraente ha sede in un paese terzo o in un paese diverso da quello del fornitore di servizi;

    b. il rischio che lunghe e complesse catene di subesternalizzazione riducano la capacità degli enti o degli istituti di pagamento di vigilare sulla funzione essenziale o importante esternalizzata e la capacità delle autorità competenti di esercitare una efficace vigilanza su essi.

68. Nell'effettuare la valutazione dei rischi prima dell'esternalizzazione e durante il monitoraggio continuo della performance del fornitore di servizi, gli enti e gli istituti di pagamento dovrebbero almeno:

    a. individuare e classificare le funzioni interessate e i relativi dati e sistemi in base alla loro sensibilità e alle misure di sicurezza richieste;

    b. effettuare un' analisi approfondita, basata sul rischio, delle funzioni e dei relativi dati e sistemi che potrebbero essere o che sono stati esternalizzati e fronteggiare i potenziali rischi, in particolare i rischi operativi, inclusi i rischi legali, ICT, di conformità e reputazionali, nonché eventuali limitazioni alle attività di controllo connesse ai paesi in cui sono prestati o è probabile che siano prestati i servizi esternalizzati e in cui sono conservati o è probabile che siano conservati i dati;

    c. considerare le implicazioni del luogo in cui ha sede il fornitore di servizi (all'interno o all'esterno dell'UE);

    d. esaminare la stabilità politica e la situazione della sicurezza dei paesi in questione, tra cui:

        i. la legislazione vigente, compresa quella sulla protezione dei dati;

        ii. le previsioni vigenti per l'applicazione della legislazione;

iii. le previsioni del diritto fallimentare applicabili in caso di dissesto di un fornitore di servizi e le eventuali restrizioni che potrebbero insorgere in particolare con riferimento al recupero urgente dei dati dell'ente o dell'istituto di pagamento;

e. definire e stabilire un adeguato livello di protezione della riservatezza dei dati, di continuità delle attività esternalizzate nonché di integrità e tracciabilità dei dati e dei sistemi nell'ambito della prevista esternalizzazione. Gli enti e gli istituti di pagamento dovrebbero altresì prendere in considerazione, ove necessario, misure specifiche per i dati in transito, memorizzati e a riposo, come l'utilizzo di tecniche di cifratura in combinazione con un'adeguata architettura di gestione delle chiavi;

f. prendere in considerazione se il fornitore di servizi è una filiazione o un'impresa madre dell'ente, se rientra nel perimetro di consolidamento contabile o se è membro di un sistema di tutela istituzionale oppure controllato da enti affiliati a tale sistema e, in caso affermativo, stabilire in quale misura l'ente controlla il fornitore di servizi o ha la capacità di influenzarne le azioni in linea con la sezione 2.

12.3 Due diligence

69. Prima di concludere un accordo di esternalizzazione e considerando i rischi operativi connessi alla funzione da esternalizzare, gli enti e gli istituti di pagamento dovrebbero assicurare, nel loro processo di selezione e valutazione, l'idoneità del fornitore di servizi.

70. Per quanto riguarda le funzioni essenziali o importanti, gli enti e gli istituti di pagamento dovrebbero far sì che il fornitore di servizi abbia la reputazione commerciale, abilità adeguate e sufficienti, la competenza, la capacità, le risorse (ad esempio umane, informatiche, finanziarie), la struttura organizzativa e, se del caso, le autorizzazioni o le registrazioni regolamentari necessarie per svolgere la funzione essenziale o importante in modo affidabile e professionale al fine di adempiere ai propri obblighi per tutta la durata del contratto proposto.

71. Ulteriori fattori da prendere in considerazione nell'effettuare la due diligence su un potenziale fornitore di servizi comprendono, tra l'altro:

a. il modello di business, la natura, le dimensioni, la complessità, la situazione finanziaria, la struttura proprietaria e di gruppo del fornitore di servizi;

b. le relazioni a lungo termine con i fornitori di servizi già valutati e che prestano servizi per l'ente o l'istituto di pagamento;

c. se il fornitore di servizi è un'impresa madre o una filiazione dell'ente o dell'istituto di pagamento, se rientra nel perimetro di consolidamento contabile dell'ente o se è membro dello stesso sistema di tutela istituzionale al quale appartiene l'ente oppure è controllato da enti che ne fanno parte;

d. se il fornitore di servizi è vigilato dalle autorità competenti.

72. Se l'esternalizzazione comporta il trattamento di dati personali o riservati, gli enti e gli istituti di pagamento dovrebbero accertarsi che il fornitore di servizi adotti misure tecniche e organizzative adeguate per proteggere tali dati.

73. Gli enti e gli istituti di pagamento dovrebbero adottare misure adeguate per assicurare che i fornitori di servizi agiscano in modo coerente con i loro valori e codici di condotta. In particolare, per quanto riguarda i fornitori di servizi situati in paesi terzi e, se del caso, i relativi subcontraenti, gli enti e gli istituti di pagamento dovrebbero accertarsi che il fornitore di servizi agisca in modo etico e socialmente responsabile e rispetti le norme internazionali in materia di diritti umani (ad esempio la Convenzione europea dei diritti dell'uomo), di protezione dell'ambiente e di condizioni di lavoro adeguate, compreso il divieto del lavoro minorile.

13 Fase contrattuale

74. I diritti e gli obblighi dell'ente, dell'istituto di pagamento e del fornitore di servizi dovrebbero essere attribuiti e definiti chiaramente in un accordo scritto.

75. L'accordo di esternalizzazione di funzioni essenziali o importanti dovrebbe perlomeno contenere:

    a. una descrizione chiara della funzione esternalizzata che deve essere svolta;

    b. la data di inizio e, ove applicabile, la data di fine dell'accordo e i termini di preavviso per il fornitore di servizi e per l'ente o l'istituto di pagamento;

    c. la normativa che disciplina il contratto;

    d. gli obblighi finanziari delle parti;

    e. una clausola che indichi se è consentita la subesternalizzazione di una funzione essenziale o importante o di parti sostanziali di essa e, in caso affermativo, le condizioni indicate nella sezione 13.1 alle quali la subesternalizzazione è soggetta;

    f. i luoghi (regioni o paesi) in cui sarà svolta la funzione essenziale o importante e/o in cui saranno conservati e trattati i relativi dati, compreso l'eventuale luogo di conservazione, e le condizioni da soddisfare, compreso l'obbligo di informare l'ente o l'istituto di pagamento se il fornitore di servizi propone di cambiare tali luoghi;

    g. se del caso, le disposizioni riguardanti l'accessibilità, la disponibilità, l'integrità, la riservatezza e la sicurezza dei relativi dati, come specificato nella sezione 13.2;

    h. il diritto dell'ente o dell'istituto di pagamento di effettuare un monitoraggio costante della performance del fornitore di servizi;

    i. i livelli di servizio concordati, che dovrebbero includere precisi obiettivi di performance, quantitativi e qualitativi, per la funzione esternalizzata, in modo da consentire un monitoraggio tempestivo che consenta di adottare, senza indebiti ritardi, le opportune azioni correttive in caso di mancato raggiungimento dei livelli di servizio concordati;

    j. gli obblighi di reportistica del fornitore di servizi all'ente o all'istituto di pagamento, compresa la comunicazione da parte del fornitore di servizi di qualsiasi sviluppo che possa avere un impatto rilevante sulla sua capacità di svolgere efficacemente la funzione essenziale o importante in linea con i livelli di servizio concordati e in osservanza del diritto applicabile e degli obblighi normativi e, se opportuno, gli obblighi del fornitore di servizi di presentare le relazioni della propria funzione di audit interno;

k. una clausola che indichi se il fornitore di servizi debba stipulare un'assicurazione obbligatoria contro determinati rischi e, ove applicabile, il livello di copertura assicurativa richiesto;

l. i requisiti per l'attuazione e la verifica dei piani di emergenza dell'impresa (business contingency plans);

m. disposizioni che assicurino l'accesso ai dati di cui l'ente o l'istituto di pagamento sono titolari in caso di insolvenza, risoluzione o cessazione dell'attività del fornitore di servizi;

n. l'obbligo del fornitore di servizi di cooperare con le autorità competenti e le autorità di risoluzione dell'ente o dell'istituto di pagamento, e con altri soggetti da questi designati;

o. per gli enti, un chiaro riferimento ai poteri dell'autorità nazionale di risoluzione, in particolare agli articoli 68 e 71 della direttiva 2014/59/UE (BRRD), e una descrizione degli «obblighi sostanziali» del contratto ai sensi dell'articolo 68 della medesima direttiva;

p. il diritto illimitato degli enti, degli istituti di pagamento e delle autorità competenti di ispezionare e sottoporre a verifiche di audit il fornitore di servizi per quanto riguarda, in particolare, la funzione essenziale o importante esternalizzata, come specificato nella sezione 13.3;

q. i diritti di cessazione, come indicato nella sezione 13.4.

13.1 Subesternalizzazione di funzioni essenziali o importanti

76. L'accordo di esternalizzazione dovrebbe specificare se è consentita o meno la subesternalizzazione di funzioni essenziali o importanti o di parti sostanziali delle stesse.

77. Se la subesternalizzazione di funzioni essenziali o importanti è consentita, gli enti e gli istituti di pagamento dovrebbero stabilire se la parte della funzione da subesternalizzare è, in quanto tale, essenziale o importante (ovvero se costituisce una parte sostanziale della funzione essenziale o importante) e, in tal caso, annotarlo nel registro.

78. Se la subesternalizzazione di funzioni essenziali o importanti è consentita, l'accordo scritto dovrebbe:

a. specificare le tipologie di attività che sono escluse dalla subesternalizzazione;

b. specificare le condizioni da rispettare in caso di subesternalizzazione;

c. specificare che il fornitore di servizi è tenuto a controllare i servizi che ha subappaltato per assicurare che tutti gli obblighi contrattuali tra il fornitore di servizi e l'ente o l'istituto di pagamento siano rispettati nel continuo;

d. richiedere al fornitore di servizi di ottenere dall'ente o dell'istituto di pagamento una preventiva autorizzazione specifica o generale, in forma scritta, prima di subesternalizzare i dati[34];

e. contemplare l'obbligo del fornitore di servizi di informare l'ente o l'istituto di pagamento di qualsiasi subesternalizzazione pianificata, o di eventuali modifiche sostanziali della stessa, in particolare se ciò potrebbe influire sulla capacità del fornitore di servizi di ottemperare alle proprie responsabilità previste dall'accordo di esternalizzazione. Ciò comprende eventuali modifiche sostanziali dei subcontraenti e del periodo di notifica; in particolare, il termine di notifica dovrebbe consentire all'ente o all'istituto di pagamento che esternalizza di effettuare almeno una valutazione dei rischi associati alle modifiche proposte e di opporsi alle stesse prima dell'effettiva entrata in vigore della subesternalizzazione pianificata o delle relative modifiche sostanziali;

f. assicurare, ove opportuno, che l'ente o l'istituto di pagamento abbia il diritto di opporsi alla subesternalizzazione pianificata o alle relative modifiche sostanziali, o che sia necessaria un'approvazione esplicita;

g. assicurare che l'ente o l'istituto di pagamento abbia il diritto contrattuale di porre termine all'accordo in caso di subesternalizzazione indebita, ad esempio quando la subesternalizzazione aumenta notevolmente i rischi per l'ente o per l'istituto di pagamento o quando il fornitore di servizi subesternalizza senza darne comunicazione all'ente o all'istituto di pagamento.

79. Gli enti e gli istituti di pagamento dovrebbero acconsentire alla subesternalizzazione solo se il subcontraente si impegna a:

    a. rispettare tutte le leggi, gli obblighi normativi e gli obblighi contrattuali applicabili;

    b. riconoscere all'ente, all'istituto di pagamento e all'autorità competente gli stessi diritti contrattuali di accesso e di audit previsti per il fornitore di servizi.

80. Gli enti e gli istituti di pagamento dovrebbero assicurare che il fornitore di servizi supervisioni adeguatamente i subfornitori di servizi, in linea con la politica definita dall'ente o dall'istituto di pagamento. Nelle circostanze in cui la subesternalizzazione proposta possa avere effetti negativi rilevanti sull'accordo di esternalizzazione di una funzione essenziale o importante o comportare un aumento sostanziale del rischio, incluso il caso in cui non siano soddisfatte le condizioni di cui al paragrafo 79, l'ente o l'istituto di pagamento dovrebbe esercitare il proprio diritto di opporsi alla subesternalizzazione, se tale diritto è stato accordato, e/o porre termine al contratto.

[34] Cfr. articolo 28 del regolamento (UE) 2016/679.

13.2 Sicurezza dei dati e dei sistemi

81. Gli enti e gli istituti di pagamento dovrebbero assicurare che i fornitori di servizi, se opportuno, si conformino a standard di sicurezza informatica appropriati.

82. Se del caso (ad esempio nel contesto dell'esternalizzazione di funzioni ICT o tramite cloud), gli enti e gli istituti di pagamento dovrebbero definire i requisiti di sicurezza dei dati e dei sistemi nell'ambito dell'accordo di esternalizzazione e monitorarne costantemente il rispetto.

83. Nel caso dell'esternalizzazione a fornitori di servizi cloud e di altri accordi di esternalizzazione che comportano il trattamento o il trasferimento di dati personali o riservati, gli enti e gli istituti di pagamento dovrebbero adottare un approccio basato sul rischio con riferimento al luogo (paese o regione) dove sono conservati e trattati i dati e alla sicurezza delle informazioni.

84. Fatti salvi gli obblighi di cui al regolamento (UE) 2016/679, gli enti e gli istituti di pagamento, in caso di esternalizzazione (in particolare verso paesi terzi), dovrebbero tenere conto delle differenze tra le previsioni nazionali in materia di protezione dei dati. Gli enti e gli istituti di pagamento dovrebbero assicurare che l'accordo di esternalizzazione preveda l'obbligo per il fornitore di servizi di proteggere le informazioni riservate, personali o altrimenti sensibili e di rispettare tutti gli obblighi normativi relativi alla protezione dei dati che si applicano all'ente o all'istituto di pagamento (ad esempio, la protezione dei dati personali e il rispetto del segreto bancario o analoghi obblighi legali in materia di riservatezza per quanto riguarda le informazioni dei clienti, ove applicabili).

13.3 Diritti di accesso, di informazione e di audit

85. Gli enti e gli istituti di pagamento dovrebbero assicurare, nell'ambito dell'accordo di esternalizzazione redatto in forma scritta, che la funzione di audit interno sia in grado di esaminare la funzione esternalizzata utilizzando un approccio basato sul rischio.

86. Indipendentemente dall'essenzialità o dall'importanza della funzione esternalizzata, gli accordi di esternalizzazione in forma scritta tra enti e fornitori di servizi dovrebbero fare riferimento ai poteri di raccolta delle informazioni e di indagine delle autorità competenti e delle autorità di risoluzione di cui all'articolo 65, paragrafo 3, della direttiva 2013/36/UE e all'articolo 63, paragrafo 1, lettera a), della direttiva 2014/59/UE nei confronti dei fornitori di servizi situati in uno Stato membro, e dovrebbero altresì assicurare tali diritti nei confronti dei fornitori di servizi situati in paesi terzi.

87. Per quanto riguarda l'esternalizzazione di funzioni essenziali o importanti, gli enti e gli istituti di pagamento dovrebbero assicurare, nell'ambito dell'accordo di esternalizzazione redatto in forma scritta, che il fornitore di servizi riconosca loro e alle autorità competenti, comprese le autorità di risoluzione, e a qualsiasi altro soggetto nominato dagli enti o dalle autorità competenti, quanto segue:

a. pieno accesso a tutti i locali aziendali (ad esempio uffici centrali e centri operativi), incluso l'intero insieme di dispositivi, sistemi, reti, informazioni e dati utilizzati per lo svolgimento della funzione esternalizzata, tra cui le relative informazioni finanziarie, il personale e i revisori esterni del fornitore di servizi («diritti di accesso e di informazione»);

b. diritti illimitati di condurre ispezioni e verifiche di audit in relazione all'accordo di esternalizzazione («diritti di audit»), per consentire il monitoraggio dell'accordo di esternalizzazione e assicurare il rispetto di tutti gli obblighi normativi e contrattuali applicabili.

88. Per l'esternalizzazione di funzioni non essenziali o importanti, gli enti e gli istituti di pagamento dovrebbero assicurare i diritti di accesso e di audit di cui al paragrafo 87, lettere a) e b), e alla sezione 13.3, secondo un approccio basato sul rischio, considerando la natura della funzione esternalizzata e i relativi rischi operativi e reputazionali, la sua scalabilità, l'impatto potenziale sullo svolgimento continuo delle sue attività e il periodo contrattuale. Gli enti e gli istituti di pagamento dovrebbero tener conto del fatto che le funzioni potrebbero diventare essenziali o importanti nel tempo.

89. Gli enti e gli istituti di pagamento dovrebbero assicurare che l'accordo di esternalizzazione o qualsiasi altro accordo contrattuale non impedisca o limiti l'effettivo esercizio dei diritti di accesso e di audit da parte loro, delle autorità competenti o di terzi da queste designati per esercitare tali diritti.

90. Gli enti e gli istituti di pagamento dovrebbero esercitare i propri diritti di accesso e di audit, determinare la frequenza delle verifiche di audit e le aree da sottoporre a tali verifiche secondo un approccio basato sul rischio e rispettare gli standard di audit comunemente accettati a livello nazionale e internazionale[35].

91. Fatta salva la loro responsabilità ultima per quanto riguarda gli accordi di esternalizzazione, gli enti e gli istituti di pagamento possono avvalersi di:

a. verifiche congiunte di audit organizzate insieme ad altri clienti dello stesso fornitore di servizi ed eseguite da essi e da tali clienti o da un soggetto terzo da questi 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;

b. certificazioni di soggetti terzi e relazioni di soggetti terzi o dell'audit interno messe a disposizione dal fornitore di servizi.

92. Per l'esternalizzazione di funzioni essenziali o importanti, gli enti e gli istituti di pagamento dovrebbero valutare se le certificazioni e le relazioni di terzi di cui al paragrafo 91, lettera b),

[35] Per gli enti, si prega di fare riferimento alla sezione 22 degli orientamenti dell'ABE sulla governance interna: https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889

sono adeguate e sufficienti per ottemperare ai loro obblighi normativi e non dovrebbero basarsi esclusivamente su tali relazioni nel tempo.

93. Gli enti e gli istituti di pagamento dovrebbero utilizzare il metodo di cui al paragrafo 91, lettera b), solo se:

    a. considerano adeguato il piano di audit per la funzione esternalizzata;

    b. assicurano 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 essenziali individuati dall'ente o dall'istituto di pagamento e la conformità agli obblighi normativi pertinenti;

    c. sottopongono a valutazione accurata il contenuto delle certificazioni o delle relazioni di audit su base continuativa e verificano che le certificazioni o le relazioni non siano obsolete;

    d. assicurano che i controlli e i sistemi essenziali siano compresi anche nelle versioni successive della certificazione o della relazione di audit;

    e. considerano idoneo il soggetto che esegue la certificazione o la verifica di audit (per quanto riguarda, ad esempio, la rotazione delle società di certificazione o di audit, le qualifiche, le competenze, la riesecuzione/verifica relativa alle risultanze contenute nel fascicolo dell'audit);

    f. assicurano che le certificazioni siano rilasciate e che le verifiche di audit siano espletate sulla base di standard professionali ampiamente riconosciuti e che comprendano anche una verifica dell'efficacia operativa dei controlli essenziali in essere;

    g. hanno il diritto contrattuale di chiedere l'ampliamento dell'ambito delle certificazioni o delle relazioni di audit per includervi altri sistemi e controlli; il numero e la frequenza di tali richieste di modifica dell'ambito dovrebbero essere ragionevoli e giustificati in un'ottica di gestione dei rischi; e

    h. mantengono il diritto contrattuale di eseguire a loro discrezione singole verifiche di audit con riferimento all'esternalizzazione di funzioni essenziali o importanti.

94. In linea con gli orientamenti dell'ABE sulla valutazione dei rischi ICT nell'ambito del processo SREP, gli enti dovrebbero, a seconda dei casi, assicurare di essere in grado di effettuare test periodici di penetrazione per valutare l'efficacia delle misure e dei processi di sicurezza ICT interni e a difesa da attacchi esterni[36]. Tenendo conto del titolo I, anche gli istituti di pagamento

[36] Cfr. anche gli orientamenti dell'ABE sulla valutazione dei rischi delle TIC: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

dovrebbero dotarsi di meccanismi di controllo ICT interni , comprese misure di mitigazione dei rischi e di controllo della sicurezza ICT.

95. Prima di effettuare un accesso in loco programmato, gli enti, gli istituti di pagamento, le autorità competenti e i revisori o i terzi che agiscono per conto dell'ente, dell'istituto di pagamento o delle autorità competenti dovrebbero dare un preavviso ragionevole al fornitore di servizi, a meno che ciò non sia possibile a causa di una situazione di emergenza o di crisi o qualora il preavviso conduca a una situazione in cui la verifica di audit non sarebbe più efficace.

96. Nell'espletare verifiche di audit in ambienti multi-cliente, sarebbe opportuno prestare attenzione affinché i rischi per l'ambiente di un altro cliente (ad esempio, l'impatto sui livelli di servizio, sulla disponibilità dei dati, sugli aspetti di riservatezza) siano evitati o mitigati.

97. Se l'accordo di esternalizzazione comporta un elevato livello di complessità tecnica, come ad esempio nel caso di esternalizzazione tramite cloud, l'ente o l'istituto di pagamento dovrebbero verificare che chiunque esegua la verifica di audit – ossia i propri revisori interni, il gruppo congiunto di revisori o i revisori esterni che operano per loro conto – abbia le capacità e le conoscenze adeguate e necessarie per eseguire le verifiche di audit e/o valutazioni efficaci. Lo stesso vale per il personale dell'ente o dell'istituto di pagamento che esamina le certificazioni di terzi o le risultanze delle verifiche di audit effettuate dai fornitori di servizi.

13.4 Diritti di cessazione

98. L'accordo di esternalizzazione dovrebbe consentire espressamente all'ente o all'istituto di pagamento di porre termine al contratto, conformemente al diritto applicabile, anche nelle seguenti situazioni:

    a. se il fornitore delle funzioni esternalizzate viola le disposizioni legislative, regolamentari o contrattuali applicabili;

    b. se vengono individuati impedimenti in grado di alterare l'esecuzione della funzione esternalizzata;

    c. in caso di modifiche rilevanti che incidono sull'accordo di esternalizzazione o sul fornitore di servizi (ad esempio, subesternalizzazione o cambiamento dei subfornitori);

    d. in caso di debolezze nella gestione e nella sicurezza dei dati o delle informazioni riservate, personali o comunque sensibili;

    e. se vengono impartite istruzioni in tal senso dall'autorità competente dell'ente o dell'istituto di pagamento, ad esempio nel caso in cui, a causa dell'accordo di esternalizzazione, l'autorità competente non sia più in grado di esercitare una vigilanza efficace sull'ente o sull'istituto di pagamento.

99. L'accordo di esternalizzazione dovrebbe facilitare il trasferimento della funzione esternalizzata a un altro fornitore di servizi o la sua reintegrazione all'interno dell'ente o dell'istituto di pagamento. A tal fine, l'accordo di esternalizzazione in forma scritta dovrebbe:

    a. indicare chiaramente gli obblighi in capo all'attuale fornitore di servizi, in caso di trasferimento della funzione esternalizzata a un altro fornitore di servizi o della sua reintegrazione all'interno dell'ente o dell'istituto di pagamento, anche per quanto concerne il trattamento dei dati;

    b. fissare un adeguato periodo di transizione durante il quale il fornitore di servizi, dopo la risoluzione dell'accordo di esternalizzazione, continuerebbe a eseguire la funzione esternalizzata per ridurre il rischio di interruzioni;

    c. contemplare l'obbligo del fornitore di servizi di sostenere l'ente o l'istituto di pagamento nel trasferimento ordinato della funzione nel caso in cui si ponga termine all'accordo di esternalizzazione.

14 Controllo delle funzioni esternalizzate

100. Gli enti e gli istituti di pagamento dovrebbero monitorare su base continuativa la performance dei fornitori di servizi con riferimento a tutti gli accordi di esternalizzazione secondo un approccio basato sul rischio e con particolare riguardo all'esternalizzazione di funzioni essenziali o importanti, accertandosi tra l'altro che siano assicurate la disponibilità, l'integrità e la sicurezza dei dati e delle informazioni. Se il rischio, la natura o l'entità di una funzione esternalizzata subisce una modifica rilevante, gli enti e gli istituti di pagamento dovrebbero rivalutare l'essenzialità o l'importanza di tale funzione in linea con la sezione 4.

101. Nel monitorare e gestire gli accordi di esternalizzazione, gli enti e gli istituti di pagamento dovrebbero applicare la debita competenza, cura e diligenza.

102. Gli enti dovrebbero aggiornare regolarmente la propria valutazione dei rischi conformemente alla sezione 12.2 e riferire periodicamente all'organo di amministrazione riguardo ai rischi individuati in relazione all'esternalizzazione di funzioni essenziali o importanti.

103. Gli enti e gli istituti di pagamento dovrebbero monitorare e gestire i propri rischi di concentrazione derivanti da accordi di esternalizzazione, alla luce della sezione 12.2 dei presenti orientamenti.

104. Gli enti e gli istituti di pagamento dovrebbero assicurare, su base continuativa, che gli accordi di esternalizzazione, con particolare riguardo alle funzioni essenziali o importanti esternalizzate, soddisfino adeguati standard in materia di performance e qualità, in linea con le proprie politiche, accertandosi di:

    a. ricevere relazioni adeguate dai fornitori di servizi;

b. valutare la performance dei fornitori di servizi mediante strumenti quali i principali indicatori di prestazione (key performance indicators), indicatori di controllo, le relazioni sull'erogazione dei servizi, l'autocertificazione e le revisioni indipendenti;

c. esaminare tutte le altre informazioni rilevanti ricevute dal fornitore di servizi, comprese le relazioni sulle misure di continuità operativa e sulla relativa attività di verifica (testing).

105. Gli enti dovrebbero adottare misure adeguate qualora individuino carenze nell'esecuzione della funzione esternalizzata. In particolare, gli enti e gli istituti di pagamento dovrebbero svolgere verifiche ogni volta che vi siano segnali che i fornitori di servizi potrebbero non eseguire la funzione essenziale o importante esternalizzata in modo efficace o in conformità delle leggi applicabili e degli obblighi normativi. Se vengono individuate carenze, gli enti e gli istituti di pagamento dovrebbero adottare misure correttive o rimedi adeguati. Tali azioni possono includere, se necessario, la cessazione dell'accordo di esternalizzazione con effetto immediato.

15 Strategie di uscita (exit strategies)

106. Nell'esternalizzare funzioni essenziali o importanti, gli enti e gli istituti di pagamento dovrebbero dotarsi di una strategia di uscita documentata che sia in linea con la propria politica di esternalizzazione e i propri piani di continuità operativa[37], tenendo conto quanto meno della possibilità di:

a. porre termine agli accordi di esternalizzazione;

b. dissesto del fornitore di servizi;

c. deterioramento della qualità della funzione eseguita e interruzioni effettive o potenziali delle attività causate dall'inadeguata o mancata esecuzione della funzione;

d. insorgenza di rischi rilevanti per lo svolgimento adeguato e continuativo della funzione.

107. Gli enti e gli istituti di pagamento dovrebbero assicurarsi di poter porre termine agli accordi di esternalizzazione senza interrompere indebitamente le proprie attività operative, senza limitare il rispetto degli obblighi normativi e senza pregiudicare la continuità e la qualità dei servizi forniti ai propri clienti. A tale scopo, essi dovrebbero:

a. sviluppare e attuare piani di uscita che siano esaustivi, documentati e, ove opportuno, sufficientemente testati (ad esempio, effettuando un'analisi dei potenziali costi,

[37] Gli enti, in linea con gli obblighi di cui all'articolo 85, paragrafo 2, della direttiva 2013/36/UE e del titolo VI degli orientamenti dell'ABE sulla governance interna, e gli istituti di pagamento dovrebbero approntare adeguati piani di continuità operativa per quanto riguarda l'esternalizzazione di funzioni essenziali o importanti.

impatti, risorse e tempistiche del trasferimento di un servizio esternalizzato a un fornitore di servizi alternativo);

b. individuare soluzioni alternative e sviluppare piani di transizione per consentire all'ente o all'istituto di pagamento di rimuovere le funzioni e i dati esternalizzati dal fornitore di servizi e trasferirli a fornitori di servizi alternativi o reintegrarli all'interno dell'ente o dell'istituto di pagamento, ovvero di adottare altre misure che assicurino la continua esecuzione della funzione o dell'attività operativa essenziale o importante in modo controllato e sufficientemente testato, tenendo conto delle difficoltà che possono insorgere a causa dell'ubicazione dei dati e adottando le misure necessarie per assicurare la continuità operativa durante la fase di transizione.

108. Nello sviluppo delle strategie di uscita, gli enti e gli istituti di pagamento dovrebbero:

a. definire gli obiettivi della strategia per il passaggio di consegne;

b. effettuare un'analisi d'impatto sulle attività aziendali che sia commisurata al rischio delle attività, dei processi o dei servizi esternalizzati, al fine di individuare le risorse umane e finanziarie necessarie per l'eventuale attuazione del piano di uscita e calcolare le relative tempistiche;

c. assegnare ruoli, responsabilità e risorse sufficienti per la gestione dei piani di uscita e la transizione delle attività;

d. definire criteri efficaci per la transizione delle funzioni e dei dati esternalizzati;

e. definire gli indicatori da utilizzare per il monitoraggio dell'accordo di esternalizzazione (come descritto nella sezione 14), che includono indicatori basati su soglie il cui superamento rappresenti un livello inaccettabile dei livelli di servizio tale da comportare l'attivazione del piano di uscita.

Titolo V. Orientamenti in materia di esternalizzazione indirizzati alle autorità competenti

109. Nello stabilire metodi adeguati per monitorare il rispetto, da parte degli enti e degli istituti di pagamento, delle condizioni per l'autorizzazione iniziale, le autorità competenti dovrebbero cercare di stabilire se gli accordi di esternalizzazione comportino una modifica rilevante delle condizioni e degli obblighi dell'autorizzazione iniziale degli enti e degli istituti di pagamento.

110. Le autorità competenti dovrebbero accertarsi di poter esercitare un'efficace vigilanza sugli enti e sugli istituti di pagamento, verificando tra l'altro che questi abbiano assicurato, nell'ambito dei rispettivi accordi di esternalizzazione, che i fornitori di servizi siano obbligati a concedere all'autorità competente e all'ente o all'istituto di pagamento in questione diritti di audit e di accesso, conformemente alla sezione 13.3.

111. L'analisi dei rischi di esternalizzazione degli enti dovrebbe essere effettuata almeno nell'ambito del processo SREP o, per quanto riguarda gli istituti di pagamento, nell'ambito di altri processi di vigilanza, comprese le richieste ad hoc, o durante le ispezioni in loco.

112. Oltre alle informazioni annotate nel registro di cui alla sezione 11, le autorità competenti possono chiedere agli enti e agli istituti di pagamento informazioni aggiuntive, in particolare per gli accordi di esternalizzazione di funzioni essenziali o importanti, come ad esempio:

a. l'analisi dettagliata dei rischi;

b. un'indicazione del fatto che il fornitore di servizi dispone o meno di un piano di continuità operativa che sia idoneo ai servizi forniti all'ente o all'istituto di pagamento che esternalizza;

c. la strategia di uscita da utilizzare se l'accordo di esternalizzazione è risolto da una delle parti o se vi è un'interruzione nella fornitura dei servizi;

d. le risorse e le misure adottate per monitorare adeguatamente le attività esternalizzate.

113. Oltre alle informazioni richieste ai sensi della sezione 11, le autorità competenti possono richiedere agli enti e agli istituti di pagamento di fornire informazioni dettagliate su tutti gli accordi di esternalizzazione, anche se la funzione in questione non è considerata essenziale o importante.

114. Le autorità competenti dovrebbero valutare quanto segue sulla base di un approccio basato sul rischio:

a. se gli enti e gli istituti di pagamento monitorano e gestiscono in modo adeguato, in particolare, gli accordi di esternalizzazione di funzioni essenziali o importanti;

b. se gli enti e gli istituti di pagamento dispongono di risorse sufficienti per monitorare e gestire gli accordi di esternalizzazione;

c. se gli enti e gli istituti di pagamento individuano e gestiscono tutti i rischi del caso;

d. se gli enti e gli istituti di pagamento individuano, valutano e gestiscono adeguatamente i conflitti di interesse in relazione agli accordi di esternalizzazione, ad esempio nel caso di esternalizzazione infragruppo o di esternalizzazione nell'ambito dello stesso sistema di tutela istituzionale.

115. Le autorità competenti dovrebbero assicurare che gli enti e gli istituti di pagamento dell'UE/SEE non operino come «empty shells», comprese le situazioni in cui gli enti utilizzano operazioni back-to-back o operazioni infragruppo per trasferire parte del rischio di mercato e del rischio di credito a un'entità non UE/SEE, e dovrebbero assicurare che tali enti e istituti di pagamento siano dotati di adeguati dispositivi di governance e di gestione dei rischi per individuare e gestire i propri rischi.

116. Nell'ambito della loro valutazione, le autorità competenti dovrebbero tenere conto di tutti i rischi, tra cui, in particolare[38]:

a. i rischi operativi[39] derivanti dall'accordo di esternalizzazione;

b. i rischi reputazionali;

c. nel caso di enti significativi, il rischio di intervento («step-in risk») che potrebbe derivare dalla necessità di fornire sostegno finanziario a un fornitore di servizi;

d. i rischi di concentrazione all'interno dell'ente, anche su base consolidata, causati da molteplici accordi di esternalizzazione con uno stesso fornitore di servizi o con fornitori di servizi strettamente connessi, oppure da molteplici accordi di esternalizzazione nell'ambito della stessa area di business;

e. i rischi di concentrazione a livello settoriale, ad esempio quando più enti o istituti di pagamento si avvalgono dello stesso fornitore di servizi o di un ristretto gruppo di fornitori di servizi;

f. la misura in cui l'ente o l'istituto di pagamento che esternalizza controlla il fornitore di servizi o ha la capacità di influenzarne le azioni, la riduzione dei rischi che potrebbe derivare da un livello di controllo più elevato, e se il fornitore di servizi è anch'esso incluso nell'ambito de vigilanza consolidata del gruppo;

g. i conflitti di interesse tra l'ente e il fornitore di servizi.

117. Qualora emergano rischi di concentrazione, le autorità competenti dovrebbero monitorare l'evoluzione di tali rischi e valutarne l'impatto potenziale sia su altri enti e istituti di pagamento sia sulla stabilità del mercato finanziario; ove opportuno, le autorità competenti dovrebbero informare l'autorità di risoluzione delle crisi in merito alle nuove funzioni individuate come potenzialmente essenziali[40] nel corso della valutazione.

118. Qualora siano individuati problemi che inducono a concludere che un ente o un istituto di pagamento non dispone più di solidi dispositivi di governance o non rispetta gli obblighi normativi, le autorità competenti dovrebbero adottare misure appropriate, che possono prevedere la limitazione dell'esternalizzazione di funzioni o la restrizione dell'ambito delle funzioni esternalizzate o l'obbligo di porre termine a uno o più contratti di esternalizzazione. In particolare, in considerazione della necessità dell'ente o dell'istituto di pagamento di operare

[38] Per gli enti soggetti alla direttiva 2013/36/UE, cfr. anche gli orientamenti dell'ABE sul processo SREP: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Cfr. anche gli orientamenti dell'ABE sulla valutazione dei rischi delle TIC: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

[40] Come definite all'articolo 2, paragrafo 1, punto 35) della BRRD.

su base continuativa, la cessazione del contratto potrebbe essere richiesta se l'esercizio della vigilanza e l'applicazione degli obblighi normativi non possono essere garantiti con altri mezzi.

119. Le autorità competenti dovrebbero accertarsi di poter esercitare una vigilanza efficace, in particolare quando gli enti e gli istituti di pagamento esternalizzano funzioni essenziali o importanti che sono svolte al di fuori dell'UE/SEE.