Luglio 2018

Le novità della consultazione EBA in tema di outsourcing

Donato Varani, Partner, Andrea Sudano, Senior Consultant, AC Annunziata & Conso

1. Premessa

Il 22 giungo 2018, l'*European Banking Autority* ("EBA") ha avviato una pubblica consultazione relativa alle linee guida in materia di esternalizzazione (di seguito le "linee guida" o "*guidelines*").

Le linee guida, riesaminando gli orientamenti CEBS in tema di *Outsourcing* pubblicati nel 2006 e diretti solo agli enti creditizi, mirano a stabilire un quadro più armonizzato per gli accordi di esternalizzazione di tutte le istituzioni finanziarie la cui regolamentazione ''compete all'EBA, quali gli enti creditizi e le imprese di investimento, soggetti alla direttiva sui requisiti patrimoniali (*Capital Requirements Directive* – "CRD"), gli istituti di pagamento (IP), soggetti alla direttiva sui servizi di pagamento (*Payment Services Directive* – "PSD2") e gli istituti di moneta elettronica (IMEL) soggetti alla direttiva sulla moneta elettronica (*e-money Directive*).

Le *guidelines* definiscono quali accordi con terze parti sono da considerarsi come esternalizzazione e specificano i criteri per valutare se un'attività, un servizio, un processo o una funzione esternalizzata, o parte di essa, sono da considerarsi importanti o critici, con un conseguente maggiore impatto sul profilo di rischio e sul sistema dei controlli interni dell'istituzione.

Nel seguito dell'esposizione, il riferimento alle "istituzioni" è da ritenersi relativo agli enti creditizi e alle imprese di investimento, agli istituti di pagamento e agli istituti di moneta elettronica.

Il processo di consultazione si concluderà il 24 settembre 2018.

<u>Quadro normativo di riferimento</u>

Occorre evidenziare che l'aggiornamento in commento tiene conto dei principi e delle previsioni contenute nelle direttive 2013/36/UE ("CRD IV"), 2014/65/UE ("MiFID II"), 2009/110/CE (direttiva sulla moneta elettronica), 2015/2366/UE ("PSD2") e 2014/59/UE ("BRRD"), inclusi i rispettivi regolamenti delegati adottati dalla Commissione europea.

Inoltre, le linee guida completano e specificano le "*Guidelines on internal governance under Directive 2013/36/EU"* dell'EBA, inclusive di specifici requisiti sulle politiche di esternalizzazione delle istituzioni e vanno ad integrare gli orientamenti EBA sulle procedure e le metodologie comuni per il processo SREP e le linee guida EBA sulla valutazione del rischio ICT in ambito SREP.

Principio di proporzionalità

Le prescrizioni previste nell'ambito delle linee guida in commento dovranno essere applicate dalle istituzioni, tenendo conto del principio di proporzionalità in relazione alle dimensioni, all'organizzazione interna, alla natura, allo scopo e alla complessità delle loro attività.

Per la declinazione del principio di proporzionalità, vengono richiamati i criteri specificati nel Titolo I delle "*Guidelines on internal governance under Directive 2013/36/EU"* dell'EBA, tra i quali, a titolo non esaustivo, assumono particolare rilievo: i) le dimensioni in termini di totale di bilancio; ii) la dimensione delle operazioni effettuate in ciascuna giurisdizione in cui opera l'istituzione; iii) la forma giuridica; iv) l'eventuale quotazione in un mercato regolamentato; v) l'autorizzazione all'utilizzo di modelli interni per la misurazione di requisiti patrimoniali; vi) il tipo di attività e servizi eseguiti; vii) il modello di business e la struttura organizzativa; vii) la strategia di rischio e la propensione al rischio; viii) la proprietà e la struttura di finanziamento; ix) il tipo di clientela servita; x) i sistemi informatici esistenti e la presenza di eventuali esternalizzazioni.

Considerazioni preliminari

È finalmente stata unificata la definizione di "funzione critica o importante". In particolare, tale definizione si basa sulla formulazione prevista ai sensi della direttiva MiFID II e del regolamento delegato (UE) 2017/565 della Commissione e viene utilizzata allo scopo di identificare servizi, attività o funzioni oggetto di accordi di esternalizzazione, includendo, inoltre, anche gli eventuali compiti e/o attività operative eseguite dalle funzioni di controllo.

A tale riguardo, il citato regolamento delegato (UE) 2017/565 fornisce ulteriori dettagli, specificando all'art. 30 che una funzione operativa è considerata critica o importante se un difetto o un fallimento nello svolgimento delle sue prestazioni comprometterebbe in modo sostanziale la conformità di un'impresa di investimento alle condizioni e agli obblighi derivanti dalla sua autorizzazione, dei suoi ulteriori obblighi ai sensi della direttiva MiFID II, o della sua solidità economico-patrimoniale o la continuità nei servizi prestati.

2. Requisiti di *governance* degli accordi di *outsourcing*

Anche nel documento in esame, viene ribadito il principio fondamentale di governance per l'esternalizzazione di funzioni o attività. Infatti, l'organo di gestione[1] dell'istituzione finanziaria rimane responsabile in qualsiasi momento dello svolgimento e dell'adeguato assetto organizzativo della funzione/attività esternalizzata e deve garantire che siano disponibili risorse sufficienti per il monitoraggio dei rischi e la gestione degli accordi di esternalizzazione, con particolare riguardo alle funzioni ritenute critiche o importanti.

Nell'ambito degli accordi di *outsourcing*, sono previsti requisiti di governance, che le istituzioni devono rispettare e anche declinare dettagliatamente nell'ambito della policy di outsourcing, garantendo almeno:

- ✓ che gli accordi di esternalizzazione non pregiudichino la capacità dell'organo di gestione di svolgere i propri compiti;
- ✓ la possibilità di prendere e attuare decisioni anche in relazione alle attività e alle funzioni aziendali esternalizzate;
- ✓ il mantenimento della regolarità del *business* e delle attività e dei servizi bancari e di pagamento forniti;
- ✓ che le funzioni di controllo interno dispongano delle competenze, dell'autorità e delle risorse necessarie per esercitare le proprie funzioni anche con riferimento al libero accesso alla documentazione dell'istituzione per lo svolgimento dei propri compiti;
- ✓ che i rischi connessi agli accordi di outsourcing, sia attuali che prospettici, siano adeguatamente identificati, valutati, gestiti e mitigati, anche con riferimento ai rischi ICT;
- ✓ che vengano mantenuti adeguati flussi informativi con i fornitori di servizi;
- ✓ il mantenimento, in relazione all'esternalizzazione di funzioni critiche o importanti, della capacità, in condizioni di continuità aziendale ed entro un termine appropriato:
  - Di trasferire la funzione critica o importante ad un fornitore di servizi alternativo;
  - Di reinternalizzare la funzione critica o importante nell'ambito dell'istituzione;

[1] In questa sede, per gli enti creditizi e le imprese di investimento, si fa riferimento "*all'organo o gli organi di un ente (...) cui è conferito il potere di stabilire gli indirizzi strategici, gli obiettivi e la direzione generale dell'ente, che supervisionano e monitorano le decisioni della dirigenza"*, ai sensi dell'art. 3, punto 7, della Direttiva CRD IV. Relativamente alle istituzioni di pagamento, per "organo di gestione" si fa riferimento ai dirigenti o persone responsabili della gestione di detta istituzione.

- ✓ l'attuazione - nel caso in cui dati sensibili, compresi i dati personali, siano elaborati o trasferiti a fornitori di servizi situati sia nell'Unione europea e/o in paesi terzi – di misure di controllo appropriate ed una archiviazione dei dati in conformità al Regolamento 2016/679 (GDPR).

Si assiste, con riferimento agli ultimi due requisiti, ad una migliore declinazione del principio di proporzionalità in caso di di sostituzione dell'outsourcer, ammettendo esplicitamente la possibilità della sua sostituzione, da declinarsi nella policy e all'esplicito richiamo ai principi del GDPR in caso di elaborazione o trasferimento di dati personali all'outsourcer con le relative problematiche legate alla declinazione dell'outsourcer come responsabile o titolare autonomo ai fini privacy.

3. Policy di outsourcing

Un ruolo di particolare rilievo nell'ambito delle *guidelines* è assunto dalla regolamentazione interna di cui le istituzioni dovrebbero dotarsi al fine di risultare in ogni momento *compliant* alla normativa di riferimento. A tal riguardo, è responsabilità dell'organo di gestione approvare e mantenere una policy di outsourcing scritta e garantirne l'attuazione, ove applicabile, su base consolidata e individuale.

La policy di outsourcing, nel descrivere le fasi principali del processo decisionale per l'esternalizzazione di funzioni aziendali, definisce i principi, le responsabilità e le funzioni coinvolte[2].

Il contenuto informativo della policy di esternalizzazione appare più ampio e profondo rispetto alle vigenti disposizioni per gli enti creditizi. La policy in parola, infatti, dovrebbe almeno stabilire.

a) le responsabilità dell'organo di gestione, delle linee di business, delle funzioni di controllo interno e degli altri soggetti rispetto agli accordi di esternalizzazione.

A tal fine, occorre da parte delle istituzioni: i) assegnare chiaramente le responsabilità per il controllo degli accordi di esternalizzazione; ii) disporre di un numero adeguato di risorse per garantire la conformità ai requisiti normativi di riferimento; iii) designare una funzione o un soggetto interno dotati di adeguati requisiti di professionalità, direttamente responsabili del controllo delle funzioni esternalizzate.

b) i criteri adottati e i processi definiti per l'identificazione di funzioni critiche o importanti.

[2] Per gli enti creditizi e le imprese di investimento, la policy di outsourcing dovrebbe tenere conto delle "*Guidelines on internal governance under Directive 2013/36/EU"* dell'EBA, con particolare riguardo alla Sezione 4 e ai requisiti di cui alla sezione 18 "nuovi prodotti e modifiche significative".

Le linee guida prevedono criteri finalizzati a garantire una maggiore armonizzazione nella valutazione della criticità o importanza delle funzioni. Al riguardo, queste chiariscono che una funzione è da considerarsi critica o importante, quando a causa della sua inadeguata esecuzione si verificherebbe i) il concreto mancato rispetto delle condizioni minime dell'autorizzazione ottenuta, ii) si comprometterebbero i risultati economico patrimoniali dell'istituzione, iii) non si garantirebbe la solidità o la continuità dei servizi bancari e di pagamento. Inoltre, sono considerate funzioni critiche o importanti anche: 1) l'outsourcing di funzioni di controllo o attività operative inerenti le funzioni di controllo o 2) l'outsourcing di servizi bancari o di pagamento che richiedono l'autorizzazione di un'Autorità competente. Importante evidenziare come anche l'esternalizzazione di attività operative inerenti funzioni di controllo siano da considerare funzione critica o importante.

c) i criteri adottati per la scelta e i controlli di *due diligence* effettuati sui potenziali fornitori di servizi.

Non costituisce una novità di rilievo rispetto alle vigenti disposizioni la necessità che il fornitore di servizi disponga delle competenze, capacità, risorse, struttura organizzativa e, se del caso, delle autorizzazioni necessarie per esercitare in maniera professionale e affidabile la funzione esternalizzata per tutta la durata del contratto. Nel caso in cui l'esternalizzazione comporti il trasferimento, l'elaborazione e la memorizzazione di dati personali o confidenziali, il fornitore di servizi deve garantire adeguate misure tecniche e organizzative e assicurare il rispetto delle norme in materia di *privacy*, conformemente al regolamento (UE) 2016/679 (GDPR).

d) l'identificazione, la valutazione e la gestione dei rischi connessi con l'esternalizzazione.

Sebbene le linee guida si concentrino sugli accordi di outsourcing, le istituzioni devono considerare che ricevere servizi da soggetti terzi crea rischi, anche quando tali accordi non sono da considerarsi esternalizzazioni o quando gli accordi di outsourcing riguardano funzioni non considerate critiche o importanti.

Al fine di identificare, gestire e monitorare tutti i potenziali rischi connessi ad un accordo di esternalizzazione, le linee guida evidenziano l'importanza della programmazione di opportune valutazioni, con particolare riguardo ai rischi operativi e di reputazione. Tenuto adeguatamente conto del principio di proporzionalità, le valutazioni dovrebbe includere opportune analisi di scenario e valutazioni del potenziale impatto di servizi non adeguati o non eseguiti, compresi i rischi connessi a processi, sistemi, persone o eventi esterni.

Inoltre, le linee guida richiedono alle istituzioni e agli istituti di pagamento di bilanciare i vantaggi attesi con i potenziali rischi dall'accordo proposto, tenendo conto almeno: i) dei rischi di concentrazione, derivanti da più accordi di esternalizzazione con lo stesso fornitore di sevizi; ii) dei rischi aggregati derivanti dall'esternalizzazione di un gran

numero di funzioni dell'istituzione; iii) delle misure attuate sia dall'istituzione che dal fornitore di servizi per la gestione e mitigazione dei rischi.

Merita menzione, infine, anche il caso in cui l'accordo di outsourcing includa la possibilità che il fornitore di servizi sub-esternalizzi funzioni critiche o importanti ad altri fornitori di servizi. In tal caso, le linee guida pongono l'attenzione sui rischi aggiuntivi che potrebbero insorgere se il sub-outsourcer si trovi in un paese terzo e i rischi connessi a catene lunghe e complesse di sub-outsourcer tali da ridurre la capacità delle istituzioni e delle istituzioni di pagamento di sovrintendere il processo di esternalizzazione e di controllarlo efficacemente.

e) le procedure per l'identificazione, la valutazione, la gestione e la mitigazione di potenziali conflitti di interesse del fornitore di servizi.

Nel caso in cui l'esternalizzazione crei conflitti di interesse rilevanti, anche tra entità all'interno dello stesso gruppo, le istituzioni, nell'adozione di misure appropriate per la gestione di tali conflitti, dovrebbero garantire che la decisione sull'accordo di esternalizzazione e la sua supervisione siano eseguite con un sufficiente livello di obiettività, ai fini di una gestione appropriata degli interessi in conflitto. Appare di primaria importanza, dunque, garantire che le condizioni per il servizio esternalizzato, comprese le condizioni finanziarie, siano stabilite a valori di mercato. Misure da considerarsi appropriate, come evidenziato nel Titolo IV, Sezione 11 delle "*Guidelines on internal governance under Directive 2013/36/EU"* dell'EBA, sono:

- l'implementazione di una policy sui conflitti di interesse, per l'identificazione, la valutazione, la gestione e la mitigazione dei conflitti di interesse, al fine di evitare che i conflitti possano arrecare pregiudizio agli interessi dei clienti;
- la previsione di un'adeguata politica di separazione delle competenze (ad es. affidando la supervisione delle responsabilità delle attività in conflitto a persone diverse);
- stabilire barriere informative (ad es. attraverso la separazione fisica di alcune linee o unità aziendali);
- stabilire procedure adeguate per le transazioni con parti correlate.

f) il piano di continuità operativa in caso di non corretto svolgimento delle funzioni esternalizzate da parte del fornitore di servizi.

Ampiamente nota per le istituzioni è la necessità di implementare un solido *business continuity plan*, al fine di garantire la continuità operativa e di limitare le perdite in caso di grave interruzione dell'attività. Lo scopo del piano di continuità operativa, come previsto nel Titolo VI delle "*Guidelines on internal governance under Directive 2013/36/EU"* dell'EBA, è quello di ridurre le conseguenze operative, finanziarie, legali, reputazionali, derivanti da una calamità o da un'interruzione prolungata dei sistemi

operativi. A tal riguardo, un valido piano di continuità operativa non può prescindere da un'attenta analisi dell'esposizione a gravi problemi aziendali e da una valutazione del loro potenziale impatto, attraverso l'utilizzo di dati e scenari interni e/o esterni, in grado di coinvolgere tutte le linee di business e le unità interne.

Una delle principali novità delle linee guida oggetto di trattazione, nel caso di grave interruzione dell'attività esternalizzata, si riferisce al coinvolgimento diretto del fornitore di servizi stesso nella pianificazione della continuità operativa, stabilendo, attuando e mantenendo piani di emergenza per il ripristino dell'emergenza (*disaster recovery*) e pianificando e attuando accordi per garantire il mantenimento della continuità della propria attività, nel caso in cui la qualità dell'esternalizzazione della funzione critica o importante si deteriori ad un livello ritenuto inaccettabile.

g) il coinvolgimento dell'organo di gestione nel processo decisionale sull'esternalizzazione.

A tal riguardo, le linee guida richiedono all'organo di gestione la responsabilità almeno:

- di garantire che l'istituzione o l'istituto di pagamento soddisfi su base continuativa le condizioni alle quali deve conformarsi per rimanere autorizzato, comprese le eventuali condizioni imposte dall'autorità competente;
- dell'organizzazione interna dell'istituzione;
- dell'identificazione, valutazione e gestione dei conflitti di interesse;
- dell'impostazione delle strategie e delle politiche dell'istituzione (ad esempio il modello aziendale, la propensione al rischio);
- della gestione quotidiana, compresa la gestione dei rischi connessi all'esternalizzazione.

h) le valutazioni continuative delle prestazioni del fornitore di servizi.

Le istituzioni, oltre a effettuare valutazioni relative ai costi, hanno anche la necessità di sorvegliare e controllare i processi, i servizi e i rischi connessi all'outsourcing. In merito, le linee guida richiedono un aggiornamento periodico delle valutazioni del rischio effettuate (Cfr. punto e) e di riferire periodicamente all'organo di gestione su eventuali rischi identificati in relazione all'esternalizzazione di funzioni critiche o importanti.

Al fine di garantire prestazioni adeguate e standard di qualità in linea con le politiche definite internamente, occorrerebbe almeno: i) assicurare la ricezione di relazioni appropriate dai fornitori di servizi; ii) valutare le prestazioni dei fornitori di servizi utilizzando strumenti quali KPI (*key performance indicator*), rapporti di esecuzione del servizio, autocertificazione; iii) analizzare tutte le altre informazioni pertinenti e le relazioni sulla continuità operativa ricevute dal fornitore di servizi.

i) le procedure di notifica e di modifica del contratto di outsourcing o di un fornitore di servizi.

j) la documentazione e la tenuta dei registri.

Le linee guida prescrivono un ampio set documentale e di informazioni che le istituzioni dovrebbero detenere, sia con riguardo all'accordo di esternalizzazione che al fornitore di servizi.

La novità più rilevante è relativa alla tenuta e alla codifica di un registro di tutti gli accordi di esternalizzazione, anche a livello di gruppo, e di documentare e registrare tutti gli accordi di esternalizzazione, distinguendo tra l'esternalizzazione di funzioni importanti e altri accordi di esternalizzazione.

Si precisa che per le istituzioni facenti parte di un gruppo, il registro può essere tenuto presso la capogruppo, a condizione che la sezione del registro relativo a ciascuna singola istituzione possa essere estratto in modo tempestivo.

Appare opportuno entrare più nel dettaglio della documentazione minima che le istituzioni dovrebbero conservare, inclusiva almeno delle informazioni di seguito sintetizzate, per tutti gli accordi di esternalizzazione esistenti.

- con riguardo all'accordo di esternalizzazione:

  – un numero di riferimento per ciascun accordo di esternalizzazione;

  – una breve descrizione della funzione esternalizzata;

  – per la funzione critica o importante, i motivi per cui è considerata tale e la data dell'ultima valutazione pertinente;

  – se i dati personali e confidenziali sono elaborati, trasferiti o detenuti dal fornitore di servizi (ai sensi del Regolamento (UE) 2016/679).

- per quanto riguarda il fornitore di servizi e, se presente, i fornitori di sub-servizi:

  – il nome e l'indirizzo registrato;

  – il paese di registrazione, o se non disponibile, il numero di registrazione aziendale;

  – la società madre, ove applicabile;

  – il paese o i paesi in cui la funzione esternalizzata sarà eseguita dal fornitore di servizi o dal fornitore di sub-servizi;

  – il paese o i paesi in cui i dati saranno o saranno potenzialmente archiviati.

- inoltre, il registro dovrebbe includere almeno le seguenti informazioni in merito all'esternalizzazione di funzioni critiche o importanti:

  - la data dell'ultimo *risk assessment* effettuato e una breve sintesi dei principali risultati emersi;
  - l'organo decisionale che ha approvato l'accordo di esternalizzazione;
  - la legge applicabile al contratto di esternalizzazione;
  - la data di inizio e, se applicabile, la data di scadenza e /o i periodi di preavviso;
  - la data dell'ultimo e del successivo *audit* programmato, ove applicabile;
  - una valutazione della sostituibilità del fornitore di servizi e/o della possibilità di reinternalizzare la funzione critica o importante;
  - l'identificazione dei fornitori di servizi alternativi, in linea con il punto precedente;
  - se l'esternalizzazione della funzione critica o importante è considerata tale nel tempo;
  - il costo stimato nel budget.

k) le strategie di uscita.

Ulteriore novità delle linee guida, è la necessità da parte delle istituzioni di definire con chiarezza una strategia di uscita per tutte le esternalizzazioni di funzioni critiche o importanti, in conformità alla policy di esternalizzazione, nei casi di fallimento del fornitore di servizi e di deterioramento materiale del servizio fornito. L'obiettivo è quello di garantire l'uscita da ogni accordo di outsourcing, senza una interruzione delle attività o violazione del *framework* normativo di riferimento. A tal fine, le *guidelines* richiedono almeno:

- di sviluppare e attuare piani di uscita (*exit plans*) completi, documentati e sufficientemente testati (ad esempio effettuando un'analisi dei costi potenziali, degli impatti previsti, delle implicazioni in termini di risorse e tempistiche per il trasferimento di un servizio esternalizzato ad un nuovo fornitore);
- di identificare soluzioni alternative e sviluppare piani di transizione (*transition plans*) per rimuovere e trasferire funzioni e dati esternalizzati da un fornitore di servizi ad un fornitore alternativo, o decidere di re-internalizzare la funzione.

4. Il ruolo della Funzione di *Internal Audit*

Le attività della funzione di *Internal Audit* dovrebbero comprendere, seguendo un approccio basato sul rischio, la revisione indipendente delle attività esternalizzate. A tal

riguardo, il piano di audit dovrebbe includere la valutazione degli accordi di esternalizzazione di funzioni critiche o importanti, tra cui specifiche analisi dell'adeguatezza delle misure di protezione dei dati, dei controlli delle misure di gestione del rischio e di continuità operativa attuate dal fornitore di servizi.

Nell'ambito dell'esternalizzazione, le linee guida demandano alla Funzione di *Internal Audit* le responsabilità di accertare:

- che la regolamentazione interna (policy e procedure) in tema esternalizzazione sia correttamente ed efficacemente attuata e rispettata e risulti in linea con le leggi e i regolamenti applicabili, con la propensione al rischio definita dall'ente e con le decisioni assunte dell'organo di gestione;
- l'adeguatezza, la qualità e la correttezza della valutazione effettuata sulla criticità o importanza della funzione/attività esternalizzata;
- l'adeguatezza, la qualità e l'efficacia della valutazione del rischio effettuate in merito agli accordi di esternalizzazione e che i rischi rimangano entro la propensione al rischio (*risk appetite*) definita;
- che la propensione al rischio, la gestione del rischio e le procedure di controllo del fornitore di servizi siano in linea con la strategia dell'istituzione;
- l'appropriato coinvolgimento degli organi aziendali;
- l'appropriato monitoraggio e gestione degli accordi di esternalizzazione.

5. Attuazione delle Linee Guida EBA

Le *guidelines*, saranno applicate a partire dal 30 giugno 2019. Gli accordi di esternalizzazione in essere oggetto di rinnovo o di revisione entro la data indicata, dovrebbero essere redatti conformemente a queste *guideline.* Per gli accordi che scadono o vengono rinnovati dopo il 30 giugno 2019, occorrerà apportare le necessarie modifiche per renderli conformi alle *guideline* e comunque, tutti gli accordi dovranno essere adeguati entro il 31 dicembre 2020.'' *L*e autorità di vigilanza dei singoli paesi dell'UE a cui si applicano le linee guida sono invitati ad integrarle nelle rispettive disposizioni di vigilanza.