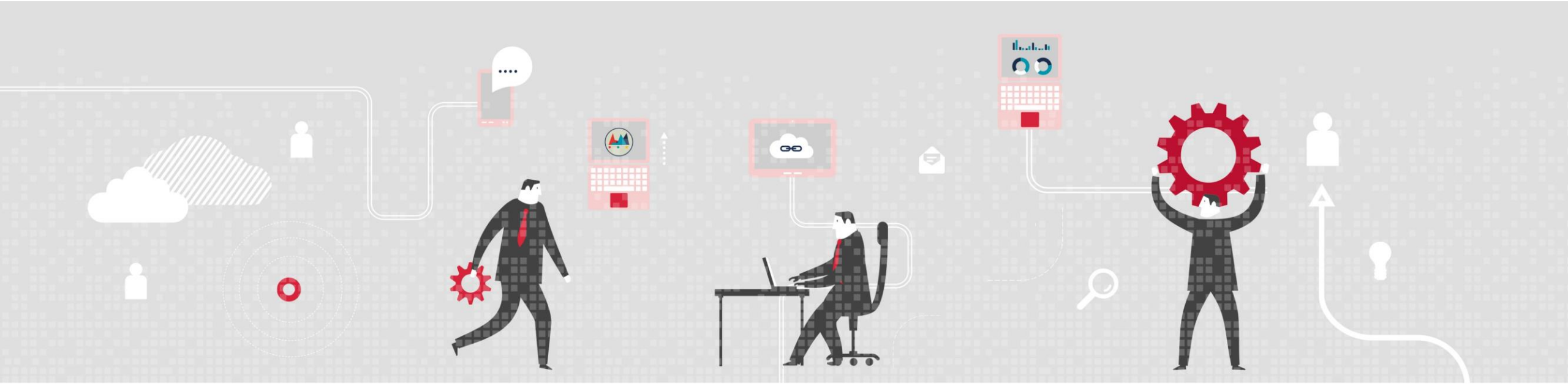
P4I

PARTNERS4INNOVATION

CLOUD SECURITY SUMMIT 2018



Le linee guida EBA (European Banking Authority) relative all'utilizzo dei servizi cloud in ambito bancario e spunti di riflessione per gli altri settori di mercato

Avv. Annamaria Italiano

Le linee guida EBA in materia di ricorso ai servizi cloud

Cinque ambiti fondamentali:

- Diritti di **accesso** e di **audit**
- **Sicurezza** de dati e dei sistemi
- **Localizzazione** dei dati
- Catene di **subfornitura**
- **Piani di emergenza** ed **exit strategies**

Diritti di accesso e di audit

Gli enti che esternalizzano dovrebbero accertarsi altresì di porre in essere con il fornitore di servizi cloud un accordo scritto in cui il fornitore si impegna a:

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

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

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

Diritti di accesso e di audit

Se l'ente che esternalizza non si avvale delle proprie risorse di audit, dovrebbe considerare l'utilizzo di almeno **uno dei seguenti strumenti**:

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

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

- **i.** **l'ambito della certificazione** o della **relazione di audit comprenda i sistemi** (ossia i processi, le applicazioni, l'infrastruttura, i centri dati, ecc.) e **i controlli che l'ente che esternalizza ha individuato come essenziali**;
- ii. Il contenuto delle certificazioni e delle relazioni di audit sia sottoposto a valutazione accurata e continua (occorre accertarsi che certificazioni e audit non siano obsoleti);
- **iii.** **l'ente che esternalizza sia soddisfatto della competenza del soggetto che esegue la certificazione o l'audit;**
- iv. le certificazioni siano rilasciate e gli audit siano eseguiti sulla base di **norme ampiamente riconosciute;**
- v. l'ente che esternalizza abbia il **diritto contrattuale di chiedere l'ampliamento dell'ambito delle certificazioni o delle relazioni di audit per includervi taluni sistemi e/o controlli rilevanti**; il numero e la frequenza di tali richieste di modifica dell'ambito dovrebbero essere ragionevoli e giustificate in un'ottica di gestione dei rischi.

La sicurezza dei dati e dei sistemi

Prima di esternalizzare e allo scopo di adottare la decisione in modo informato, l'ente dovrebbe:

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

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

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

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

Localizzazione dei dati

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

Esternalizzazione «a catena» 1/2

- L’ente che esternalizza dovrebbe acconsentire a un’esternalizzazione «a catena» soltanto se anche **il subfornitore adempirà pienamente agli obblighi esistenti tra l’ente stesso e il fornitore di servizi di esternalizzazione**.
- L’accordo di esternalizzazione tra l’ente che esternalizza e il fornitore di servizi cloud dovrebbe specificare i tipi di attività che sono esclusi da un eventuale subappalto, nonché precisare che **il fornitore di servizi cloud rimane pienamente responsabile** per i servizi che ha subappaltato e per la loro supervisione.
- L’accordo di esternalizzazione dovrebbe altresì contemplare **l’obbligo del fornitore di servizi cloud di informare l’ente che esternalizza di eventuali modifiche sostanziali dei subappaltatori** o dei servizi subappaltati citati nell’accordo iniziale.
- Il **periodo di notifica** di tali modifiche dovrebbe essere **prestabilito contrattualmente**, per consentire all’ente che esternalizza di effettuare una **valutazione dei rischi** relativa agli effetti delle modifiche proposte dei subappaltatori o dei servizi subappaltati prima che le stesse siano attuate.

Esternalizzazione «a catena» 2/2

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

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

Piani di emergenza ed exit strategy

L'ente che esternalizza dovrebbe pianificare e attuare provvedimenti atti a garantire la continuità operativa della sua azienda anche in caso di interruzione o inaccettabile deterioramento dell'erogazione dei servizi da parte di un fornitore di servizi esternalizzati.

- **Piani di emergenza** e una **strategia di uscita** chiaramente definita
- Previsione di obblighi contrattualmente vincolanti di **collaborazione e assistenza al trasferimento** del servizio
- Previsione di **facoltà di recesso** in favore dell'ente che esternalizza
- Inclusione nel monitoraggio continuo e nella supervisione dei servizi erogati degli **indicatori che possono innescare l'avvio del piano di uscita.**

P4I

PARTNERS4.INNOVATION

GRAZIE!

annamaria.italiano@p4i.it

CLOUD SECURITY SUMMIT 2018

DIGITAL 360 | Group