# ENTERPRISE RISK MANAGEMENT E CLOUD COMPUTING

**di Lorenzo Neri**
Senior Lecturer in Financial and Management Accounting - University of Greenwich - Dottore Commercialista, Revisore Legale dei Conti
**e Antonella Russo**
Università Parthenope

***In risposta al crescente numero di organizzazioni che utilizzano il cloud computing come una valida alternativa per soddisfare le loro esigenze tecnologiche, il Committee of Sponsoring Organizations of the Treadway Commission (COSO) nel 2012 ha pubblicato un paper intitolato "Enterprise Risk Management for Cloud Computing". Il documento fornisce indicazioni sui principi identificati dal COSO per valutare e mitigare i rischi derivanti da cloud computing. Il COSO nel giugno 2016 ha pubblicato il documento "Enterprise Risk Management - Aligning Risk with Strategy and Performance". La nuova versione è stata progettata per migliorare l'approccio aziendale ai rischi nuovi ed esistenti soprattutto in contesti in continua evoluzione per contribuire a creare, conservare, sostenere e realizzare il valore, in altre parole a migliorarne le performance. Una delle recenti evoluzioni è rappresentata dall'impiego da parte delle aziende del cloud computing e dei rischi e dei benefici a esso connessi ed è per questo che il presente lavoro si pone l'obiettivo di analizzare le best practice in tema di gestione del rischio applicato al cloud computing.***

## Introduzione

Il *cloud computing* si fonda sulla possibilità di sfruttare una serie di "capacità" informatiche indipendentemente dalla loro presenza su supporti fisici, da qui la definizione di "nuvola", i cui contenuti sono accessibili e gestibili da qualsiasi postazione e con qualsiasi dispositivo grazie ad accessi certificati. Fattori, quali la riduzione dei costi, la scalabilità e la flessibilità che derivano dall'applicazione del *cloud computing*, investono tutti i tipi di settori e i loro effetti si riscontrano sia sul livello della produzione sia sul mercato del lavoro.
Nonostante i notevoli benefici, è importante tenere in considerazione alcuni rischi che si possono incontrare nell'adottare questo nuovo tipo di tecnologia (per esempio, *privacy* e sicurezza).
I potenziali problemi di violazione della *privacy* aumentano notevolmente con l'utilizzo di reti wireless e nel caso delle aziende è elevato il rischio di spionaggio industriale. Un ulteriore problema che può manifestarsi quando i *Data Center* contenenti i dati pubblici sono di natura privata o sono localizzati in stati diversi, in assenza di norme internazionali appropriate, è il rischio che non ci siano le adeguate garanzie.
Attraverso l'utilizzo del *Framework* del COSO, il *management* avrà un approccio effettivo che gli consente di identificare i rischi specifici nonché le risposte al rischio necessarie per una corretta adozione del *cloud computing*.
L'*Enterprise Risk Management* (ERM) è un modello che consente di gestire nel miglior modo i rischi connessi al raggiungimento degli obiettivi aziendali. Gli obiettivi di questo modello sono da ricondurre al concepimento dei rischi relativi alla gestione aziendale e al miglioramento della valutazione del processo di gestione del rischio.
Il Committee Of Sponsoring Organizations of Tradeway Commission (COSO) definisce l'ERM come segue: "La gestione del rischio aziendale è un processo, posto in essere dal consiglio di amministrazione, dal *management* e da altri operatori della struttura aziendale; utilizzato per la formulazione delle strategie in tutta l'organizzazione; progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti del rischio accettabile e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali"[1].
Questo modello è utilizzato per andare a definire la strategia e/o, più precisamente, definire gli obiettivi strategici. L'ERM, infatti, permette al *management* di prendere in considerazione, nel momento di definizione degli obiettivi, i relativi rischi, questo potrà indurre l'Alta Direzione a scegliere una strategia più appropriata. Un ulteriore elemento di novità del modello ERM è il *risk appetite* o rischio accettabile, il quale può essere definito come il livello di rischio che l'azienda nel suo complesso e i suoi singoli soggetti sono propensi ad accettare per il conseguimento degli obiettivi. La propensione al rischio può essere misurata in termini qualitativi e quantitativi. Gli elementi chiave del sistema ERM sono i seguenti:
- il processo - l'ERM è un processo in quanto interessa una serie coordinata di azioni interdipendenti che riguardano l'azienda nel suo complesso, volto all'identificazione e alla valutazione dei rischi potenziali ed effettivi. L'ERM raggiunge il massimo della sua efficacia quando questi meccanismi sono radicati nella struttura organizzativa e fanno parte della cultura aziendale;
- le persone - l'ERM è un processo implementato dai soggetti aziendali (Consiglio di Amministrazione, *management* e altri soggetti) i quali stabiliscono la *mission*, la strategia e gli obiettivi dell'azienda e

[1] Cfr. COSO (2004).

attivano i meccanismi del processo di gestione del rischio. Si tratta, principalmente, di soggetti che possiedono informazioni sulle diverse situazioni di rischio e che sono in grado di comprendere i fattori che determinano i rischi e le loro implicazioni;
• la strategia - l'ERM è un sistema integrato nella pianificazione strategica aziendale. Esso, infatti, deve svolgere un ruolo determinante nel fornire tutti gli elementi utili alle scelte tra le possibili strategie aziendali;
• la propensione al rischio - l'ERM deve effettuare valutazioni che siano compatibili con la propensione al rischio aziendale. La propensione al rischio è l'ammontare qualitativo e quantitativo del danno collegato al rischio che l'azienda e il suo *management* sono disposti ad accettare per il perseguimento dei loro obiettivi. Esso riflette la filosofia della gestione del rischio e, a sua volta, influenza la cultura e gli stili operativi di un'organizzazione. Molte aziende stabiliscono il rischio accettabile in termini qualitativi, usando aggettivi come "alto", "moderato" o "basso", mentre altre preferiscono valutarli dal punto di vista quantitativo, determinando *target* equilibrati di crescita, di redditività e di rischio. L'ERM aiuta la direzione a scegliere la strategia che allinea la creazione del valore al rischio accettabile;
• la ragionevole sicurezza - l'ERM fornisce al *management* e al Consiglio di Amministrazione solo una ragionevole sicurezza sul raggiungimento degli obiettivi aziendali, pertanto non fornisce alcuna certezza che ciò avvenga. L'ERM, infatti, aiuta l'azienda nel perseguimento degli obiettivi prestabiliti; tuttavia, si possono verificare eventi imprevisti, errori o *report* sbagliati, per cui anche un ERM efficace può rivelarsi illusorio. Ragionevole sicurezza non significa certezza assoluta.
Il *Framework* COSO ERM si prepone l'obiettivo di rappresentare un linguaggio comune, fornendo al contempo indicazioni chiare per l'implementazione di un sistema di gestione dei rischi e definendone le componenti essenziali.

## Cloud Computing

Il *Cloud Computing* (*Cloud*) descrive l'utilizzo di una quantità di servizi, applicazioni, informazioni e infrastrutture, le quali comprendono aggregati di risorse e di informazioni. Il *Cloud* aumenta la collaborazione, l'agilità, la scalabilità e la disponibilità, fornendo il potenziale per ridurre i costi mediante l'utilizzo ottimizzato ed efficiente delle risorse computazionali.
Il National Institute of Standards and Technology (NIST), ovvero l'ente di standardizzazione americano, ha prodotto la definizione di *cloud computing* che ha trovato il consenso più ampio:
"*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*".
Il *cloud* è un modello di distribuzione che permette l'accesso *on-demand*, attraverso una rete, a un insieme condiviso di risorse IT configurabili, che sono approvvigionate rapidamente con un minor sforzo di gestione e minima interazione tra cliente e fornitore.
I servizi *cloud* rivelano cinque caratteristiche essenziali che dimostrano la loro relazione con, e le differenze da, gli approcci tradizionali al *computing*[2]:
• *on-demand self service*: l'utilizzatore può unilateralmente disporre di risorse computazionali, come la capacità di calcolo, di *storage* e di rete, in modo automatico, senza richiedere l'interazione umana con il fornitore del servizio;
• ampio accesso alla rete: le capacità di calcolo sono disponibili attraverso la rete e accessibili mediante meccanismi *standard* che consentono il loro utilizzo da dispositivi-piattaforme *client* eterogenee di tipo *thin* o *thick* (per esempio cellulari, *laptop* e PDA);
• condivisione delle risorse (*resource pooling*): le risorse computazionali del fornitore sono raggruppate in un insieme (*pool*) per poter servire una molteplicità di consumatori usando un modello *multi-tenant* con differenti risorse fisiche e virtuali dinamicamente assegnate e riassegnate secondo le richieste dei consumatori (*on-demand*). Esempi di risorse includono *storage*, elaboratori, memorie, larghezza di banda e macchine virtuali;
• elasticità rapida: le risorse a disposizione sono fornite rapidamente ed elasticamente, in alcuni casi in modo automatico, incrementate e decrementate in modo altrettanto veloce. Per l'utilizzatore le capacità disponibili spesso appaiono illimitate e possono essere acquistate in qualsiasi quantità e in ogni momento per ottenere la potenza richiesta. Si può utilizzare il termine scalabilità, che indica la capacità di un sistema di "crescere o decrescere" in funzione delle necessità; può essere diviso in scalabilità orizzontale, che si riferisce all'ammontare delle richieste da soddisfare, e in scalabilità verticale, relativa alla dimensione delle richieste;
• servizio misurato: l'utilizzo delle risorse è controllato e ottimizzato automaticamente grazie alla rilevazione di parametri, misurati a livello di astrazione adeguato al tipo di servizio (ad esempio *storage*, processore, banda, o utenti attivi). L'utilizzo delle risorse è quindi monitorato, controllato e documentato attraverso *report* in modo trasparente, sia per il fornitore del servizio che per l'utilizzatore dello stesso. Come riferimento alla fatturazione, possono essere utilizzati parametri come la quantità di dati salvati, la larghezza

[2] *Cfr. P. Mell, T. Grance (2009).*

di banda, le risorse di processore e la memoria utilizzata nel tempo.
Facendo riferimento alla definizione fornita dal NIST, è possibile entrare più nel dettaglio distinguendo tre modelli di riferimento di servizio, in funzione del tipo di risorse erogate:
1) *Infrastructure as a Service* (IaaS);
2) *Platform as a Service* (PaaS);
3) *Software as a Service* (SaaS).
A tali modelli spesso si fa riferimento come al "Modello SPI", dove SPI sta per *Software*, Piattaforma o Infrastruttura.
Con riferimento agli utenti di riferimento e all'utilità percepita nel caso del SaaS si evidenzia come sia destinato agli utenti finali, che ne percepiscono l'utilità in maniera diretta, grazie al fatto di essere in grado di accedere a un servizio complesso senza la necessità di installare o aggiornare le applicazioni sui loro dispositivi. Lo scenario PaaS si pone invece l'obiettivo di supportare gli sviluppatori di applicazioni *web*, senza che lo stesso debba interessarsi dell'installazione, della configurazione e della gestione di un opportuno *application container*. Infine il livello IaaS interessa gli architetti e gli amministratori di sistema, fornisce loro la possibilità di gestire macchine virtuali e *database* come unità computazionali e di *storage* virtuali, offre loro la possibilità di modificare la capacità computazionale a disposizione, interagendo tramite una semplice interfaccia *web*.
Oltre ai modelli di servizio (IaaS, Paas e SaaS), il NIST individua quattro modelli di implementazione dei servizi *Cloud*:
• *Private Cloud* - l'infrastruttura *Cloud* è utilizzata esclusivamente da un'organizzazione. Può essere gestita dall'impresa o da uno o più *provider* specializzati, e può essere mantenuta (*hosted*) nel *Data Center* all'interno dell'organizzazione (*on-premise*) o presso il *Data Center* del *provider* (*off-premise*). L'impresa ha il pieno controllo sull'infrastruttura e quindi riesce a soddisfare anche i requisiti di *governance* IT;
• *Community Cloud* - l'infrastruttura *Cloud* è condivisa da più organizzazioni e supporta una comunità di utenti-consumatori che hanno gli stessi interessi (ad esempio *mission*, requisiti di sicurezza, *policy*, esigenze relative alla conformità, ecc.). Può essere gestita da una o più imprese della comunità o da una terza parte, e può esistere in forma *on premise* o *off premise*;
• *Public Cloud* - l'infrastruttura *Cloud* è messa a disposizione del pubblico o di un settore industriale di grandi dimensioni ed è di proprietà dell'organizzazione che vende i servizi *cloud*. Gli investimenti infrastrutturali sono interamente sostenuti dal fornitore, mentre il cliente paga a consumo solamente per i servizi effettivamente fruiti (modalità di pagamento *pay-per-use*). Il modello *Public Cloud* permette alle aziende clienti di contenere i costi e di sperimentare servizi aggiornati e tecnologicamente avanzati direttamente attraverso il mercato;
• *Hybrid Cloud* - l'infrastruttura *Cloud* è una composizione di due o più modelli di distribuzione (del tipo privato, pubblico, comunitario), che rimangono entità distinte ma sono, contemporaneamente, integrate da tecnologie standardizzate o proprietarie, che consentono di effettuare la portabilità dei dati e delle applicazioni.
Per il modello *Cloud*, il NIST definisce anche gli "attori" coinvolti nell'erogazione e nell'utilizzo del servizio:
• *Cloud Service Provider* (CSP): il quale fornisce servizi ai *Cloud Service Consumer* a costi e livelli di servizio concordati. Il *provider* gestisce l'infrastruttura tecnica necessaria per l'erogazione dei servizi e produce i dati e la reportistica prevista per la fatturazione; praticamente, non è altro che la nuova figura del fornitore di servizi IT;
• *Cloud Service Consumer* (CSC): è un'organizzazione o un soggetto che ha sottoscritto un contratto con il CSP per l'erogazione dei servizi *cloud.* Al CSC competono sia le responsabilità legate alla definizione dei requisiti dei servizi e all'*audit* della loro conformità alle esigenze, sia quelle relative all'esecuzione delle attività di amministrazione per l'adozione dei servizi stessi (come per esempio la gestione delle identità dei propri utenti);
• *Cloud Service Developer* (CSD): è la figura che si occupa della progettazione e dell'implementazione delle componenti di un servizio *cloud*. Il CSD interagisce con il CSP, descrivendo il servizio necessario per l'implementazione delle varie componenti precedentemente definite, sulla base del servizio adottato;
• *Cloud Service Distributor*: è la figura che fornisce connettività e trasporto per le applicazioni e servizi tra i fornitori di servizi *cloud* e i consumatori.

## Benefici e rischi del cloud computing

### Benefici

I benefici della "nuvola" possono rappresentare i *driver* per soddisfare i bisogni del *business*[3] e, nel contesto attuale, è possibile individuare i seguenti elementi:
• migliorare la struttura di costo;
• rispondere ai cambiamenti del mercato;
• aumentare la produttività.

#### *Migliorare la struttura di costo*

La conversione dei costi fissi in variabili può rappresentare un importante contributo alla situazione dei costi nel lungo periodo e, da tale conversione, si può generare un miglioramento della liquidità aziendale.

[3] *Cfr. A. Ferrari, E. Zanleone (2011).*

Le risorse finanziarie possono essere utilizzate per altri scopi, come ad esempio per coprire situazioni di insolvenza; oppure l'eccesso di liquidità potrebbe essere utilizzato per andare ad aumentare l'*equity*, riducendo così il rischio finanziario dell'azienda.
Si può dedurre che, la riduzione dei costi di *Information and Communication Technology* (ICT) ha un effetto diretto sulla struttura dei costi dell'intera organizzazione.

### *Rispondere ai cambiamenti del mercato*

Rispetto al passato, le organizzazioni si trovano a competere in mercati dove il ciclo di vita dei prodotti si riduce notevolmente; i prodotti, di conseguenza, diventano obsoleti più velocemente. Anche gli attori che operano nel mercato mutano più rapidamente; si assiste a un crescente numero di *joint venture* e acquisizioni di aziende. Le aziende hanno bisogno di reagire e porre in essere strategie adeguate di fronte al connaturarsi di tali cambiamenti. In questo contesto aumenta la pressione, non solo sul *management* ma anche sulle sue ICT, le quali devono essere veloci e flessibili nell'adattarsi alle nuove circostanze.

### *Aumentare la produttività*

Oggi le ICT sono di fondamentale importanza per le aziende, in quanto i processi di *business* sono caratterizzati dalla presenza di tali tecnologie. È fondamentale, inoltre, che tali soluzioni tecnologiche siano veloci e garantiscano semplicità nell'utilizzo, facilitino gli aspetti collaborativi sia a livello di collaborazione diretta (come ad esempio condivisione dei documenti, riunioni con partecipanti da diversi continenti), sia a livello strutturale (ad esempio facilità di accesso da ogni *location*).
Alla luce dei bisogni descritti, si andrà ad analizzare come i requisiti del *cloud computing* (velocità e flessibilità, scalabilità, sicurezza e contenimento dei costi e trasparenza) siano in grado di migliorare l'efficienza e l'efficacia dei processi di *business* delle organizzazioni.
Per quanto concerne la velocità e la flessibilità, in generale, il *cloud computing* consente di ridurre i tempi di realizzazione di nuovi progetti IT. Con l'approccio tradizionale ciò non era possibile, perché per la realizzazione di un servizio informatico erano richieste una serie di fasi che vanno dall'ideazione fino allo sviluppo, per cui era necessario un periodo di tempo più lungo per la realizzazione. Il *cloud computing* permette alle aziende di accedere ad applicazioni che risulterebbero particolarmente onerose se implementate in modalità *on-premise* e addirittura rende possibile l'implementazione di applicazioni che in passato non era possibile utilizzare. Ciò conferisce alle aziende che adottano il *cloud* un alto grado di agilità in situazioni che vedono nuovi progetti di *business* e/o in caso di cambiamenti organizzativi.
La velocità e la flessibilità sono legate alla scalabilità. Il *cloud computing* permette alle imprese di scalare in maniera dinamica le risorse in funzione del carico richiesto con la minima interazione da parte del *provider*, in alcuni casi anche nulla. Da ciò si può evidenziare la caratteristica di elasticità del *cloud computing*. Un altro aspetto è legato alla velocità con la quale le risorse possono essere modificate. Dall'unione della velocità, flessibilità e scalabilità, il principale effetto è un miglior allineamento dell'ICT con i requisiti del *business*.
I servizi *cloud* variano in maniera significativa a seconda dell'organizzazione che li utilizza. Ciò è dovuto alle caratteristiche intrinseche che distinguono tra loro le imprese, come gli obiettivi, gli *asset* posseduti, gli obblighi legali, la propensione al rischio.
Per quanto concerne il contenimento dei costi e trasparenza alcuni studi hanno dimostrato che le aziende possono raggiungere significativi risparmi di costo attraverso il *cloud computing*. Per esempio, il modello di fatturazione è di tipo *pay-per-use* e le risorse utilizzate dall'utente possono essere fatturate in diverse modalità:
- pagamento di un canone fisso che consente l'utilizzo di un set di risorse predeterminato;
- pagamento in funzione dell'utilizzo delle risorse.

Il livello della tariffa di un servizio varierà anche in funzione del livello di qualità richiesto e questo modello rende necessario il monitoraggio continuo dei servizi da parte del *provider* e la trasparenza commerciale verso il cliente.

## Potenziali rischi del Cloud Computing

Il *Cloud Computing*, oltre a presentare notevoli benefici, quali *driver* per i bisogni del *business*, è caratterizzato dalla presenza di notevoli rischi che possono impattare sull'ambiente *cloud*, e che, opportunamente, devono essere ridotti o eliminati mediante strategie di mitigazione, precedentemente elaborate dal *management*.
I migliori approcci alla valutazione del rischio sono quelli nei quali l'analisi è commisurata alla criticità dei dati e dei servizi che si pensa di trasferire *on the cloud*.
La Cloud Security Alliance (CSA), nella propria *Security Guidance*[4], propone che vengano adottati, nel processo di *risk assessment* connessi all'utilizzo dei servizi *cloud*, metodi semplificati nonché la conseguente individuazione delle azioni per mitigare tali eventi aleatori.
Tale metodo di valutazione, prevede, innanzitutto, una prima individuazione degli *asset* oggetto del trasferimento sui servizi *cloud* che riguardi i processi, le funzioni, le applicazioni e i dati.
Questo primo passo, caratteristico di tutte le metodologie di valutazione dei rischi, è particolarmente importante nell'ambiente *cloud*, in quanto, i dati e le

[4] *Cfr. Cloud Security Alliance (CSA) (2010).*

applicazioni possono essere separati e quindi si potrebbero creare situazioni dove solo una parte dei dati o delle applicazioni possono essere oggetto di trasferimento *on the cloud*.
A seguito dell'individuazione degli *asset*, si deve procedere con il processo di *risk assessment* vero e proprio. La CSA, a tal proposito, propone una serie di domande per poter delineare un primo quadro dei rischi. Ad esempio, che tipo di danno si verrebbe a creare se:
1) l'*asset* in valutazione diventasse di pubblico dominio?
2) un dipendente del fornitore di servizi *cloud* avesse accesso all'*asset* in valutazione?
3) il processo o la funzione fossero fraudolentemente manipolati da un *hacker* esterno?
4) il processo o la funzione non fornissero i risultati attesi?
5) le informazioni/dati fossero modificati in maniera non autorizzata?
6) l'*asset* in valutazione non fosse disponibile per un dato periodo di tempo?
La CSA suggerisce, infine, tramite l'analisi di questa serie di risposte, di procedere nella consapevole individuazione del "Modello di erogazione" più adatto alle esigenze dell'azienda e solo dopo cominciare a cercare un eventuale fornitore che possa soddisfare i requisiti individuati.
Al fine di facilitare l'analisi delle minacce nell'ambiente *cloud*, è opportuno descrivere alcuni dei principali rischi a cui sono esposte le organizzazioni che adottano sistemi *cloud computing*. Si tratta di:
• mancanza di trasparenza. È improbabile che un CSP divulghi informazioni dettagliate sui suoi processi, operazioni e controlli. Ad esempio, i clienti *cloud* possono non conoscere la localizzazione dei dati, gli algoritmi usati dal CSP per provvedere a immagazzinare i diversi dati e i controlli specifici usati per salvaguardare l'architettura *cloud computing*;
• affidabilità e problemi di esecuzione. L'errore del sistema rappresenta un evento aleatorio che può verificarsi in qualsiasi *computing environment*. Anche se i *service-level agreements* possono essere strutturati per soddisfare particolari esigenze, le soluzioni CSP potrebbero, in alcune circostanze, essere incapaci di soddisfare queste metriche di *performance*, se un proprietario *cloud* colloca una domanda di risorsa inaspettata nell'infrastruttura *cloud*;
• *vendor lock* e mancanza di portabilità dell'applicazione o interoperabilità: molti CSP offrono strumenti di sviluppo del *software* con le loro soluzioni *cloud*. Quando questi strumenti sono brevettati, essi possono creare applicazioni che operano soltanto nell'architettura della soluzione specifica del CSP. Di conseguenza queste nuove applicazioni operano in maniera inadeguata con i sistemi che risiedono fuori dalla soluzione *cloud*;
• preoccupazioni di sicurezza e conformità: a seconda dei processi che il *cloud computing* sta sostenendo, la sicurezza e i problemi di *privacy* possono sorgere rispetto alla conformità con regolamenti e leggi quali Sarbanes-Oxley Act of 2002 (SOX) e la *privacy* dei vari dati e i regolamenti di protezione emanati in diversi Paesi[5]. In base alla soluzione *cloud* adoperata (SaaS, PaaS, IaaS), i clienti di tale soluzione non possono ottenere e rivedere le operazioni di rete perché essi sono in possesso del CSP. Il CSP non è obbligato a diffondere questa informazione o potrebbe non essere in grado di farlo, senza violare la riservatezza degli altri proprietari che condividono l'infrastruttura *cloud*;
• *high-value cyber-attack target*: il consolidamento di molteplici organizzazioni che operano su un'infrastruttura del CSP rappresenta un obiettivo più attrattivo rispetto ad una singola organizzazione, aumentando così la probabilità di attacchi. Di conseguenza, i livelli di rischio inerenti alla soluzione CSP sono di solito più alti rispetto alla riservatezza e all'integrità dei dati;
• rischio di dispersione dei dati: un ambiente *cloud* multi-proprietà nel quale le organizzazioni utenti e le applicazioni condividono risorse, presentano un rischio di dispersione dei dati che non sussiste quando i server specializzati e le risorse sono usate esclusivamente da un'organizzazione. Questo rischio di dispersione dei dati rappresenta un ulteriore punto di considerazione oltre alla *privacy* dei dati e ai requisiti di riservatezza[6];
• cambiamenti organizzativi IT: se il *cloud computing* è adottato in maniera significativa, un'organizzazione ha bisogno di meno personale interno IT nelle aree di gestione dell'infrastruttura, distribuzione della tecnologia, sviluppo dell'applicazione e mantenimento;
• viabilità del *Cloud service provider*: molti fornitori di servizi *cloud* sono nuove aziende, per cui la proiettata longevità e profittabilità di tali sistemi tecnologici sono sconosciuti. Per tale ragione alcuni CSP stanno limitando le offerte di servizi *cloud* perché non generano profitti.
Le aziende devono riconoscere i rischi e gli effetti che il *cloud computing* può avere nel loro ambiente operativo nonché l'impatto che potrebbe avere sui loro programmi ERM. In alcune circostanze, il *cloud computing* può facilmente insediarsi all'interno dell'azienda ed essere in grado di raggirare i controlli di sorveglianza tipici del *management*.
La Tavola 1 illustra come con il *cloud computing*, alcuni dei controlli tipici (come le risorse del personale e le finanze richieste) non raggiungono i livelli che, tipicamente, interessano la supervisione del *senior management*.
La Tavola 2 illustra poi il livello di controllo che l'organizzazione detiene e cede a seconda del tipo di fornitura di servizio *cloud* e del modello di distribuzione. Specificatamente, il livello massimo di controllo e la quantità minima di rischio inerente sono associate

[5] *Esempi di* privacy *dei dati e leggi di protezione sono USA Patriot Act e EU Data Protection Directive.*
[6] *Cfr. L. Bean (2011). Un fattore principale potrebbe essere la percezione che i dati e le funzioni sensibili vengono spostati su* internet, *e chiunque con adeguate competenze tecniche potrebbe abbastanza facilmente accedervi.*

a soluzioni IaaS (*private cloud*). Al contrario, con una soluzione SaaS (*public cloud*) l'organizzazione detiene un minor livello di controllo e deve accettare un livello più alto di rischio inerente. In tutti i casi, il *management* deve valutare i modelli di distribuzione e le forniture di servizio *cloud* nel contesto di un rischio accettabile, in quanto questo determinerà l'ambiente *cloud computing* tipico nonché stabilirà i controlli necessari ad esso correlati.

## ERM e cloud computing

Lo sviluppo di un piano che definisca gli obiettivi dell'organizzazione e le specificità dei ruoli del *cloud computing* permetterà al *management* di assumere con maggiore consapevolezza e ponderazione le decisioni aziendali. Alcuni dei prerequisiti dell'ERM che dovrebbero essere presi in considerazione in un piano di *cloud computing* di qualità, rappresentano un forte modello di *governance* capace di effettuare un'accurata analisi delle capacità IT interne e analizzare il livello di *risk appetite.* Spesso le organizzazioni adottano soluzioni *cloud computing* senza applicare una valutazione del rischio formale mediante l'adozione di un programma ERM o un piano di direzione.

È di fondamentale importanza incorporare la *cloud governance* nella fase iniziale (quando si definisce una strategia di *cloud computing*) prima che la soluzione *cloud* venga adottata. Le organizzazioni che hanno già adottato il *cloud computing* senza applicare le *best practice* dell'ERM, possono comunque effettuare la valutazione dei rischi e stabilire la *cloud governance*.

**Tavola 1 - Cloud solution e controlli**

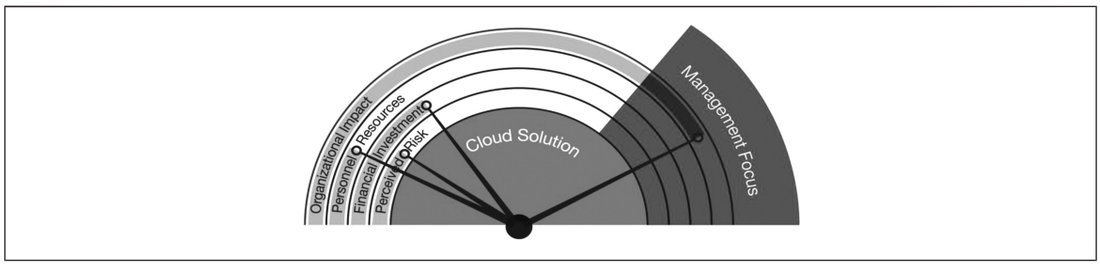
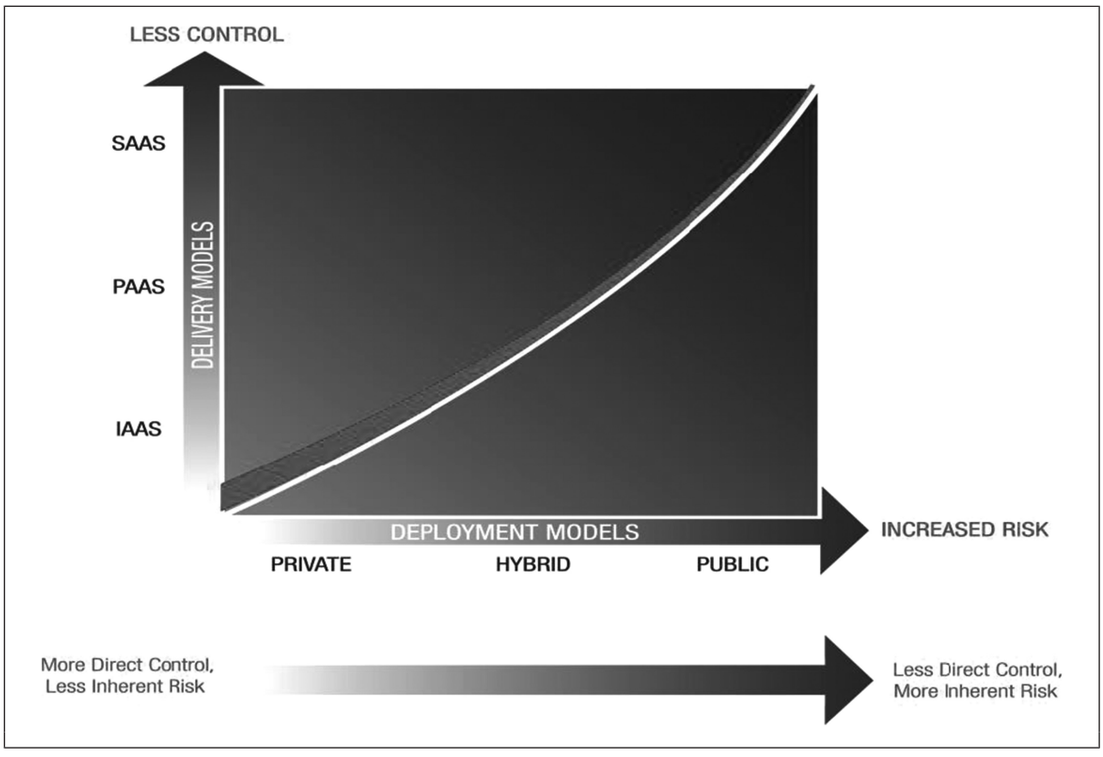



**Tavola 2 - Inherent Risk Relationship, Cloud Service Delivery e modelli di distribuzione**



Il livello di adattamento richiesto a un programma ERM, nell'ambito di un'organizzazione che impiega soluzioni *cloud computing*, dipende fortemente dai processi di *business* che il *cloud* sostiene, dai modelli di distribuzione, dai modelli di erogazione del servizio, dalla natura dei rischi del CSP e dall'ambiente di controllo. In molti scenari, le organizzazioni non hanno più il controllo completo o diretto sulla tecnologia e sui processi di gestione legati alla tecnologia. Il *management* ha il compito di determinare il livello di propensione al rischio dei potenziali eventi associati a una determinata soluzione *cloud*[7], come alcuni di questi eventi si estendono oltre i limiti dell'organizzazione nonché comprendere gli eventi che impattano sul CSP.

La Tavola 3 rappresenta come i candidati della specifica soluzione *cloud* prediligono le varie opzioni, sulla base dei processi di *business* sostenuti dal *cloud*, modelli di distribuzione e modelli di erogazione dei servizi.

L'adozione del *cloud computing* potrebbe rappresentare un notevole cambiamento per l'organizzazione, e per tale ragione il *management* adotta il *Framework* ERM per valutare e gestire i rischi connessi alle soluzioni *cloud*. Nella Tavola 4 il *Framework* viene rappresentato come una sorta di sentiero nel quale per ogni componente ERM applicato si evidenziano i vantaggi e gli svantaggi specifici che ogni determinata soluzione ERM per il *cloud* potrebbe arrecare all'organizzazione. Quando il processo è completato, la soluzione *cloud* ideale emergerà, insieme ai suoi requisiti, al fine di stabilire la *cloud governance*.

Nell'ipotesi in cui la soluzione *cloud* sia già stata implementata, il *Framework* del COSO ERM può essere impiegato per stabilire, perfezionare o eseguire un controllo di garanzia e di qualità del programma di

**Tavola 3 - Creazione soluzioni cloud**

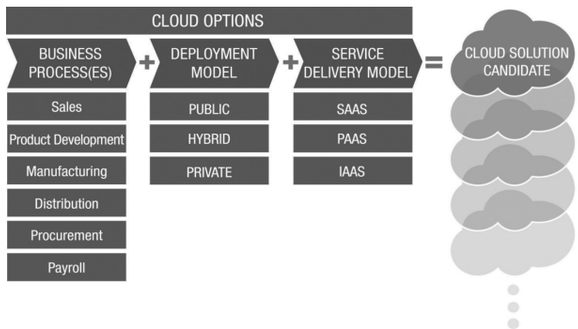
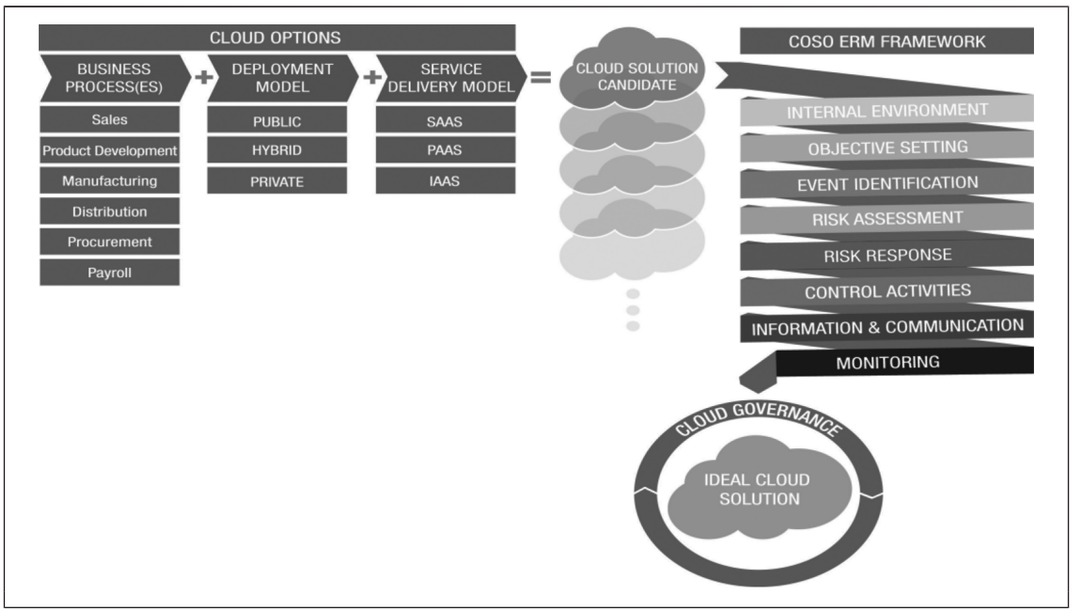



**Tavola 4 - Applicazione COSO ERM Framework alle opzioni di cloud computing**




[7] *Cfr. N. Brender, I. Markov (2013).*

direzione *cloud*, assicurando che tutti gli aspetti del piano (per esempio gli obiettivi, valutazione del rischio e *risk response*) siano stati affrontati nel rispetto delle esigenze del *management*. Un efficace programma di direzione può ancora realizzarsi applicando il *Framework* del COSO ERM dopo l'attuazione di una soluzione tecnologica.
La circostanza di *best practice* si verifica quando il *Framework* del COSO ERM viene applicato per identificare la migliore opzione tra le soluzioni *cloud* proposte (per esempio processo di *business*, modello di distribuzione, modello di erogazione del servizio) che si adatta al *risk appetite* del *management*. Valutando le varie soluzioni nel contesto di ogni componente proposto dal *Framework* del COSO ERM, il *management* può sinteticamente identificare i rischi connessi, il livello di rischio accettabile e le strategie di mitigazione da applicare a ogni soluzione *cloud* (in quanto i rischi variano a seconda della soluzione tecnologica da adottare).
È opportuno, ora, procedere con l'analisi della valutazione delle soluzioni *cloud computing* attraverso le componenti proposte dal *Framework* del COSO ERM.

## Ambiente interno

L'ambiente interno mantiene in equilibro tutte le altre componenti, influenzando però gli obiettivi, le strategie, i processi di gestione del rischio. L'ambiente interno del modello ERM è incentrato su tutti gli aspetti interni all'azienda legati ai rischi aziendali e attraverso i quali è possibile costruire un approccio alle attività di controllo orientate al futuro.
L'ambiente interno serve come base per definire il livello di propensione al rischio dell'organizzazione; per esempio se il *management* ha la politica di non esternalizzare alcuna delle sue operazioni questo sistema limiterà le opzioni che porterebbero proficui profitti in modo che le soluzioni *private cloud* non rappresentino l'unica alternativa accettabile.

## Obiettivi strategici

L'attività di individuazione degli obiettivi non può prescindere dalla determinazione della *mission* aziendale, la quale rappresenta un elemento cruciale nella pianificazione strategica, che condiziona la predisposizione della strategia generale e lo sviluppo di specifiche strategie funzionali. In relazione alle scelte strategiche, vincolate sulla base della *mission* aziendale, il *management* effettuerà la selezione, lo sviluppo e l'implementazione dei *sub*-obiettivi operativi, informativi e di conformità che saranno oggetto del modello ERM.
Il *management*, nell'ambito delle soluzioni *cloud*, ha il compito di valutare come il *cloud computing* si allinea agli obiettivi dell'organizzazione. A seconda delle circostanze, il *cloud computing* potrebbe rappresentare un'opportunità per l'organizzazione per accrescere la sua capacità di raggiungere gli obiettivi esistenti, o potrebbe presentare l'opportunità di ottenere un vantaggio competitivo, ma in questo caso è necessario ridefinire nuovi obiettivi.

## Event identification

L'identificazione dell'evento è quel componente dell'ERM che definisce gli avvenimenti interni ed esterni all'azienda che influenzano l'implementazione dell'ERM e/o il raggiungimento degli obiettivi. Il *management* è responsabile nell'identificazione degli eventi (si parla sia di opportunità che di rischi) che possono influenzare il conseguimento degli obiettivi. La complessità dei processi di identificazione degli eventi e della valutazione del rischio incrementa quando l'azienda assume dei fornitori di servizio *cloud*. Il *management* nel processo di valutazione e identificazione degli eventi aleatori considera sia i fattori interni all'azienda quali la cultura, il personale e la salute finanziaria, ma anche i fattori ambientali esterni come per esempio gli eventi economici esterni, gli eventi naturali, politici, sociali e l'evoluzione tecnologica. Il *management*, inoltre, deve avere un inventario completo degli eventi, poiché la natura e la qualità dei processi di valutazione del rischio possono essere influenzati dagli eventi inaspettati.

## Risk assessment

La valutazione del rischio è la componente centrale dell'ERM che consente al *management* di comprendere come i rischi potenziali influenzano il raggiungimento degli obiettivi prestabiliti.
Il *management* ha quindi il compito di valutare gli eventi aleatori associati alle strategie *cloud* al fine di determinare l'impatto potenziale che tali rischi hanno su tali soluzioni tecnologiche. Teoricamente, le valutazioni del rischio devono essere completate prima che la soluzione *cloud* venga impiegata. Il *cloud computing* può interessare punti focali critici di una valutazione del rischio quali:
- *risk profile* - il *risk profile* di un'organizzazione racchiude l'insieme dei rischi che il *management* deve opportunamente gestire. Quando viene adottata una soluzione *cloud*, il profilo dei rischi di un'azienda viene alterato a seguito dei cambiamenti nella probabilità dei rischi, il potenziale impatto degli stessi nonché la considerazione dei rischi connessi al CSP;
- rischio inerente e residuo - l'organizzazione deve valutare i rischi inerenti associati agli eventi per poi sviluppare le risposte al rischio e determinare conseguentemente il rischio residuo.Il rischio inerente o intrinseco è il rischio gravante sull'attività

indipendentemente dalle operazioni di controllo messe in atto mentre, quello residuo o residuale è il rischio a cui rimane esposta l'attività aziendale dopo aver adottato le opportune precauzioni di controllo. I fattori che caratterizzano il rischio inerente sono legati alla natura stessa dell'attività economica posta in essere ma possono essere influenzati dall'ampiezza delle risorse economiche a disposizione della stessa e dalla presenza di un *management* fortemente orientato al rischio;
• probabilità e impatto - il processo di analisi dei rischi comporta che per ogni rischio vengano individuati due parametri: la probabilità di verificazione e l'impatto o significatività, rappresentato dall'ammontare del possibile danno. La probabilità di certi eventi e l'impatto potenziale variano a seconda dell'adozione o meno di soluzioni *cloud*[8].

## Risk response

L'attività di *risk response* riguarda la scelta da parte del *management* delle attività da porre in essere per controllare il rischio aziendale tra quelle possibili precedentemente individuate con il *risk assessment*. Inoltre, la risposta al rischio deve valutare quanto le tecniche di gestione del rischio siano attuabili in termini economici. Il limite all'implementazione di tali tecniche è rappresentato dal costo. Difatti un rischio è ritenuto accettabile se il costo richiesto per la sua eliminazione o riduzione è eccessivo rispetto ai benefici ottenibili.
Una volta che i rischi sono stati identificati e valutati nel contesto degli obiettivi organizzativi relativi al *cloud computing*, il *management* deve determinare la sua risposta al rischio. È possibile analizzare quattro tipologie di *risk response*:
• *avoidance*: l'approccio prevede un atteggiamento riluttante nell'intraprendere azioni che potrebbero comportare eventi aleatori. Nel caso del *cloud computing* l'approccio *avoidance* consiste nell'uscire dalle attività che possono dare origine a eventi rischiosi (vale a dire non muoversi verso soluzioni *cloud* o considerare solo soluzioni di *private cloud*);
• *reduction*: tale approccio è volto all'adozione di un ampio raggio di decisioni aziendali atte a ridurre determinati rischi. In pratica consiste nel realizzare le attività di controllo e porre in essere le azioni per ridurre la probabilità e l'impatto del rischio;
• *sharing*: consiste nel ridurre la probabilità e l'impatto del rischio mediante la possibilità di trasferire o condividere i rischi identificati mediante i processi aziendali;
• *acceptance*: questo approccio si caratterizza per la decisione di non intraprendere azioni in presenza di determinati rischi. Il *management*, sulla base della tolleranza al rischio, valuta il rischio in termini di probabilità e di impatto per decidere quale parte di esso accettare o meno.

## Attività di controllo

Le attività di controllo sono strettamente collegate alla fase successiva al *risk response*. Identificata la migliore strategia di risposta al rischio coerente con il grado di propensione al rischio dell'azienda e con i costi e i benefici delle operazioni di gestione, il *management* deve selezionare le attività di controllo necessarie ad assicurare che le risposte al rischio siano effettivamente eseguite dalle risorse umane e nei tempi prestabiliti.
Le tradizionali tipologie di controllo vengono applicate anche nell'ambito del *cloud computing*, con la differenza che, mentre alcune responsabilità di controllo sono di competenza dell'azienda, altre responsabilità vengono trasferite al CSP. Se le attività di controllo esistenti all'interno dell'azienda hanno un livello di qualità particolarmente moderato o basso, adottare una soluzione *cloud* potrebbe aggravare le carenze e le debolezze del controllo interno. Per esempio, se un'azienda applica controlli con un basso livello di sicurezza in termini di password o in termini di pratiche della sicurezza sui dati e, decide di trasferire il suo ambiente di calcolo verso una soluzione *public cloud* o *hybrid*, la possibilità di violare la sicurezza dei dati è destinata ad aumentare in modo significativo a causa del fatto che l'accesso alla tecnologia da parte dell'organizzazione avviene ora attraverso la rete *internet*.

## Informazione e comunicazione

Per operare efficacemente la propria attività e gestire i rischi relativi, il *management* si affida a informazioni e comunicazioni tempestive e accurate da varie fonti che riguardano eventi esterni e interni. Con il *cloud computing*, le informazioni ricevute dal CSP potrebbero non essere tanto tempestive o della stessa qualità delle informazioni della funzione interna IT. Il *management*, inoltre, ha anche il compito di monitorare le informazioni esterne correlate al suo CSP (per esempio rapporti finanziari, informativa al pubblico, richieste di autorizzazione, periodici di settore, annunci dei soci proprietari del *cloud*), dal momento che certi eventi che impattano il CSP o i soci proprietari del *cloud* potrebbero influenzare l'organizzazione.

## Monitoraggio

L'intero processo ERM deve essere monitorato e modificato ove necessario. Il *management* deve continuare a monitorare l'efficacia del proprio programma ERM per verificare che esso affronti adeguatamente i rischi rilevanti e faciliti il raggiungimento degli obiettivi dell'organizzazione.
Il monitoraggio rappresenta l'elemento necessario a determinare una corretta implementazione di tutti i

[8] *Cfr. B. W. Nocco, R. M. Stulz (2006).*

componenti del modello, nonché un loro efficace ed efficiente funzionamento. In particolare, la presenza del monitoraggio continuo, permette al *management* di identificare le eccezioni o le violazioni nei vari elementi dell'ERM.

## Le risposte al rischio suggerite per il cloud computing

In questo paragrafo si andrà a descrivere e analizzare le risposte al rischio raccomandate per alcuni dei più significativi rischi legati al *cloud computing*.

### Rischio: attività cloud non autorizzata

*Risposta al rischio: politiche e controlli cloud*

Tutte le aziende dovrebbero avere delle politiche per stabilire i controlli per prevenire e scoprire l'utilizzo non autorizzato dei servizi *cloud computing*. Per le organizzazioni che hanno deciso di adottare il *cloud computing*, quelle che seguono sono alcune delle possibili risposte al rischio suggerite in relazione all'attività *cloud* non autorizzata:

- stabilire una politica d'uso del *cloud* che chiaramente articola i processi di *business* e i dati che la gestione giudica appropriati a essere supportati dalle soluzioni *cloud computing*;
- creare o aggiornare una politica che identifica chi è autorizzato a procurare i servizi *cloud computing*;
- identificare i venditori *cloud* approvati;
- definire la politica e comunicare la guida sulla gestione delle relazioni con i CSP.

### Rischio: mancanza di trasparenza

*Risposta: valutazioni dell'ambiente di controllo del CSP*

Eseguire un processo di *risk assessment* di elevata qualità nell'ambito del CSP, può risultare impegnativo soprattutto quando le informazioni sono incomplete e difficili da reperire. Nella maggior parte dei casi, l'ambiente di controllo interno del CSP non è completamente visibile ai propri clienti. Per esempio, i controlli relativi ai cambi di gestione, all'accettazione degli utenti e la separazione tra la produzione e gli ambienti di sviluppo, sono normalmente adoperati per assicurare la qualità nei sistemi di applicazione. Attraverso una soluzione SaaS *public* e *Hybrid cloud*, i clienti *cloud* non hanno il diretto controllo o la conoscenza dettagliata sui controlli di gestione e sulle modifiche applicate alle applicazioni del CSP. Di conseguenza, i clienti possono aver bisogno di aumentare o cambiare i loro processi per testare i cambiamenti nelle applicazioni a seconda della loro propensione al rischio.

### Rischi: sicurezza, conformità, fuga dei dati e giurisdizione dei dati

*Risposta: politiche e processi di classificazione dei dati*

L'adozione di soluzione *public* e *Hybrid cloud* potrebbero modificare la locazione corrente del magazzino dati dell'impresa, il processo di transazione delle informazioni e la struttura dei controlli. Questi cambiamenti richiedono, necessariamente, un'attenta analisi poiché possono avere impatti sulle operazioni aziendali, per cui è opportuno verificare la *compliance* alle leggi e ai regolamenti in vigore. È fondamentale che il contratto *cloud* debba chiaramente definire le responsabilità del CSP in merito alla verifica della conformità o meno delle informazioni alle leggi applicate e alle normative vigenti. Se i dati di un'organizzazione risiedono in una soluzione *cloud*, risulta particolarmente difficile identificare la locazione corrente o la residenza storica dei dati (ci si riferisce sia ai server che al magazzino dati). Anche se le aziende non sono in grado di identificare esattamente dove sono localizzati e immagazzinati i dati quando si adoperano soluzioni *public cloud*, esse hanno comunque la possibilità di controllare il tipo di informazione che risiede nei sistemi *cloud computing*.

Le politiche di classificazione dei dati devono chiaramente definire le tipologie di informazioni considerate particolarmente sensibili per l'azienda. Tali politiche devono, dunque, assicurare che lo scopo, il possesso e la sensibilità dei differenti dati aziendali siano esplicitamente comunicati e compresi in tutta l'organizzazione. Queste politiche dovrebbero essere supportate dai processi di classificazione dei dati che includono i seguenti aspetti:

- applicare le richieste della proprietà e della sicurezza legale, regolamentare, intellettuale ai vari tipi di dati;
- determinare la sensibilità (pubblica, ristretta o altamente sensibile) dei vari tipi di dati;
- stabilire i requisiti (come la crittografia) per la trasmissione dei dati;
- identificare i proprietari dei dati - individui che hanno la conoscenza adeguata e l'autorità per decidere a chi dovrebbe essere garantito l'accesso ai dati e il tipo di accesso (per esempio, un *business manager* o un responsabile di *compliance*).

### Rischi: trasparenza e abbandono del controllo diretto

*Risposta: sorveglianza di gestione e controlli sulle operazioni di verifica*

Nelle situazioni di non *outsourcing*, il *management* può porre in essere azioni dirette sugli aspetti del suo ambiente di controllo interno. Nei modelli *public* e *hybrid cloud*, il *management* trasferisce in maniera

parziale o totale il controllo diretto al CSP. Nella maggior parte delle circostanze, il CSP ha il compito di fornire una piattaforma stabile e sicura in grado di soddisfare le richieste di controllo dei suoi clienti da una prospettiva macro. La responsabilità del *management* è quella di valutare dettagliatamente le varie soluzioni del CSP nonché realizzare i controlli in modo che tali soluzioni siano in grado di rispondere a tutti i requisiti richiesti dall'organizzazione. È fondamentale che il *management* abbia una approfondita conoscenza dei controlli, cosicché da porre in essere le attività di monitoraggio specifico che la stessa dovrebbe realizzare.
Il *management* e il CSP sono responsabili congiuntamente sul controllo dell'ambiente interno della soluzione *cloud*. Le aziende che adottano tali soluzioni (*public* e *hybrid*) dovrebbero validare le attività di controllo, per assicurarsi che essi si allineano adeguatamente con la propensione al rischio dell'azienda. Inoltre le aziende devono periodicamente verificare l'efficacia dei controlli e, a seconda del modello di distribuzione selezionato, la responsabilità del controllo tra l'organizzazione e il CSP può essere condivisa nelle aree di implementazione, nelle operazioni tecnologiche e nell'amministrazione di accesso degli utenti.

### Rischio: vendor lock-in

*Risposta: preparazione di una strategia di uscita*

Più un'organizzazione adotta sistemi *cloud computing* da un unico CSP e più dipenderà da esso. Al fine di evitare di essere totalmente dipendente dal futuro di uno specifico CSP sarebbe prudente per il *management* anticipare la sua futura necessità di cambiare il fornitore CSP o di muoversi verso soluzioni alternative. Di conseguenza, la gestione dovrebbe sviluppare una strategia di uscita o un piano di contingenza come parte della sua strategia *cloud* complessiva.

### Rischio: non conformità con gli obblighi di comunicazione

*Risposta: nuove informazioni nel financial reporting*

Alla luce del potenziale impatto che le soluzioni *cloud computing* hanno sulle operazioni di *business*, le aziende devono avere la dovuta consapevolezza che tutte le nuove informazioni devono essere comunicate nel reporting finanziario, al fine di rispettare gli obblighi di trasparenza e garantire la *compliance* alle leggi e ai regolamenti vigenti.

## Novità implicazioni e conclusioni

Nel giugno 2016 il COSO ha pubblicato un aggiornamento sul *Framework* ERM[9]. Questo documento rappresenta un importante cambiamento al quadro ERM COSO del 2004, in particolare la rimozione del COSO *Cube* è un segnale positivo perché avvertito da molti *practitioners* come un fatto prescrittivo, rigido che ha avuto conseguenze non intenzionali, come per esempio, la limitata flessibilità necessaria per la gestione del rischio, dovendo identificare, valutare e segnalare i rischi secondo i dettami previsti dal cubo. Inoltre, il Progetto 2016 rappresenta un "accoglimento" delle dinamiche contemporanee di *enterprise risk management* relativamente alla propensione al rischio, alla cultura, alla strategia e, soprattutto, all'affermazione del legame tra rischio e obiettivi di *business* e, per questo motivo, il *Framework* originario del 2004 si può considerare già adesso, sebbene il documento sia tuttora in fase di lavorazione (dato che nel mese di dicembre 2016 sono state pubblicate le lettere di commento al *draft*) esplicitamente "pensionato".
Il *Framework* allo stato attuale dell'arte è migliorato senz'altro anche per il fatto che sviluppa meglio gli obiettivi alla base del modello stesso e stabilisce in maniera maggiormente chiara i concetti principali dell'ERM.
Per questo motivo, il *draft* in alcuni suoi punti sembra meglio proporre schemi applicabili al sistema di controllo interno e a varie tematiche quale appunto il *cloud computing*.
Tuttavia il documento non affronta completamente alcuni vincoli inerenti l'ERM quali i costi/benefici, la capacità di adattamento con le altre iniziative di gestione del rischio e la valutazione del livello di significatività dei rischi collegati agli obiettivi più importanti.
Indubbiamente dalla futura evoluzione e dalla *final release* che, presumibilmente avverrà nella primavera/estate del 2017 si svilupperanno scenari da tenere in considerazione anche per una migliore considerazione della tematica del *cloud computing*.
Nonostante i rischi, data la portata innovativa e i notevoli vantaggi che il *cloud computing* offre, numerosi saranno gli investimenti per potenziarla e renderla sempre più affidabile, ma soprattutto, usata appropriatamente, con le dovute precauzione e in particolare mediante l'applicazione del *Framework* del COSO ERM.

## Bibliografia

Bean L. (2011), "Cloud Computing: Retro Revival or the New Paradigm?", in *The Journal of Corporate Accounting & Finance*, July/August, pagg. 9-14.

[9] Cfr. COSO (2016).

Brender N., Markov I. (2013), "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies", in *International Journal of Information Management*, Vol. 33, pagg. 726-733.

Cloud Security Alliance (CSA) (2010), "Top Threats to Cloud Computing", versione 1.0.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004), *Internal Control - Integrated framework.*

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2012), *Enterprise Risk Management for cloud computing.*

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2016), *Internal Control - Integrated framework.*

Ferrari A., Zanleone E. (2011), *Cloud computing. Aspettative, problemi, progetti e risultai di aziende passate al modello "as a service"*, Milano, Franco Angeli.

Mell P., Grance T. (2009), *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology (NIST).

Nocco B.W., Stulz R.M. (2006), "Enterprise Risk Management: Theory and practice", in *Journal of Applied Corporate Finance*, Vol. 18, No. 4, pagg. 8-20.