La governance IT e il Cloud:
principi e pratiche per governare l'adozione del Cloud Computing

Ron Speed, CISA, CRISC, CA, è un dirigente IT con oltre 20 anni di esperienza nel settore e negli ambiti della gestione del rischio, della governance, della sicurezza e della consulenza. Ha diretto e fornito consulenza in merito a iniziative di trasformazione strategica in Australia e negli Stati Uniti. Le sue aree di specializzazione comprendono il settore dei servizi finanziari e la conformità normativa per l'area dell'Asia-Pacifico.

In tutto il mondo, le aziende assistono all'ingresso sul mercato di una miriade di nuovi servizi di Cloud Computing. Pressoché chiunque può facilmente partecipare ed accedere a queste offerte che coprono ogni servizio dal backup di file personali alla gestione di server di produzione e servizi applicativi.

Riuscirà il Cloud Computing a offrire alle aziende vantaggi economici durevoli? Qual è l'impiego ottimale dei servizi Cloud? È possibile adottarli con modalità tali da non mettere in pericolo il profilo di rischio di un'azienda? Questioni che, nel prossimo futuro, saranno dibattute in molti consigli di amministrazione, e a ragione. Una cosa è certa: il Cloud Computing come tendenza sta mettendo sotto pressione i tradizionali processi di governance IT, imponendo loro di adeguarsi. Perché le aziende possano prendere decisioni avvedute in relazione ai servizi Cloud, i responsabili della governance e del rischio IT devono lavorare a stretto contatto con i manager di business, allo scopo di promuovere una comprensione dei principi chiave del Cloud Computing e per contribuire a definire pratiche di governance efficaci.

PERCHÉ TUTTO QUESTO TRAMBUSTO?

Per coloro che non avessero familiarità con l'espressione, si intende per "Cloud Computing" la tecnologia basata su Internet (in termini di software, piattaforma, infrastruttura, o di una loro combinazione) per l'archiviazione e l'elaborazione delle informazioni, fornita come servizio on-demand.

Allora qual è l'elemento così innovativo e rivoluzionario di questa tecnologia? A prima vista, sembrerebbe una versione Internet dell'outsourcing IT. In un certo senso è così, ma con alcune differenze importanti. Per spiegare meglio il concetto può essere utile ricorrere a un'analogia: prendiamo i pendolari che, recandosi al lavoro in auto, arrivano spesso in ritardo a causa del traffico, dei lavori stradali e dei frequenti guasti (perché possiedono auto vecchie e dalla manutenzione poco curata). Ora, si può cercare di affrontare il problema acquistando GPS, comprando nuove auto, provvedendo a interventi di manutenzione periodici o perfino assumendo autisti professionisti che accompagnino i dipendenti nel tragitto casa-lavoro. Questo approccio sarebbe simile all'impiego dei modelli classici di servizio IT, con l'utilizzo di un autista analogo al tradizionale outsourcing IT.

Un approccio alternativo per affrontare la situazione potrebbe essere vendere l'auto e recarsi al lavoro in treno, acquistando abbonamenti ferroviari annuali. Così facendo, i pendolari essenzialmente rinuncerebbero a un approccio individualistico al problema e adotterebbero un metodo standard, tecnologicamente agnostico, per ottenere il medesimo risultato. Tutti i problemi connessi all'inaffidabilità dei singoli mezzi e ai costi del loro utilizzo vengono sostituiti con una soluzione dalla struttura di costi completamente diversa, e con rischi e opportunità dissimili. Questo approccio è analogo alla transizione verso l'utilizzo dei servizi di Cloud Computing.

Come per questa analogia, sono diversi e importanti i pro e i contro da considerare nel passaggio al Cloud Computing dall'IT tradizionale (in-house o tramite il classico outsourcing). Quali esattamente dipende dalla specificità dei servizi coinvolti, ma tipicamente si tratterà di:

- **Flessibilità** – Quando utilizzano l'IT tradizionale, le aziende dispongono di flessibilità quasi completa, in quanto decidono in prima persona le modalità di utilizzo. Con il Cloud Computing, invece, la flessibilità rischia di essere più limitata, in base alla modalità di fornitura dei servizi. Ad esempio, molti servizi Cloud PaaS (Platform as a Service) vengono mantenuti aggiornati rispetto alle versioni del sistema operativo corrente: se un'azienda desiderasse utilizzare una versione precedente, questo potrebbe non essere possibile o richiedere la predisposizione di un servizio più personalizzato (e quindi più costoso). Alcuni servizi Cloud, come EC2 di Amazon,

Avete commenti su questo articolo?

Visitate le pagine *Journal* del sito web di ISACA *(www.isaca.org/journal)*, cercate l'articolo e cliccate sulla linguetta Comments per condividere le vostre opinioni.

Vi interessa questo articolo?

- Leggere *IT Control Objectives for Cloud Computing*.

www.isaca.org/ITCOCloud

- Leggere *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*.

www.isaca.org/cloud

- Valutare la partecipazione alla Information Security and Risk Management Conference di ISACA a Las Vegas, Nevada, USA; San Juan, Puerto Rico; o Barcellona, Spagna, dove saranno organizzate più sessioni dedicate al Cloud.

www.isaca.org/isrm

- Per saperne di più e collaborare in relazione a *Cloud Computing e governance dell'impresa IT*.

www.isaca.org/knowledgecenter

offrono una varietà di opzioni flessibili; la loro impostazione e la manutenzione delle configurazioni richiede però più impegno e maggiore competenza rispetto ad altre offerte preconfezionate. D'altro lato, un elemento di flessibilità dei servizi Cloud è la possibilità di attivarli e disattivarli rapidamente, senza acquistare e vendere costose infrastrutture e software.

- **Sicurezza** – Con l'IT tradizionale, le aziende si occupano direttamente della sicurezza: il livello di protezione dei loro sistemi, chi ha accesso a essi e chi altri può (eventualmente) condividere le loro capacità di elaborazione e storage. Nel Cloud, è il fornitore del servizio a controllare molti di questi aspetti. È possibile che svolga un buon lavoro, magari migliore di quello di molte aziende, ma i clienti non hanno molta visibilità sul livello di sicurezza del proprio servizio. Inoltre, è molto probabile che i clienti Cloud condividano risorse con altre aziende, senza sapere chi siano. Per molti, questo significa ripensare profondamente le modalità di gestione della sicurezza.
- **Affidabilità e disponibilità** – Come nell'analogia di cui sopra, la promessa di servizi più affidabili e disponibili è una delle ragioni principali per cui le aziende sono attirate dal Cloud. Sebbene (almeno in teoria) i servizi Cloud siano potenzialmente più affidabili, non tutti i problemi risultano eliminati, e inoltre la visibilità dei clienti sulle cause delle interruzioni o dei problemi di affidabilità è inferiore. Anche questo richiede un diverso approccio alla governance.
- **Scalabilità** – Senza dubbio, è l'ambito in cui il Cloud Computing presenta i maggiori vantaggi rispetto all'IT tradizionale: la possibilità di adeguare rapidamente, nei due sensi, i requisiti di elaborazione e di storage, senza grandi variazioni dei costi generali. Per molte aziende, questa capacità può portare a una notevole riduzione del rischio ma, ancora una volta, le strategie di governance devono cambiare per sfruttare al massimo questo vantaggio.

Chiaramente, sia l'IT tradizionale che i servizi Cloud-based presentano pro e contro. Uno dei grandi benefici della profusione di nuovi servizi sul mercato, tuttavia, è che quasi tutte le aziende possano trarre vantaggio, attraverso la riduzione dei costi, la limitazione dei rischi o entrambe le cose, dal maggior numero di alternative disponibili. Per questo motivo, ha senso tenere d'occhio i nuovi servizi via via che emergono.

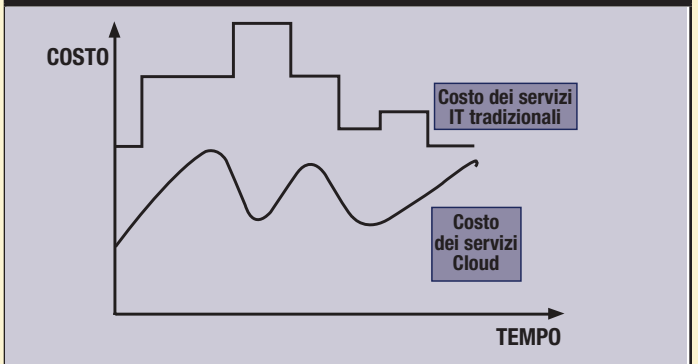
ASPETTI ECONOMICI DI BASE DEL CLOUD

Per comprendere i profili di rischio e di ritorno dei servizi Cloud, è importante comprenderne gli aspetti economici. Ecco una breve sintesi dei principi di base. In sostanza, i fornitori Cloud sono in grado di offrire servizi meno costosi rispetto ai tradizionali modelli di servizi IT, grazie a due fattori chiave:

1. Attraverso la standardizzazione e l'astrazione delle tecnologie (ad esempio, l'utilizzo di macchine virtuali), è possibile adeguare (nei due sensi) le capacità di elaborazione e storage in modo più efficiente. Questo riduce i costi derivanti dall'aggiunta e dalla rimozione dei sistemi in base al variare della domanda di servizio.
2. Attraverso la condivisione delle funzionalità IT tra più client con cicli di domanda diversi, è possibile eliminare il sottoutilizzo delle risorse. Questo riduce i costi generali associati alla capacità inutilizzata.

La figura 1 mostra come possano essere questi risparmi sui costi per un'attività con alti e bassi periodici e con una domanda di servizi IT altamente imprevedibile.

Figura 1: aspetti economici di base del Cloud



Risparmio derivante da:
- Upscaling/downscaling efficiente in base ai cambiamenti della domanda
- Riduzione della sottoutilizzazione derivante dai servizi di condivisione

Nota: i risparmi potenziali aumentano se nel Cloud vengono trasferiti più livelli IT: SaaS (Software as a Service) offre un risparmio maggiore rispetto a IaaS (Infrastructure As A Service).

Il differenziale di costo potenziale tra i due modelli è ancora maggiore quando a venire trasferiti al Cloud sono più livelli dello stack IT. Ad esempio, i risparmi sui costi del modello Software as a Service (SaaS), dove i livelli software, piattaforma e infrastruttura sono riuniti in un unico servizio Cloud, sono potenzialmente superiori rispetto al modello Infrastructure as a Service (IaaS), che include solo i livelli hardware (come storage, CPU, rete). Questo perché l'efficienza aumenta all'aumentare dei componenti standardizzati e pacchettizzati.

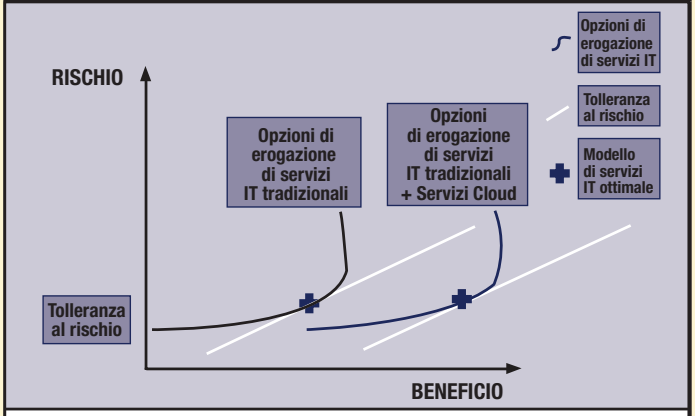
Come per l'analogia sui trasporti di prima, nessuno dei due approcci (IT tradizionale o Cloud Computing) sarà superiore all'altro in assoluto. Il Cloud Computing ha introdotto ulteriori opzioni per l'erogazione dei servizi IT. Un approccio ottimale, che sfrutti il meglio di entrambi i modelli, consentirà a molte aziende di ottenere un migliore rapporto tra rischio e beneficio. **La figura 2** illustra questo concetto.

Inoltre, nel corso del tempo, i fornitori Cloud mirano a creare risparmi sui costi ancora maggiori, con la continua acquisizione di quote di mercato maggiori e lo sfruttamento delle economie di scala.

CONDUCENTE O PASSEGGERO (O UNA COMBINAZIONE DI ENTRAMBI)?

Ma se i risparmi sui costi dalla transizione sono così attraenti, perché le aziende non trasferiscono totalmente il proprio IT nel Cloud? È un'ottima domanda, che emerge regolarmente durante i consigli di amministrazione delle aziende di tutto il mondo. Purtroppo, però, la risposta non è così semplice come potrebbe sembrare: i fattori da considerare sono numerosi, non ultimi quelli relativi alla gestione del rischio, alla conformità e alla sicurezza.

Figura 2: in che modo le opzioni Cloud possono migliorare il rapporto tra rischio e beneficio

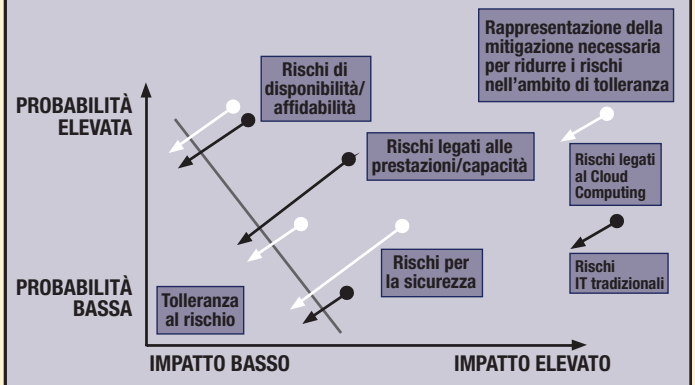


Si consideri che le opzioni di Cloud Computing possono cambiare il modello di offerta dei servizi ottimale e migliorare il rapporto rischio/beneficio.

La risposta giusta alla domanda: "Conducente o passeggero?", quindi è: "Dipende". Dipende dalla natura del servizio IT, dalle aspettative di crescita futura, dalla propensione al rischio dell'attività, dai requisiti di conformità legislativa e normativa, e dai costi. Con tutti questi fattori da considerare, è essenziale che le imprese valutino con attenzione la propria strategia di erogazione dei servizi IT e preparino un business case che tenga conto di tutti questi fattori. **La figura 3** illustra un approccio alla misurazione dei costi di riduzione del rischio, in modo che possano essere confrontati all'interno dei diversi modelli di erogazione e riportati in un business case che integri i servizi Cloud.

La figura 4 mostra alcuni esempi di strategie di erogazione dei servizi IT, che utilizzano il Cloud Computing, e alcune considerazioni essenziali.

Figura 3: creazione di un business case per il Cloud Computing



Valore attuale netto Cloud = (risparmio sul valore attuale Cloud) – (costi di mitigazione del rischio legato al Cloud) + (costi di mitigazione dei rischi IT tradizionali) – (costi di trasferimento nel Cloud)

CONSIDERARE LE OPZIONI DI CONTROLLO DEL CLOUD COMPUTING

Il Cloud Computing presenta benefici potenziali attraenti, ma porta anche con sé una serie di rischi nuovi e preoccupanti. Di seguito sono riportati i requisiti o le opportunità di controllo tipiche che le imprese potrebbero dover considerare nel valutare il passaggio al Cloud. Si tenga presente che, proprio come avviene per il Cloud, l'emersione di nuove tecnologie e tecniche è continua.

- **Un treno tutto per sé** – Per le aziende che tremano al pensiero delle loro applicazioni e dati in hosting su un server pubblico, fianco a fianco alle risorse di chissà chi altro, un Cloud privato può essere la risposta. Un Cloud privato potrebbe essere considerato l'equivalente su Internet del viaggiare in treno in uno scompartimento privato, con molti dei vantaggi del trasporto pubblico associati a una sicurezza e privacy maggiori. Una soluzione che, naturalmente, costerà di più, ma che resta potenzialmente più economica dei sistemi IT tradizionali. In generale, i Cloud privati possono essere forniti alle imprese in due modi: isolando i sistemi di business tramite firewall, o separandoli virtualmente dagli altri mediante un ambiente autenticato e crittografato all'interno di un Cloud pubblico (Cloud privato virtuale).
- **Essere pronti a tornare sui propri passi** – Un pensiero che potrebbe essere lontano nella mente dei dirigenti di business che adottano i servizi Cloud, ma che spesso rappresenta uno dei

Figura 4: strategie di erogazione dei servizi IT		
Esempi di modelli di servizi che utilizzano il Cloud Computing	**Vantaggi principali**	**Rischi principali da considerare**
1. Far funzionare l'intera applicazione di produzione utilizzando servizi PaaS o SaaS basati su Cloud pubblico, inclusi interfaccia utente, trasmissione dati, elaborazione e storage.	• Costi di supporto ed esercizio notevolmente inferiori • Servizio potenzialmente più affidabile e resiliente rispetto al modello on-premise • Riduzione dell'esposizione alle minacce specifiche del sito (ad esempio, disastri) mediante l'uso di siti distribuiti • Servizi rapidamente scalabili, come e quando richiesto • Migliore capacità di evitare rischi futuri di fine vita dell'architettura e di obsolescenza tecnologica	• Considerare piani di risposta agli incidenti e di ripristino dei servizi in caso di interruzione del servizio Cloud. • Considerare la protezione dei dati nel Cloud, ad esempio tramite crittografia. • Considerare altre misure di protezione delle risorse e dei servizi Cloud-based. • Considerare strategie per tornare alla situazione preesistente o cambiare fornitore se necessario.
2. Far funzionare l'ambiente di produzione attraverso tradizionali server di proprietà e utilizzare l'IaaS Cloud per gli ambienti di sviluppo, test e failover/ripristino.	• Riduzione dei costi di mantenimento di ambienti ridondanti utilizzati solo occasionalmente • Migliore qualità del servizio grazie alla scalabilità per test di carico e sotto sforzo e/o recupero durante i periodi di picco	• Considerare la protezione dei dati nel Cloud, quando si eseguono test con dati reali o si svolgono attività di recupero.
3. Far funzionare l'ambiente di produzione attraverso tradizionali server di proprietà e utilizzare l'IaaS Cloud per storage e CPU aggiuntivi durante i periodi di picco della domanda.	• Riduzione dei costi di mantenimento della capacità di esercizio sottoutilizzata durante periodi non di picco • Riduzione dei rischi legati alla capacità, grazie alla migliore scalabilità (nei due sensi) quando la richiesta di elaborazione di picco è superiore o inferiore al previsto	• Fare considerazioni analoghe allo scenario 1, anche se i rischi sono limitati ai periodi di picco della domanda di elaborazione.
4. Utilizzare IaaS o PaaS Cloud per sviluppare nuovi servizi durante le iterazioni dei primi rilasci, man mano che le funzioni si evolvono e la domanda si adegua.	• Maggiore flessibilità di accesso alle risorse IT man mano che i servizi si evolvono e crescono; meno preoccupazioni in relazione all'acquisizione di risorse che possono diventare ridondanti in un secondo momento	• Considerare i rischi per la sicurezza delle risorse di proprietà intellettuale (ad esempio software, algoritmi) memorizzate nel Cloud. • Considerare l'aumentato della criticità delle misure di reazione agli incidenti e di recupero con l'evoluzione dei servizi.

fattori più essenziali da considerare. Il crollo di Satyam[1] qualche anno fa dimostra che un fornitore di servizi apparentemente in buone condizioni può collassare improvvisamente, a causa di circostanze impreviste. Questo tipo di situazioni è difficile da prevedere, e ancora più difficile da prevenire: e quando ci si affida ad oscuri servizi di provider minori, l'incertezza e i rischi possono sembrare ancora maggiori. Le aziende devono sapere cosa fare se e quando un provider Cloud cessasse di fornire i propri servizi. In altre parole, hanno bisogno di una strategia di ripristino che garantisca di poter passare con facilità a un modello di servizio IT alternativo in qualsiasi momento. Questo include:

– Sapere esattamente quali risorse di elaborazione e informazioni sono presenti nel Cloud.
– Conservare competenze sufficienti (in-house o presso un fornitore indipendente dal provider) per riassumere il controllo di sistemi e servizi e ripristinarli.
– Eseguire backup periodici delle risorse critiche basate sul Cloud, presso strutture indipendenti dal provider.
– Eseguire periodicamente test di ripristino, possibilmente mediante l'esecuzione di servizi in-house o mediante un produttore indipendente per un determinato periodo (potenzialmente, anche con un altro provider Cloud).

Le strategie di ripristino costano, in tempo e in denaro, ma sono importanti per ridurre il rischio in caso di fallimento di un provider Cloud. Inoltre, mettono i clienti Cloud in una posizione molto più solida al momento di rinegoziare un contratto di servizi, perché danno la consapevolezza di poter abbandonare facilmente il provider, se necessario.

- **Tenere gli oggetti di valore sotto chiave e stare allerta –** La necessità di proteggere i dati sensibili o le risorse di proprietà intellettuale è particolarmente importante quando si utilizza un servizio di Cloud pubblico. Tipicamente, il modo migliore per proteggere queste risorse è utilizzare tecnologie di crittografia. Negli ultimi anni, la crittografia è diventata più facilmente disponibile, meno costosa e più facile da impostare, ma resta una questione complessa, con numerosi aspetti da considerare. Ecco un paio di punti chiave da non trascurare:
  – La protezione dei dati archiviati e in trasmissione nel Cloud può essere ottenuta facilmente utilizzando la crittografia, ma la protezione dei dati durante l'elaborazione nel Cloud resta problematica. Essenzialmente perché, quando i dati vengono decrittografati per l'elaborazione, sono a rischio, anche se per un tempo molto breve. Fondamentalmente, la maggior parte delle aziende che intende eseguire l'elaborazione di dati sensibili nel Cloud farebbe meglio a non utilizzare un modello di Cloud pubblico.

– La crittografia è robusta tanto quanto lo sono le pratiche usate per la gestione delle chiavi. Molte aziende hanno faticato per definire processi validi per creare, distribuire e rinnovare le chiavi di crittografia. Con il passaggio al Cloud, in cui la distribuzione delle chiavi può essere anche maggiore, rendere operativi questi processi diventa ancora più critico. Le aziende non abituate ad attuare pratiche di gestione delle chiavi farebbero bene a consultare un esperto.

Le aziende devono utilizzare la crittografia e stare allerta. Con i servizi IT tradizionali, l'impiego di tecniche di rilevamento delle intrusioni, allarmi e prevenzione è diventato comune. Ma in termini di passaggio al Cloud, molti di questi strumenti sono ora nelle mani dei fornitori del Cloud, che possono usare queste tecniche per proteggere reti e server dagli attacchi. Questo non significa, però, che i fornitori Cloud informino i clienti nel caso in cui una minaccia arrivi vicino a compromettere le loro risorse. In realtà, a meno che le aziende specifichino al provider Cloud di voler ricevere gli alert su eventi di sicurezza, il provider potrebbe supporre che i clienti non vogliano sapere.

Fortunatamente, molti fornitori Cloud offrono ai clienti la possibilità di ricevere gli alert su eventi di sicurezza, e perfino di contrassegnare le risorse specifiche che desiderano siano monitorate. Qualora si verifichi un evento di sicurezza sulla rete di un provider Cloud, le aziende potrebbero continuare a fare affidamento sul provider Cloud perché blocchi l'attacco, oppure adottare direttamente azioni evasive per proteggere le proprie risorse, ad esempio portandole offline.

NON DIMENTICARE LA LEGGE QUANDO SI VIAGGIA NEL CLOUD

Prima di impegnarsi con un fornitore Cloud, c'è un altro ambito importante che deve essere considerato: i requisiti legali e normativi. In passato (pre-Unione europea [UE]), ogni volta che un treno varcava una frontiera in Europa, funzionari governativi salivano a bordo e controllavano il passaporto dei passeggeri, prima che il treno potesse proseguire. E il fatto che i passeggeri acquistassero un biglietto per una certa destinazione non significava che avrebbero potuto raggiungerla, se privi, ad esempio, dei visti richiesti.

Nel Cloud può avvenire qualcosa di simile. Solo perché un'azienda acquista un servizio che funziona tramite vari data center nel mondo, questo non significa che l'azienda sia autorizzata a trasmettere i suoi dati in varie parti del mondo. Leggi e requisiti sulla privacy dei dati e sulla sovranità sono emersi in tutto il mondo negli ultimi decenni. Se le aziende gestiscono dati cui si applicano questi requisiti, devono muoversi nel Cloud con grande cautela, o rischiano di violarli.

La conformità con queste leggi e regolamenti può essere complessa, per la presenza di molte zone d'ombra e situazioni giuridicamente non verificate, ad esempio che cosa si intenda effettivamente con "esportazione di dati". La migliore raccomandazione è quella di ricorrere alla consulenza di un legale prima di stipulare eventuali accordi con provider Cloud, in particolare quando si opera in settori fortemente regolamentati, come i servizi finanziari o l'assistenza sanitaria, o nel caso i sistemi debbano gestire dati sensibili. In alcuni casi, le aziende potrebbero volersi consultare direttamente con gli enti regolatori (o essere tenute a farlo).

Per le aziende soggette a legislazioni rigorose sulla privacy o l'esportazione dei dati, esistono misure che è possibile applicare. Ad esempio, è possibile ricercare un fornitore Cloud che offra servizi geo-specifici, in cui le operazioni sono confinate entro determinati confini giurisdizionali.

A seconda delle circostanze, esistono molte altre aree di potenziale complessità giuridica. Ad esempio, cosa succede se si verifica un incidente nel Cloud? Il cliente ha diritto di condurre un'indagine forense? Chi sarà responsabile per gli eventuali danni? Chiaramente, ottenere una consulenza legale valida è fondamentale perché le imprese possano proteggere i propri diritti e rispettare gli obblighi loro imposti.

SCEGLIERE UN FORNITORE DI SERVIZI – TRASPARENZA E AFFIDABILITÀ

Quando per un'azienda viene il momento di iniziare a valutare i fornitori di servizi rispetto alle proprie esigenze, c'è un fattore molto importante da considerare: la trasparenza. Il Cloud Computing è molto più che un semplice acquisto di hardware o software IT. Si tratta di attivare un servizio al quale affidare la gestione di risorse e servizi critici, potenzialmente con una visibilità molto limitata sulle modalità materiali di tale gestione. Le aziende, tuttavia, possono e devono garantirsi un certo livello di trasparenza.

Con il modello IT tradizionale (on-premise o tramite una serie di accordi di outsourcing), ottenere visibilità di solito equivale a predisporre un audit, ad opera di revisori interni o di un soggetto esterno. Tuttavia, per i servizi Cloud, è molto meno probabile che questa opzione sia disponibile o praticabile, dato che le strutture di elaborazione dei provider di servizi Cloud possono essere distribuite in tutto il mondo.

Pertanto, saranno spesso necessari metodi alternativi per ottenere visibilità su sicurezza e controllo. I metodi disponibili sono diversi e, riconoscendo la necessità di guadagnare la fiducia della clientela, i provider Cloud stanno investendo sempre più per mettere a disposizione dei clienti le informazioni di cui hanno bisogno. Si tratta di un'area che è destinata a crescere ed evolvere, con la possibilità, in futuro, che venga elaborato un unico standard comune. Nel frattempo, però, ecco alcuni metodi utilizzati tipicamente dai fornitori Cloud per garantire la trasparenza. Ognuno ha pro e contro; di conseguenza, l'approccio migliore consiste spesso nel cercare la combinazione più adatta alle proprie esigenze.

- **Accordi di riservatezza** – Comprensibilmente, molti fornitori Cloud sono parecchio protettivi rispetto alle informazioni sulla propria architettura, sicurezza e controlli. Tuttavia, riconoscendo la legittima necessità del potenziale cliente di conoscere questi dati, condivideranno informazioni limitate previa sottoscrizione di un accordo di riservatezza. Se offerta, è un'alternativa che vale sicuramente la pena di considerare, perché molto probabilmente

fornirà informazioni preziose sui servizi del provider. È importante, però, tenere a mente che non è detto che sia possibile verificare queste informazioni in modo indipendente.

- **Relazioni di auditor indipendenti** – Molti fornitori di servizi oggi ingaggiano auditor indipendenti per la valutazione della progettazione e dell'esercizio dei propri controlli, e per mettere questi dati a disposizione dei clienti, sotto forma di relazioni di verifica indipendenti. A volte genericamente denominate "relazioni SAS 70", sono disponibili in una varietà di forme. Negli Stati Uniti, includono lo Statement on Auditing Standard (SAS) n. 70, le relazioni Service Organization Control (SOC) 1, SOC-2 o SOC-3, basati sugli standard dell'American Institute of Certified Public Accountants (AICPA). Esistono standard equivalenti in altre parti del mondo.[2]
- **Certificazioni** – Le relazioni di verifica indipendenti hanno sicuramente valore, ma la portata e la natura dei controlli può variare da provider a provider. Un modo per confrontare più facilmente i fornitori sono le certificazioni di settore. Tra le certificazioni più diffuse e significative:
  - Certificazioni ISO 27001 e 27002: garantiscono che il provider abbia messo in opera una serie di controlli di sicurezza, nonché implementato un sistema di pratiche di gestione per monitorare tali controlli.
  - Certificazione ISO 31000: indica che il provider ha istituito un framework e pratiche per la gestione dei rischi operativi in relazione all'erogazione dei suoi servizi chiave.
  - La conformità con il Payment Card Industry Data Security Standard (PCI DSS) implica la messa in atto da parte del provider di controlli di sicurezza sufficienti a consentire l'archiviazione, il trattamento o la trasmissione di dati delle carte di credito mediante i propri sistemi. Questo requisito è molto rigoroso e prezioso per un'azienda che desideri utilizzare un servizio per la gestione dei propri dati sensibili.

Attenzione: è importante non dare per scontata la validità di una relazione di verifica o di una certificazione senza esaminare i dettagli. È fondamentale esaminarne la finalità, l'ambito e le eventuali eccezioni principali, e valutare questi aspetti rispetto alle esigenze essenziali di conformità, gestione del rischio e controllo dell'azienda.

CONCLUSIONI

Di recente, è stata pubblicata la notizia che Dropbox avrebbe fornito ai propri clienti informazioni fuorvianti sui livelli di protezione dei dati forniti dal servizio. Questo è avvenuto poco dopo il verificarsi di gravi interruzioni del servizio Amazon EC2. Dati questi e altri episodi, sui media serpeggia il dubbio che l'età dell'innocenza del Cloud Computing sia arrivata al termine. La realtà è che, con la crescita e l'affinamento dei servizi Cloud, qualche problema lungo il percorso è inevitabile. Ma i dati economici sembrano essere validi e convincenti, e molte delle tecnologie alla base del Cloud si stanno evolvendo e diffondendo rapidamente. Sembra insomma che il Cloud Computing sia una tendenza di settore destinata a rimanere. Detto questo, la transizione verso il Cloud presenta chiaramente una serie di rischi e incertezze, e una governance e un controllo forti sono una parte essenziale di qualsiasi decisione in questa direzione.

Tuttavia, per i manager aziendali che si limitano a scorrere i titoli sui giornali o a leggere svogliatamente accattivanti materiali marketing, la strada da percorrere potrebbe essere fonte di confusione e, a volte, di preoccupazione. L'ambito Cloud presenta opportunità notevoli per i responsabili della governance e del rischio IT, in termini di formazione e guida dei propri leader di business su come cogliere i vantaggi del Cloud prendendo le dovute precauzioni. I responsabili della governance e del rischio IT possono fornire un valore eccezionale nello sviluppo di strategie che sfruttino gli innegabili vantaggi finanziari e di attenuazione del rischio del Cloud, adottando al contempo anche metodi di controllo e garanzia che consentano di prevenire tali rischi.

BIBLIOGRAFIA

Armbrust, Michael; *et al*; "Above the Clouds: A Berkeley View of Cloud Computing," University of California – Berkeley, USA, febbraio 2009

Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing v2.1*, dicembre 2009

Wright, Dave; "Selecting a Hosting Partner for Your Software Plus Services Application," Microsoft Communication Sector, agosto 2008

NOTE FINALI

[1] Kumar, Manoj; "Scandal at Satyam: Truth, Lies and Corporate Governance," India Knowledge@Wharton, gennaio 2009

[2] Un confronto valido tra le relazioni è reperibile all'indirizzo *www.aicpa.org.*