# IT Audit & Cloud

## Rischi e strategie di *assurance*

Negli ultimi anni il panorama dei servizi *cloud* appare travolto dalla rapidità dei cambiamenti tecnologici e dall'accentuarsi di una tendenza all'acquisto di tali servizi da parte delle aziende indipendentemente dalla dimensione e dal settore in cui si opera. Non si tratta di una semplice esternalizzazione di attività o servizi IT, ma di una trasformazione significativa nel business, nei processi aziendali, nel sistema di controllo interno, nelle relazioni dell'azienda con gli altri attori (esempio clienti, partner, fornitori) e altro ancora.

La trasformazione, indotta dai servizi *cloud*, pone alle aziende nuove sfide che riguardano: la contrattualistica, la scelta di adeguati servizi, la conformità a leggi e regolamenti nazionali ed internazionali (es. data privacy), la valutazione di nuovi rischi, la cyber security e altro ancora.

In tale contesto l'auditor, per poter rispondere alle aspettative dei propri *stakeholder*, deve affrontare nuove tematiche e integrarle nelle proprie attività e competenze.

Questo documento vuole essere una sintesi del contesto, dei rischi e degli approcci di auditing introdotti dal *cloud* in modo da fornire i principi generali per impostare l'attività di IT audit.

AIEA Associazione Italiana Information Systems Auditors
ISACA Capitolo di Milano

# Introduzione

Un recente studio svolto da ISACA e CSA (Cloud Security Alliance) dal titolo *Cloud Computing – Market Maturity*[1] ha evidenziato un incremento dell'utilizzo di servizi *cloud* a partire dal 2013 con tassi di crescita maggiori del 90% negli anni 2014 e 2015. Ciò richiede una attenta e costante valutazione del fenomeno interno ed esterno alla propria azienda. Tale valutazione deve essere proattiva e indurre ad affrontare le attività di IT audit con un approccio che integri le tradizionali competenze con gli aspetti specifici che derivano dal contesto e dalle caratteristiche di acquisizione ed erogazione di tali servizi.

Questo documento si propone di contribuire alla definizione e pianificazione delle attività di IT audit fornendo una panoramica sui seguenti aspetti:

- **rischi nell'utilizzo di servizi *cloud* –** identificare i rischi di natura organizzativa, tecnologici e legali;
- **termini e condizioni contrattuali –** termini e condizioni contrattuali per la regolamentazione dei servizi *cloud*;
- **strategie di *assurance* –** identificare le strategie di *assurance* che possono avere un ruolo determinante nel caso di servizi fortemente standardizzati;
- **approccio per il programma di audit –** approccio per la definizione di un programma di lavoro che tenga conto dei rischi e delle caratteristiche dei servizi *cloud*.

# Rischi nell'utilizzo di servizi *cloud*

In questa sezione sono richiamati i rischi più noti legati all'utilizzo e all'erogazione di servizi *cloud*, come rilevati da diversi osservatori ed analisti indipendenti, con l'intento di dare spunti utili a concentrare gli sforzi di *assurance* laddove tali rischi possano effettivamente avere un impatto per gli obiettivi dell'organizzazione.

Comprendere i rischi specifici dell'organizzazione e del contesto di utilizzo dei servizi *cloud* è fondamentale per applicare il principio di proporzionalità nella identificazione di controlli interni adeguati.

A questo scopo la sezione include un'elencazione dei rischi connessi al *cloud* che può essere utilizzata per individuare e valutare quelli maggiormente rilevanti nel contesto specifico dell'iniziativa di *assurance*.

## Categorie di rischio

In letteratura è possibile trovare diverse tassonomie più o meno tecniche, dettagliate ed aggiornate, di rischi e minacce nell'ambito del cosiddetto *cyber-space*. In questo ambito, evidentemente, rientra a pieno titolo il *cloud computing*, per il quale è possibile creare una vista specifica selezionando un sottoinsieme di elementi dal complesso - in continua evoluzione - di rischi *cyber*.

A questo scopo si è voluto prendere spunto da fonti autorevoli, riassumendone i contenuti in modo utile agli scopi di questo documento e dove opportuno, integrando con considerazioni frutto di esperienza diretta. Le principali fonti utilizzate sono: ENISA (*Cloud Computing: Benefits, risks and recommendations for information security*[2]), ISACA (*Managing Cloud Risk* [3]; *Cloud Computing Risk Assessment – A case study*[4]; La *Governance* IT e il *Cloud*[5]).

In linea con la categorizzazione di ENISA, sono di seguito elencati e sinteticamente descritti i rischi appartenenti alle principali tre macro-categorie:

- rischi di natura organizzativa;
- rischi tecnologici;
- rischi legali e di *compliance.*

### RISCHI DI NATURA ORGANIZZATIVA

***Lock-in –*** Rischio legato alla potenziale dipendenza da un *service provider* dovuta all'utilizzo di tecnologie e servizi IT non standard (per esempio, logiche applicative e/o schemi dati non standard) che

[1] © 2015 ISACA, Cloud Computing – Market Maturity, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/cloud-computing-market-maturity.aspx

[2] © European Network and Information Security Agency (ENISA), 2009, https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[3] Phil Zongo: "Managing Cloud Risk: Top Considerations for Business Leaders" - http://www.isaca.org/Journal/archives/2016/volume-4/Pages/managing-cloud-risk.aspx

[4] Gadia, Sailesh; "Cloud Computing Risk Assessment - A Case Study", ISACA Journal, vol. 4, 2011, http://www.isaca.org/Journal/archives/2011/Volume-4/Documents/jpdf11v4-Cloud-Computing.pdf

[5] Ron Speed, CISA, CRISC, CA: La governance IT e il Cloud: principi e pratiche per governare l'adozione del Cloud Computing, http://www.isaca.org/Journal/archives/2011/Volume-5/Pages/IT-Governance-and-the-Cloud-Principles-and-Practice-for-Governing-Adoption-of-Cloud-Computing-italian.aspx

## Cloud Computing Risk Assessment – A Case Study

Negli anni il *cloud* si è significativamente sviluppato trasformandosi da un mero termine alla moda a uno strumento rilevante con un elevato potenziale per i consumatori di prodotti e servizi tecnologici.

L'adozione del *cloud* ha accelerato negli ultimi anni e continua a subire una crescita fenomenale. Proprio come alla nascita di Internet, ci sono molte variabili sconosciute nel *cloud computing*.

A causa della sua natura nebulosa, è importante comprendere i rischi associati con l'utilizzo del *cloud*. Non è solo una nuova tecnologia; è un modo diverso di fare business.

Le aziende si stanno rendendo conto del potere del *cloud computing* e il suo uso sta crescendo. Il caso di studio presentato in questo articolo rappresenta un tentativo specifico di *risk assessment* per un accordo di *cloud computing*. Il *risk assessment* ha aiutato a scoprire alcuni dei rischi chiave, assegnare una priorità a tali rischi e definire un piano d'azione.

Data la natura in evoluzione dei rischi nel *cloud computing*, un *risk assessment* occasionale non può più essere sufficiente. Mentre nuovi rischi emergono, è necessario che il *risk assessment* evolva e l'approccio di gestione muti.

Un *risk assessment* deve essere effettuato prima che un'impresa si impegni con un accordo di *cloud computing* – per evitare sorprese e per ridurre i costi per l'implementazione e mantenimento dei controlli.

Gadia, Sailesh; "Cloud Computing Risk Assessment - A Case Study", ISACA Journal, vol. 4, 2011,

potrebbero portare ad elevati costi, in caso di cambio di *service provider* (dovuto, per esempio, ad aumento dei prezzi o ad una modifica delle policy del fornitore in contrasto con quelle dell'organizzazione). Tali costi potrebbero risultare particolarmente elevati in caso di personalizzazione spinta del servizio offerto, formazione utente specifica per l'utilizzo del servizio, vincoli contrattuali stringenti, formato dei dati difficilmente esportabili, unicità dei servizi offerti dal *service provider*, forti strategie di fidelizzazione del cliente da parte del *service provider*.

**Perdita di *governance* –** Rischio connesso alla possibile perdita di controllo sulle attività in carico al fornitore, con possibili disallineamenti con la strategia e/o con le procedure dell'organizzazione cliente (per esempio, configurazioni di sicurezza applicativa o infrastrutturale) e/o normative di riferimento (per esempio, PCI-DSS). Tali aspetti potrebbero risultare rilevanti in caso di mancanza di una struttura adeguata di *governance* all'interno dell'organizzazione e/o dell'assenza di vincoli contrattuali che disciplinino ruoli/responsabilità tra cliente e fornitore.

***Long term viability* –** Rischio connesso alla possibilità di fallimento, cambio di business, acquisizione o inadeguatezza sopraggiunta nell'erogazione dei servizi offerti da un provider, con conseguente impatto sulla continuità del business per il cliente. Tale casistica ha una probabilità maggiore nel caso di una inadeguata analisi del *service provider* in fase di selezione dello stesso.

***Supply chain failure* –** Rischio connesso alla possibilità da parte del *service provider* di esternalizzare parte del servizio oggetto del contratto, portando alla dipendenza del livello complessivo di servizio e di sicurezza da ogni singolo attore coinvolto. In generale il problema è acuito dalla mancanza di trasparenza: nei casi in cui non sussiste l'obbligo di dichiarazione/autorizzazione della subfornitura[6], una valutazione consapevole da parte del cliente non è possibile.

**Conflittualità nel funzionamento dei controlli –** Rischio connesso alla conflittualità negli obiettivi dei controlli posti in essere dal fornitore e dal cliente, qualora il *service provider* fornisca un servizio per più clienti (per esempio il blocco del traffico di rete a protezione di un cliente può limitare la visibilità dei flussi informativi per un altro). Tali aspetti potrebbero risultare rilevanti in caso di difficoltà di segregazione tecnologica tra gli ambienti gestiti dal *service provider* o in caso di organizzazioni clienti appartenenti a settori eterogenei con requisiti (ad esempio normativi) e/o servizi differenti.

**Disallineamento strategico (include *shadow IT*) –** Rischio connesso al disallineamento della strategia IT con quella aziendale. Può essere legato alla gestione di un progetto di migrazione al *cloud* con un approccio

[6] Il subappalto necessita nel nostro ordinamento di un'autorizzazione da parte dell'appaltante (art. 1656 cod. civ.) o della stazione appaltante in ambito pubblico.

guidato esclusivamente da scelte tecnologiche e IT che potrebbero non essere completamente allineate alla strategia di business. Tali scelte dovrebbero sempre essere condivise al massimo livello aziendale in modo da valutare il progetto sulla base anche degli obiettivi di business e del livello di *risk appetite* / *risk tolerance*. Altro caso di disallineamento deriva dal mancato coinvolgimento della funzione IT dell'organizzazione nel processo di selezione e gestione dei fornitori di servizi *cloud*, con impatti sulla visione globale della sicurezza informatica aziendale e sull'efficienza dei processi IT aziendali. Tale casistica può essere riscontrata con maggior probabilità in caso di mancata regolamentazione aziendale del processo di approvvigionamenti di bene e servizi IT, nonché di una *governance* IT non matura.

**Perdita di competenze interne –** Rischio connesso alla possibilità di spostamento delle competenze tecniche all'esterno dell'organizzazione con conseguente dipendenza dal *service provider* e possibile beneficio da parte di altri clienti del know-how costruito nella propria organizzazione. Tale rischio è più rilevante nel momento in cui le competenze portate all'esterno siano specifiche (p.e. relative a customizzazioni create "ad hoc", nuovi servizi non ancora presenti sul mercato).

**Indisponibilità di *log* e *audit trail* –** Rischio connesso alla difficoltà di ottenere log relativi al funzionamento dei sistemi o applicazioni in *cloud* in quanto, spesso le difficoltà tecniche di segregazione dei log per cliente (in particolare in caso di piattaforme *multi-tenant*) e/o i costi relativi sono considerati eccessivi per il *service provider*.

## RISCHI DI NATURA TECNOLOGICA[7]

**Esaurimento delle risorse –** La natura *on demand* o *just in time* self service dei servizi *cloud*, unita alla condivisione delle risorse, caratteristica *by design* del *cloud computing*, porta con sé il rischio di esaurimento delle risorse stesse.

Tale rischio può derivare da un approccio di utilizzo delle risorse basato su modelli statistici inadeguati, da un errato capacity plan o da insufficienti investimenti in ambito infrastrutturale. Alcune conseguenze possono essere:

- indisponibilità dei servizi;
- compromissione dei sistemi di controllo accessi[8];
- perdite economiche e di reputazione;
- sovradimensionamenti infrastrutturali (con conseguenti perdite di profitto) [9];
- mancato rispetto degli SLA dei clienti.

***Isolation failure –*** La condivisione delle risorse e l'architettura *multi-tenancy* sono due caratteristiche intrinseche del *cloud computing*.

La capacità di calcolo, lo storage e le risorse di rete sono condivise fra tutti gli utenti; ciò porta con sé il rischio di assenza o fallimento dei meccanismi di separazione di *storage, routing*, memoria, *virtual machine* fra differenti *tenants* (*guest hopping*, *guest breakout*, *side channel attack*, ecc.) e la possibilità che i clienti possano accedere ad informazioni non di loro appartenenza.

Ad esempio, con riferimento anche al rischio legato alla compromissione del *service engine* (*hypervisor*), in una architettura IaaS è possibile eludere i controlli di isolamento degli ambienti fra i diversi clienti di un provider e guadagnare accesso ai dati contenuti, modificare l'assegnazione delle risorse, provocare DoS, ecc..

***Malicious insider –*** Le architetture *cloud* necessitano di ruoli con alto rischio operativo e gestionale (*Cloud Administrator*, *Cloud Application Architect*, *Cloud Data Architect*, *Cloud Storage Administrator*, ecc.).

Operatori non affidabili in possesso di questi profili possono facilmente minare la confidenzialità, l'integrità e la disponibilità dell'intera infrastruttura (dati, servizi, IP, ecc.) e colpire indirettamente la reputazione dell'organizzazione oltre che indebolire la fiducia che i clienti ripongono nel *service provider*.

**Compromissione della *management interface* –** Le interfacce di gestione dei *public cloud*, che mediano l'accesso a un esteso set di risorse, sono accessibili via Internet dagli amministratori dei *provider* per gestire l'intero sistema *cloud*, e dai clienti per manutenere e controllare le loro *virtual machine*. Gli accessi svolti da remoto assieme alle vulnerabilità intrinseche dei *web*

[7] Nel *cloud computing* la componente tecnologica è governata e gestita dal *service provider*. Tuttavia i rischi che incombono sulla gestione di tale componente hanno impatto sulle attività del cliente dei servizi.

[8] In alcuni casi può essere possibile forzare i sistemi in modalità "*fail-open*" al verificarsi di esaurimento delle risorse. In questa modalità i meccanismi di controllo non agiscono sui flussi dati.

[9] È la conseguenza opposta all'esaurimento di risorse, comunque dovuta a stime non accurate delle capacità necessarie.

*browser* accrescono il rischio di compromissione di tutte le interfacce di management.

***Intercepting data in transit –*** Un'architettura distribuita come quella *cloud* implica la necessità di avere più dati in transito rispetto ad architetture più tradizionali[10].

Ogni volta che i dati vengono trasferiti tra computer o siti diversi, vi è la possibilità che i dati in transito possano essere intercettati. *Sniffing*, *spoofing*, *man-in–the-middle attack*, *side channel* e *replay attack* e altre tipologie di attacco che hanno l'obiettivo di catturare il traffico dati devono quindi essere considerati come possibili minacce.

**Non corretta cancellazione dei dati –** L'eliminazione dei dati dallo *storage* di un *cloud* non significa che i dati siano rimossi effettivamente dai dischi o da eventuali altri supporti di backup. Se i dati nello *storage* non sono stati salvati in maniera cifrata o se non sono state messe in campo particolari procedure di cancellazione sicura dei dati (*wiping)*, questi potrebbero essere accessibili da altri clienti del *service provider*.

***Distributed Denial of Service* (DDoS) –** Gli attacchi DDoS hanno l'obiettivo di sovraccaricare una risorsa inondandola di richieste provenienti da diverse fonti distribuite in vaste area geografiche impedendo agli utenti legittimi di utilizzare la risorsa.

Un attacco DDoS indirizzato ad un fornitore di servizi *cloud* o a un suo cliente può avere effetti amplificati, estesi a tutte le organizzazioni clienti del *provider*.

**Compromissione *Service Engine*[11] –** La compromissione del *software* che gestisce l'ambiente *cloud* darà la possibilità a un utente malintenzionato di accedere ai dati di tutti i clienti del *provider*, con una conseguente potenziale violazione dei requisiti di confidenzialità, integrità o disponibilità.

Alcuni esempi di compromissione di un *hypervisor*:

- *guest breakout*: elusione del perimetro di un sistema operativo *guest* (S.O. virtuale ospitato sulla macchina fisica *host - hypervisor*) e conseguente accesso ad altri *guest* e all'*hypervisor* stesso;
- *violazione delle snapshot*: spesso le *snapshot*[12], utilizzate per costruire ambienti di test, di collaudo o semplicemente per backup, possono contenere dati che necessitano di trattamento appropriato (ad esempio, dati personali, dati sanitari, ecc.);
- *sprawl*: proliferazione di VM/istanze *cloud* senza adeguato controllo. Porta all'uso incontrollato di risorse con conseguente aumento di costi per l'organizzazione.

**Perdita back-up –** Questo rischio è analogo a quello comunemente noto per le tradizionali architetture IT.

I back-up dei dati/informazioni dei clienti possono essere persi e/o danneggiati. Inoltre i supporti fisici su cui i dati sono conservati possono essere indebitamente sottratti.

**Problemi di network –** Il *cloud* soffre degli stessi problemi legati alla rete di cui soffrono le tradizionali architetture IT. Ad esempio perdite di connettività, riduzioni di banda, problemi di *routing*. Se la rete è indisponibile o non presenta un'adeguata affidabilità (rete di back-up) il *cloud* potrebbe non essere la soluzione ideale.

**Perdita chiavi di crittografia –** La perdita o la compromissione delle chiavi di crittografia utilizzate per la cifratura, l'autenticazione o la firma digitale può portare alla perdita di dati, alla negazione dei servizi, o a danni finanziari.

Il rischio in esame include la *disclosure* di chiavi segrete (SSL, chiavi private dei clienti, ecc.), la perdita o il danneggiamento di quelle chiavi, o il loro uso non autorizzato per l'autenticazione e non ripudio (firma digitale).

**User Identity Federation –** È molto importante per le organizzazioni mantenere il controllo sulle identità degli utenti che si muovono fra servizi e applicazioni di diversi *cloud provider*. Il rischio è quello di concedere che ogni *provider* crei delle "isole" di identità rendendo molto complessa la loro gestione. Gli utenti dovrebbero essere identificabili in maniera univoca con un autenticazione federata (ad esempio *Security Assertion Mark-up Language*) fra i diversi *cloud provider*.

[10] Per esempio i dati devono essere trasferiti per aggiornare le immagini delle *virtual machine*, per necessità di *failover*, per il *live migration* di VM fra *hypervisor* in cluster, per consentire la gestione da remoto dell'infrastruttura *cloud* mediante web browser, ecc..

[11] Il *service engine* è un elemento fondamentale di un servizio *cloud*. Esso, in generale, rappresenta uno strato software che gestisce le risorse dei clienti a diversi livelli di astrazione. Ad esempio nel modello di servizio IaaS il *service engine* è rappresentato da un *hypervisor*, macchina (Host) contenente virtual machines.

[12] Una *snapshot* è un'istantanea dei dati sul disco di un sistema in un particolare momento.

Di contro, l'utilizzo di *Social Identity Federation*, oggi sempre più diffuso per facilitare l'adesione da parte degli utenti a nuovi servizi ("*usa il tuo account Facebook/Linkedin/Google per accedere a servizi di business*"), deve essere attentamente valutata (la violazione di un *account* "social" può portare alla compromissione di servizi di business).

## RISCHI LEGALI E DI *COMPLIANCE*

**E-Discovery –** In caso di procedimenti in ambito giudiziario, le autorità competenti potrebbero richiedere ai gestori di infrastrutture IT di fornire informazioni rilevanti, anche attraverso la consegna, quali evidenze, di elementi fisici (*media storage*,hardware ecc.). La condivisione delle risorse hardware ed infrastrutturali tra più organizzazioni, tipica delle soluzioni *cloud*, può implicare il coinvolgimento, in modo indiretto, di un cliente in procedimenti riguardanti terze parti o lo stesso *cloud provider*.

Perciò, in caso di sequestro di elementi infrastrutturali (hardware, ecc.), la centralizzazione dell'archiviazione dei dati presso il *cloud provider* implica il fatto che molteplici clienti corrano il rischio di subire una divulgazione involontaria delle proprie informazioni a terze parti.

**Problemi di giurisdizione –** Quando i dati sono conservati o trattati in un *data center* situato in un Paese diverso da quello del cliente dei servizi *cloud*, eventuali cambiamenti nella giurisdizione possono influire anche in modo significativo sulla sicurezza delle informazioni. Tale rischio è considerevolmente maggiore nelle soluzioni cloud, poiché potrebbero essere potenzialmente coinvolte un grande numero di giurisdizioni di Paesi diversi.

Inoltre i dati di un cliente potrebbero contemporaneamente risiedere in più Paesi, alcuni dei quali con giurisdizioni in termini di sicurezza delle informazioni non sufficientemente mature oppure con problemi di instabilità socio-politica con conseguente aumento del rischio di perdita, compromissione o divulgazione delle informazioni stesse.

Per tale ragione, in fase di definizione contrattuale, l'organizzazione deve prestare particolare attenzione alla locazione dei *data center* del *cloud provider* ed alla valutazione dei livelli di maturità delle giurisdizioni in materia.

**Data Protection –** Il trattamento dei dati in un determinato Paese potrebbe non essere effettuato in modo conforme con la legislazione in materia o potrebbe addirittura essere considerato illegale da parte delle autorità responsabili della protezione dei dati. La probabilità di incorrere nel rischio in questione è maggiore nelle soluzioni *cloud* considerando che il *cloud provider* potrebbe, se non diversamente normato, trasferire dati tra *data center* situati in Paesi diversi senza neppure comunicarlo alle organizzazioni clienti.

Le conseguenze legate al rischio in esame potrebbero comportare, per il cliente, la difficoltà se non addirittura l'impossibilità di mantenere il controllo sulle modalità di trattamento dei propri dati e di verificarne la conformità rispetto alla legislazione in materia, la cui responsabilità (ad esempio nel caso di dati personali) rimane comunque in carico all'organizzazione.

***Licensing* –** La comprensione delle logiche e metriche di *licensing* è materia già complessa e l'avvento di nuovi paradigmi di utilizzo del software come il *cloud* pone nuovi rischi a cui far fronte.

Spesso gli accordi di licenza software restano vaghi rispetto all'uso in ambienti *cloud*. Le licenze possono basarsi sul numero di utenti, nominali o concorrenti; o sul numero di processori o core, sui quali il software può girare; o ancora sull'utilizzo del software, indipendentemente dal numero di utenti. Nel caso del *cloud*, soprattutto con servizi di tipo IaaS o PaaS, questi parametri possono essere visti dal vendor come un'espansione rispetto all'uso interno con conseguente aumento dei costi o, almeno, aumento della complessità di calcolo e rischi di violazione dei contratti.

Le violazioni degli accordi di licenza di un fornitore di software possono comportare sia sanzioni finanziarie rilevanti che interruzioni di servizio. La stima di tale impatto è essenzialmente la medesima sia per le architetture *cloud* che per le tradizionali architetture IT.

**Proprietà intellettuale –** Nel *cloud*, come in tutti gli altri ambienti di sviluppo all'interno della propria organizzazione, è possibile che si sviluppino nuovi software e/o applicazioni frutto dell'inventiva e del genio delle risorse impiegate. Tale proprietà intellettuale, se non protetta da appropriate clausole contrattuali può essere esposta a rischio di violazione. Ovviamente, per le caratteristiche dell'architettura *cloud*, la probabilità di incorrere in tali violazioni è sicuramente maggiore rispetto alle tradizionali architetture IT.

In tale ottica, prima di avvalersi di soluzioni *cloud*, devono essere valutati attentamente i rischi connessi, analizzando attentamente tutte le clausole contrattuali

al fine di determinare se il cloud provider offra sufficienti garanzie di protezione delle proprietà intellettuali. È consigliabile che i diritti di proprietà intellettuale siano regolati attraverso clausole contrattuali dedicate all'interno del contratto.

**Rischi di *compliance* –** La natura dei servizi *cloud* porta ad avere frammenti di record distribuiti in centri di calcolo diversi in vari Paesi. Questo può rappresentare un problema soprattutto per l'adempimento ad obblighi legali e a regolamenti nazionali ove il servizio viene fornito. Il rischio è legato in particolar modo all'accesso a dati personali da parte di persone non autorizzate, alla protezione di identità e credenziali digitali, alla conservazione dei dati, ai tempi di retention e alle condizioni che stabiliscono il ruolo delle terze parti. Talvolta tali rischi tendono ad aggravarsi quando le società che usufruiscono di servizi di *cloud computing* sono poco consapevoli del fatto che l'obbligo primario di rispettare le disposizioni in materia di protezione dei dati incombe in primo luogo su di loro e non sul fornitore di servizi che memorizza e gestisce i dati su un server in *cloud*, portando così a sottovalutare i rischi legati alla *compliance* e le relative conseguenze.

## Termini e condizioni contrattuali

Nella valutazione del profilo di rischio e di controllo di ciascun contesto specifico, molto rilevanti sono le condizioni contrattuali che il fornitore è disposto ad accettare mentre, d'altra parte, è necessario considerare l'esigenza del cloud provider, specie se multinazionale, di garantire uniformità ai termini ed alle condizioni contrattuali.

Occorrerà, quindi, tenere in considerazione gli obiettivi fondamentali per il cliente, riservando un ruolo centrale al requisito della trasparenza, che – indipendentemente dall'equilibrio del sinallagma contrattuale, ovvero della corretta allocazione di rischi e responsabilità – consente alle parti, sin dal momento della conclusione del contratto, di avere un quadro preciso dei rispettivi diritti ed obbligazioni e di evitare così possibili rischi occulti.

> Il requisito della trasparenza consente alle parti di avere un quadro preciso dei rispettivi diritti ed obbligazioni evitando possibili rischi occulti.

Naturalmente – come in ogni relazione contrattuale – la possibilità di ottenere modifiche sostanziali ai termini ed alle condizioni contrattuali proposte dal *cloud provider* e, a maggior ragione, la possibilità di imporre le proprie condizioni contrattuali saranno strettamente connesse al potere negoziale delle parti: potere negoziale che, oggi, nei confronti dei cosiddetti *Over The Top* (Google, Amazon, Microsoft, ecc.) è tendenzialmente basso.

Infine, un importante aspetto di cui tener conto è la cornice normativa e legale in cui sarà collocato il contratto di fornitura con particolare riferimento alla legge applicabile al contratto ed al foro competente.

### Termini e condizioni caratteristiche per normare i servizi *cloud*

**Legge Applicabile –** La legge applicabile è l'insieme di norme alle quali il contratto deve conformarsi. La legge applicabile al contratto ha un'importanza fondamentale e si riverbera sulla validità (o meno) di molte altre clausole del contratto. La cosa più ragionevole è quella di scegliere un *provider* che abbia indicato come legge applicabile una coerente con le normative 'affini' al cliente.

**Giurisdizione / Arbitrato –** La giurisdizione è l'attività, svolta dai giudici, con la quale lo Stato dirime le controversie. La clausola sul foro competente ha un impatto economico notevole.

Pertanto, soprattutto nel caso di clienti corporate, la cosa più opportuna è scegliere un fornitore che abbia indicato come foro competente quello di un Paese in cui l'organizzazione cliente abbia la possibilità di agire (in modo economicamente conveniente).

Nell'accettare clausole arbitrali, oltre alle considerazioni svolte per il foro competente, occorre inoltre sempre tenere conto del trade-off, che le procedure arbitrali presentano, tra rapidità della procedura e costo della stessa.

**Uso accettabile del servizio / Violazioni contrattuali –** Clausole per regolamentare che il servizio sarà utilizzato dal fruitore per gli scopi ed i fini indicati nel contratto. È consigliabile verificare il contenuto di tale clausola, ove presente, per accertarsi che gli usi non consentiti (ma non per ciò stesso illeciti) non coincidano anche solo parzialmente con gli usi che l'organizzazione intende fare e per accertarsi che alla condizione sugli usi consentiti non siano associate clausole di manleva particolarmente gravose.

**Sicurezza –** Le clausole concernenti la sicurezza regolamentano il processo volto alla protezione (da atti

dolosi, colposi o accidentali) delle informazioni affidate dal fruitore del servizio, per evitarne la perdita di integrità e riservatezza dell'informazione.

Su questo ambito si segnala l'importanza alla adozione di opportuni controlli volti al presidio di integrità e riservatezza dei dati, quali ad esempio back-up periodici ed automatici, meccanismi di protezione all'accesso ai dati, ecc..

La riservatezza dei dati è un aspetto di fondamentale importanza per numerose ragioni, tra cui:

- garantire la *compliance* del trattamento dei dati personali rispetto alla normativa in materia di *privacy*;
- assicurare il rispetto di obblighi contrattuali di riservatezza che il cliente abbia assunto con riferimento a soggetti terzi e mettere il cliente stesso al riparo da responsabilità risarcitoria;
- preservare la proprietà intellettuale dell'organizzazione (con riferimento, ad esempio, alle informazioni aziendali segrete - *know how* - e ad eventuali innovazioni brevettabili).

In tal senso è bene acquisire servizi *cloud* da quei fornitori che si impegnino espressamente a garantire la riservatezza dei dati e, in caso di *data breach*, la opportuna e tempestiva notificazione all'organizzazione cliente.

Quando si selezionino dei *provider* che non assumono specifiche obbligazioni sui punti sopra indicati è consigliabile procedere alla cifratura dei dati e a frequenti back up.

**Privacy –** Le clausole relative alla *privacy* regolamentano il controllo e la gestione delle informazioni afferenti i dati personali di un soggetto.

Su questo, si prendano come riferimento i seguenti punti:

- *compliance* con la Normativa Europea sulla *Privacy* sia in relazione al trattamento del dato che al suo trasferimento (all'interno dei paesi dell'UE o extra-UE);
- inserimento delle clausole contrattuali standard (*EU Model Clauses*) definite dall'Unione Europea.

**Riconsegna e successiva cancellazione dei dati –** Queste clausole regolamentano l'obbligo del fornitore, al termine del servizio, che i dati affidatigli dall'organizzazione cliente vengano reimmessi nella disponibilità di quest'ultimo e la successiva cancellazione degli stessi in tempi certi e/o stabiliti da regolamentazioni.

Gli interessi del cliente, in questo ambito, sono almeno due:

- avere la garanzia della disponibilità dei dati per un certo periodo di tempo dopo la risoluzione del contratto;
- avere la garanzia che, trascorso tale periodo di tempo, i dati verranno definitivamente cancellati.

**Portabilità dei dati –** Queste clausole regolamentano l'obbligo del fornitore, anche durante l'espletamento del servizio, di mettere a disposizione del cliente, su sua richiesta, i dati in formato intellegibile secondo lo standard concordato.

**Proprietà intellettuale –** È opportuno verificare che il contratto preveda espressamente che la titolarità dei diritti di proprietà intellettuale (diritti d'autore, diritti connessi al diritto d'autore, diritto sui generis del costitutore della banca dati) appartiene all'organizzazione cliente (o – almeno – che non sia stabilito il contrario).

**Accessibilità da parte di terze parti –** Questa clausola definisce le modalità di accesso ai dati del cliente da terze parti, in particolare:

- l'accesso ai dati da parte del fornitore solo per gli usi concordati e funzionali all'erogazione del servizio;
- l'accesso ai dati da parte di terze parti deve essere subordinato all'approvazione del cliente.

Sono consentiti gli accessi per rispondere ad ordinanze delle Autorità Giudiziaria.

**Luogo in cui vengono memorizzati i dati –** La normativa in materia di trasferimento all'estero dei dati personali rende particolarmente critico il profilo del luogo in cui sono memorizzati i dati. Occorre dunque fare attenzione alle clausole contrattuali relative all'eventuale collocazione dei server e al trasferimento dei dati da parte del *cloud provider*.

In particolare è opportuno preferire quei *cloud provider* che, alternativamente: ospitano i dati su server collocati all'interno di Stati UE, ospitano i dati su server collocati in Paesi extra UE che garantiscono un livello di protezione dei dati adeguato, fanno ricorso alle clausole contrattuali standard approvate dalla Commissione

europea (cfr. da ultimo le decisioni della Commissione europea 2004/915/CE e 2010/87/UE).

### Altri termini e servizi

**Diritto di Audit diretto o di terze parti –** Il diritto di effettuare un audit è chiaramente definito e copre le esigenze del cliente (Consiglio di Amministrazione, revisione esterna, ecc.). Questo diritto può essere esercitato, se convenuto nel contratto, in modalità diretta tramite l'esecuzione di revisioni/audit a carico dell'organizzazione cliente. In alternativa, il fornitore deve sottoporsi a revisione da parte di opportune società terze in modo da ottenere una certificazione standard sul corretto funzionamento del proprio sistema di controllo.

**Certificazione standard –** Strumento attraverso il quale un *service provider* fornisce ai suoi clienti una *assurance* sull'adeguato funzionamento del proprio sistema di controllo (ad esempio ISO27001 oppure la più recente ISO27018, primo Standard Internazionale elaborato specificamente per i fornitori di servizi di servizi di *public cloud* che operano come responsabili esterni del trattamento). Il *provider* dovrà fornire delle attestazioni tramite report quali SOC 1 Tipo II e SOC 2.

**Limiti alla capacità del *provider* di modificare i termini del contratto –** Le parti possono determinare contrattualmente la possibilità di modificare, anche unilateralmente, alcune condizioni contrattuali. Al netto di ogni considerazione circa la validità di tali clausole, è consigliabile preferire quei fornitori che, pur riservandosi il diritto di modificare le condizioni contrattuali, prevedano (almeno) obblighi di notificazione nei confronti del cliente e gli riconoscano il diritto di recedere dal contratto al fine di evitare che tali modifiche vengono considerate accettate per fatti concludenti (ad es. il continuare ad usare il servizio).

**Responsabilità del cliente e risarcimenti / Responsabilità del fornitore e risarcimenti –** La violazione degli obblighi contrattuali comporta la responsabilità del soggetto inadempiente. Qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.

L'atteggiamento corretto da tenere in caso di clausole di esclusione o limitazione della responsabilità è:

- verificare la validità delle clausole in questione rispetto alla legge applicabile al contratto;
- scegliere i *provider* che offrono maggiori garanzie contrattuali;
- scegliere in ogni caso i *provider* che offrano maggiori garanzie patrimoniali;
- valutare l'opportunità di protezioni esterne (assicurazioni).

***Service Level Agreements –*** L'assunzione, da parte del provider, di specifici obblighi sugli standard di servizio, sulla *business continuity* e sul *disaster recovery*, sono fondamentali per le organizzazioni che ricorrono a servizi *cloud* per gestire dati critici e/o per fornire servizi in *real-time*. L'assunzione di obblighi specifici da parte del *provider* può essere considerato come uno dei principali indici di affidabilità del fornitore.

Il contratto dovrebbe normare:

- le modalità di calcolo degli SLA;
- il processo di reporting periodico nei confronti del cliente.

## Strategie di assurance

### Assurance interna

L'adozione di un servizio *cloud* da parte di un'organizzazione è caratterizzata, come qualsiasi altro servizio, da un ciclo di vita e prassi specifiche per ogni fase. Lo standard ***eSCM***[13] suddivide le prassi nelle fasi: *Ongoing*, *Analysis*, *Initiation*, *Delivery* e *Completion*.

Senza entrare nel dettaglio delle prassi, ampiamente ed in modo molto più esauriente descritte nello standard, si vuole qui suggerire il ricorso a *best practice* codificate e consolidate per sviluppare una **strategia di assurance**. Oltre ad *eSCM*, sono diverse le pubblicazioni di ISACA e di altri autorevoli *advisor* ed osservatori, sull'argomento.

Un fattore comune a standard e *best practice*, per la prospettiva dell'internal audit, è il focus sui processi di governance della propria organizzazione. Laddove diminuiscono le possibilità di svolgere audit diretti sui service provider, sempre meno inclini a lasciarsi visitare, per ovvie ragioni di sovraccarico ispettivo, più che di poca trasparenza, è sana preoccupazione dell'audit interno assicurarsi che un'iniziativa *cloud* sia

[13] eSourcing Capability Model for Service Providers, sviluppato dal ITSqc, un gruppo di ricercatori della Carnegie Mellon University. http://www.itsqc.org/models/escm-sp/ .

correttamente indirizzata e controllata o, in una parola, governata.

> Fattore comune, per la prospettiva dell'*Internal Audit*, è il focus sui processi di *governance* della propria organizzazione.

Cosa deve intendersi per *governance* di un'iniziativa *cloud*? Qui tornano utili gli standard di cui sopra per richiamare alcune delle prerogative basilari della *governance* di un servizio in *cloud*:

- definizione delle strategie di *sourcing*;
- definizione delle *policy* di *sourcing*;
- definizione del modello di *governance*, organizzazione, ruoli, responsabilità;
- selezione dei *provider*;
- allineamento di strategie ed architetture, gestione dei cambiamenti di business;
- gestione delle relazioni e interazioni con i *provider* (in modo da promuovere collaborazione ed innovazione) e con gli *stakeholder* interni;
- valutazione delle performance (rispetto a *benchmark* di mercato);
- continuo miglioramento e cultura dell'innovazione;
- *change management* (per supportare l'adozione di nuovi modelli operativi e tecnologici);
- gestione dei rischi (*sourcing*, IP, *security & privacy*, *compliance*, continuità operativa, ecc.);
- documentazione dei requisiti di servizio;
- gestione dei contratti, SLA;
- gestione della transizione;
- gestione operativa del servizio (monitoraggio, gestione finanziaria, gestione degli incidenti e dei problemi, gestione dei cambiamenti);
- chiusura del servizio (*Knowledge* / *people transfer*).

L'importanza relativa di tali prerogative e delle relative attività pratiche non è predeterminabile e dipende dal contesto e dagli obiettivi che si intende perseguire con l'iniziativa *cloud*.

Tuttavia va tenuto presente che il *cloud*, quando riguarda servizi applicativi di business (come diversi servizi SaaS) che non richiedono competenze specifiche, può prescindere dal coinvolgimento della struttura IT, come di qualsiasi struttura aziendale predefinita; questo comporta la impellenza di chiare *policy* di *sourcing* atte a prevenire situazioni "fuori controllo", a disciplinare, se non altro, il flusso autorizzativo di un servizio *cloud* e a promuovere un modello sostenibile.

L'iniziativa *cloud* non può prescindere dalle strategie IT in quanto componente delle strategie aziendali. Obiettivi, benefici, vincoli e rischi devono trovare riscontro in un *business case*, più o meno formalizzato, condiviso e sostenuto dal vertice aziendale. Resta quindi imprescindibile una chiara espressione degli **obiettivi** insieme alla valutazione dei rischi del progetto, a partire dalla classificazione delle informazioni che resterebbero esternalizzate nel *cloud*. Insieme a policy, obiettivi definiti, strategie condivise, il **modello di governance**, con responsabilità e competenze ben delineate, completa il quadro in cui si inserisce ed opera l'attività di *assurance* interna.

## Assurance esterna

L'indisponibilità dei fornitori di servizi a subire attività di audit condotte da parte delle numerose organizzazioni clienti e, in alcuni casi, la mancanza o scarsità di competenze interne per condurre attività di verifica su tali servizi, possono essere ovviate attraverso il ricorso a certificazioni esterne.

> I fornitori di servizi *cloud* ricorrono ad una attestazione di terza parte sull'adeguatezza del proprio sistema di controllo interno come *assurance* da fornire ai propri Clienti.

I fornitori di servizi *cloud* ricorrono sempre più spesso all'ottenimento di certificazioni riconosciute a livello internazionale rilasciate da terze parti indipendenti, da poter utilizzare nei confronti dei propri clienti quale attestato sull'adeguatezza del sistema di controllo interno adottato.

In tale contesto, lo standard maggiormente diffuso, riconosciuto ed utilizzato per la valutazione del sistema di controllo interno di un fornitore di servizi *cloud*, pur non essendo stato sviluppato specificatamente per tale

contesto, è lo standard **ISAE 3402**[14]. Tale standard ha sostituito il SAS70 a partire dal 15 giugno 2011, passando da uno standard di tipo 'americano' (SAS70) ad uno standard 'internazionale' (ISAE 3402), conferendone dunque una valenza e significatività maggiori rispetto al precedente.

L'attestazione ISAE 3402 è la valutazione del sistema di controllo interno della *Service Organization* (ad esempio un fornitore dei servizi *cloud* ) che eroga servizi, prevalentemente in ambito IT, alla *User Organization* (fruitore dei servizi offerti dalla *Service Organization*) ed è rilasciata, su mandato della *Service Organization* stessa, da *Auditor Indipendenti* per poterla utilizzare nei confronti della *User Organization* e dei suoi rispettivi *Auditor*.

In particolare il report di attestazione *Service Organization Control* (SOC) è un report analitico di terza parte che documenta come la *Service Organization* abbia raggiunto obiettivi e adottato controlli di conformità ottimali. Lo scopo di questo report è di aiutare le *User Organization*, e le loro entità di controllo, a raccogliere informazioni sui controlli creati dalla *Service Organization* per supportare operatività e conformità.

Lo standard definisce tre tipologie di report di *assurance*:

- **SOC 1**:
  - tipologia di attestazione e focalizzazione limitata ai controlli relativi all'**informativa finanziaria**;
  - obiettivi e attività di controllo definiti dalla *Service Organization*;
  - utilizzo del report rivolto e **limitato alla *User Organization*** che usufruisce dei servizi;
  - adatto ad organizzazioni che erogano servizi di tipo amministrativo e finanziari (esempio *payroll*, *corporate banking* ecc.);
- **SOC 2**:
  - focalizzazione sulle tematiche di **sicurezza, disponibilità, integrità, confidenzialità e *privacy*** (*Trusted Services Principles – TSP*) relativamente ad uno specifico sistema;
  - obiettivi di controllo predefiniti relativi agli ambiti sopraccitati;
  - utilizzo del report rivolto e **limitato alla *User Organization*** che usufruisce dei servizi;
  - applicabilità estesa ai processi IT;
- **SOC 3**:
  - focalizzazione sulle tematiche di **sicurezza, disponibilità, integrità, confidenzialità e *privacy*** relativamente ad uno specifico sistema;
  - report di sintesi dei risultati (non include il livello di dettaglio del report SOC 2) **adatto alla distribuzione a terze parti** o pubblicazione sul sito web della *Service Organization* senza particolari restrizioni.

Per ciascun report, sono definite due distinte tipologie:

- ***type 1***: fornisce informazione relativamente a livello di **disegno dei controlli** in essere ad una certa data;
- ***type 2***: fornisce evidenze in merito all'**operatività dei controlli** a seguito delle attività di verifica eseguite per un determinato periodo temporale.

Il report SOC 2 *Type 2* risulta lo strumento più adeguato e completo di *assurance* per le organizzazioni che forniscono servizi *cloud*

Normalmente la validità del report SOC è annuale ma può essere richiesta dalla *Service Organization* una attestazione semestrale.
La *Service Organization* mette a disposizione il report SOC alla *User Organization* e a sua volta non lo può distribuire ad altre entità.

Nell'ambito della certificazione, la *Service Organization* è responsabile della scelta delle aree (TSP) oggetto dell'attestazione da parte della terza parte indipendente. Periodicamente l'AICPA (American Institute of Certified Public Accountants) pubblica una versione aggiornata dei *Trust Service Principles*[15] al fine di contemplare le recenti evoluzioni nell'erogazione dei servizi IT.

[14] International Standard on assurance Engagements (ISAE) 3402, emesso nel dicembre 2009 dall'International Auditing and Assurance Standards Board ("IAASB"). http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf.

[15] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/TrustDataIntegrityTaskForce.aspx

Sulla base delle valutazioni in merito all'ambito delle attività di verifica, alle tematiche oggetto delle attività di verifica e al livello di dettaglio delle informazioni riportati all'interno dei report, il report SOC 2 Type 2 risulta ad oggi lo strumento più adeguato e completo di *assurance* delle *Service Organization* che erogano servizi *cloud;* ciò è confermato dal fatto che CSA (Cloud Security Association) e AICPA collaborano costantemente per allineare la *Cloud Security Matrix* (CSM) ed i criteri *Trust Service Principles* utilizzati per le verifiche in ambito SOC 2.

# Approccio per la definizione di un programma di audit

L'ultima sezione di questo documento si pone l'obiettivo di fornire indicazioni per migliorare l'approccio alla definizione di un programma di audit sui servizi *cloud* acquisiti da un'organizzazione.

In particolare ISACA definisce l'*assurance* come un "*esame obiettivo di una evidenza allo scopo di fornire una valutazione sulla gestione del rischio, sui processi di controllo o governance per l'organizzazione*" [16].

Sposando questa definizione, ogni azienda, prima di perseguire la decisione di rilasciare un servizio *cloud* o di utilizzare il *cloud computing*, dovrebbe implementare adeguati meccanismi di *assurance*.

In tale contesto ISACA ha sviluppato l'*IT Assurance Framework* (ITAF[17]) che rappresenta un modello e una raccolta completa delle *best practice* di *assurance*.

La sezione riguardante i rischi del *cloud computing* fa diretto riferimento a tale framework.

Uno degli obiettivi principali che si pone questa sezione è quello di definire con cura gli ambiti di audit al fine di intercettare per intero l'insieme dei rischi legati all'utilizzo e all'erogazione di servizi in *cloud*.

Così facendo si vuole fornire una "mappa" sintetica e veloce per implementare un programma di audit "tessuto" su misura per le proprie esigenze specifiche.

## Macro-ambiti di audit

In merito all'argomento trattato in questa sezione è disponibile una vasta bibliografia. Ogni pubblicazione fornisce metriche diverse per definire un programma di audit. Nella fattispecie, l'approccio che si è deciso di dare, è mutuato dall'*Information Technology Assurance Framework* (ITAF). Questo prevede la definizione di tre macro ambiti di audit che raccolgono gli obiettivi principali atti a definire il corretto "scope" dell'attività declinandolo rispetto: *pianificazione e ambito dell'audit*, *governance del cloud* e *operatività nel cloud*.

Oltre ad una descrizione sintetica dei vari ambiti, si è cercato di correlare ognuno di questi con le categorie di rischio più comunemente identificate e, quando è stato possibile, con i vari modelli di cloud offerti sul mercato dai CSP.

### PIANIFICAZIONE E AMBITO DELL'AUDIT

Gli obiettivi principali della presente fase sono, in analogia a tutti i progetti di *assurance* significativi, quelli di individuare il 'corretto' ambito (in seguito "scope") dell'audit e definire il piano delle attività.

**Definizione degli obiettivi e criteri di audit** – La presente attività consiste nella definizione ad alto livello degli obiettivi di *assurance*, atti a fornire le indicazioni generali di pianificazione ed esecuzione dell'intervento, e nella determinazione dei criteri rispetto ai quali verrà eseguita la valutazione finale.

**Censimento degli *asset* supportati dal *cloud computing*** – La presente attività consiste nell'identificazione degli **asset** (dati, funzionalità applicative, intere applicazioni, processi) dell'organizzazione supportati dal *cloud computing*. Tale censimento conduce alla definizione di un inventario che documenta, per ciascun *asset* individuato, gli attributi delle soluzioni *cloud* adottate quali, ad esempio, modello implementativo (pubblico, privato, ibrido, comunitario), modello di servizio (IaaS, PaaS, SaaS), caratteristiche essenziali del servizio (*on-demand* self-service, *broad network access*, *rapid elasticity*, *measured service*, *resource pooling*), localizzazione dell'*hosting*, ecc.. Gli *asset* individuati e le soluzioni *cloud* a supporto saranno oggetto di un processo di valutazione del rischio 'inerente' che ha lo scopo di definire l'ambito dell'intervento e la pianificazione preliminare delle attività.

16 ISACA Glossary, http://www.isaca.org/Pages/Glossary.aspx?tid=3880&char=A.

17 © 2014 ISACA, ITAF™: A Professional Practices Framework for IS Audit/Assurance. 3rd Edition. http://www.isaca.org/Knowledge-Center/Research/Documents/ITAF-3rd-Edition_fmk_Eng_1014.pdf

## Controls and Assurance in the Cloud: Using COBIT® 5

Si tratta di una guida operativa rivolta alle aziende che utilizzano e che stanno valutando l'utilizzo del *cloud computing*.

Essa è composta da un *framework* di *governance* e controllo basato su *COBIT 5* e da un programma di audit basato su *COBIT 5 for Assurance*. Le informazioni in essa contenute possono essere utilizzate dalle aziende per valutare il valore potenziale degli investimenti nel *cloud* e per determinare se il rischio è entro il livello accettabile. Inoltre, la guida contiene un elenco di pubblicazioni e risorse che possono aiutare a determinare se il *cloud* è la soluzione appropriata per i dati e i processi considerati.

[1] © 2014 ISACA http://www.isaca.org/Knowledge-Center/Research/Research Deliverables/Pages/Controls-and-Assurance-in-the-Cloud-Using-COBIT-5.aspx

**Determinazione del campo di applicazione dell'audit** – La presente attività consiste nella conduzione di un processo di valutazione del rischio 'inerente' correlato agli *asset* censiti e alle soluzioni di *cloud computing* a supporto al fine di determinare i confini e l'applicabilità dell'intervento e stabilirne il campo di applicazione dell'attività di *assurance*.

Il processo di valutazione del rischio 'inerente' contempla le seguenti macro attività:

- Individuazione del rischio 'inerente' correlato agli *asset* censiti (in termini di confidenzialità, integrità e disponibilità) e alle soluzioni *cloud* che supportano gli *asset* critici
- Revisione dei precedenti audit report in ambito *cloud* (laddove esistenti) e determinazione dell'adeguata mitigazione dei rischi identificati
- Valutazione del rischio 'inerente' correlato ai singoli *asset* supportati dalle soluzioni *cloud*.

Predetto processo di valutazione del rischio consente di definire l'estensione (*scope*) dell'audit al fine di indirizzare gli 'sforzi' nelle aree dell'universo *cloud* a più alto rischio mettendo in secondo piano le aree a minor rischio.

**Definizione del piano delle attività** – La pianificazione, o planning, si basa sullo *scope* definito nell'attività precedente e consiste nel produrre una descrizione delle attività di *assurance* da effettuare sul campo, nella relativa schedulazione (data di inizio e data di fine), nell'assegnazione dei ruoli e responsabilità del personale coinvolto nelle attività di audit, nella stima dell'*effort* (ore) richiesto alle risorse competenti e nella definizione delle procedure per condurre le verifiche.

### *GOVERNANCE* DEL *CLOUD*

Un adeguato governo del *cloud* prevede che in sede di audit si identifichino puntualmente tutti gli ambiti necessari all'adeguata intercettazione dei rischi connessi. A tal proposito gli ambiti di audit specifici di questa sezione sono riportati di seguito.

***Governance* e *Enterprise Risk Management* (ERM)** – L'attività di valutazione relativa a questo obiettivo di audit consiste nella corretta identificazione delle funzioni di governo al fine di garantire efficaci processi di gestione che si traducano in trasparenti decisioni aziendali, chiare assegnazioni delle responsabilità e una adeguata sicurezza delle informazioni, sempre in linea con gli standard aziendali definiti dal cliente. A supporto di questo è necessario implementare adeguati meccanismi di gestione dei rischi intrinsechi dei diversi modelli del *cloud computing*.

**Obblighi legali e contrattuali** – Questa specifica attività consiste nella valutazione degli aspetti giuridici riguardanti i requisiti funzionali, normativi e contrattuali rivolti a proteggere entrambe le parti coinvolte. Tali aspetti devono essere adeguatamente documentati, approvati e monitorati.

***Compliance* e Audit** – Assicurare la conformità e definire opportunamente diritti e obblighi di audit, garantisce le prospettive del top management, delle funzioni aziendali di audit, delle società di revisione e degli organismo normativi che hanno giurisdizione sul cliente.

**Portabilità ed interoperabilità** – Questa attività intende misurare l'efficienza che riveste la pianificazione della migrazione di dati e servizi, oltre che l'opportuna definizione di formati e metodologie di accesso, e quanto questi siano fondamentali per l'abbattimento dei rischi operativi e finanziari. In quest'ottica la transizione dei servizi verso i vari modelli di cloud deve essere programmata fin dall'inizio dell'attività di negoziazione del contratto di servizio.

## OPERARE NEL *CLOUD*

Gli ambiti di audit operativi sono demandati alla definizione degli adeguati controlli che permettano di intercettare i rischi operativi derivati dall'adozione di servizi erogati in cloud.

**Risposta agli incidenti, notifiche e *remediation* –** Le attività da implementare riguardano la valutazione delle metodologie di notifica degli incidenti, le eventuali risposte e le attività di bonifica che devono essere documentate tempestivamente, "aggredendo" opportunamente i rischi di incidente e avviando all'occorrenza il processo di escalation.

**Sicurezza applicativa –** L'attività in questo caso deve valutare che le applicazioni siano sviluppate con una adeguata comprensione delle interdipendenze inerenti le applicazioni *cloud*, che sia svolta l'analisi dei rischi, una adeguata progettazione per la gestione della configurazione e del processo di approvvigionamento in modo da supportare al meglio le mutevoli architetture applicative del *cloud*.

**Sicurezza e integrità dei dati –** In questo caso l'attività richiede la valutazione dei meccanismi di trasmissione, al fine di verificarne il grado di sicurezza e il livello di mantenimento con l'obiettivo di impedire accessi e modifiche non autorizzati.

**Gestione dell'identità e degli accessi –** Questa attività deve valutare i processi di identificazione al fine di assicurare che solamente gli utenti autorizzati possano accedere ai dati e alle risorse, che le attività degli utenti siano debitamente controllate ed analizzate e il cliente abbia il controllo sulla gestione degli accessi.

**Virtualizzazione –** L'attività si pone l'obiettivo di valutare che i meccanismi di virtualizzazione siano adeguatamente fortificati al fine di evitare che l'ambiente del cliente possa essere contaminato da quello di altri clienti.

## Conclusioni

Il *cloud computing* ha ormai un successo indiscutibile e rappresenta una leva competitiva irrinunciabile per molte realtà. I rischi connessi non sono pochi e alcuni, per certi aspetti, al momento irrisolvibili; il successo stesso del fenomeno implica anche che i rischi continueranno ad evolversi, perché è dove c'è il maggiore interesse di mercato che il crimine informatico investe e la tecnologia evolve con tutti i difetti di gioventù.

La novità è che la sua stessa diffusione ha creato una base di conoscenza, in continuo sviluppo, utile a identificare zone di rischio e di incertezza ed affrontarle con consapevolezza. I rischi, come è possibile evincere dalla sintesi qui riportata o da una ricerca più approfondita sull'ampia letteratura disponibile, non hanno lo stesso valore per ogni realtà e applicazione. Possono essere più o meno gravi e significativi in funzione del settore di mercato, delle funzioni esternalizzate, della maturità dei controlli interni e degli obiettivi aziendali. Da qui il principio di proporzionalità dei controlli da implementare in fase di esercizio e dei criteri di valutazione da considerare in fase di scelta di un servizio *cloud*.

La funzione di assurance può avere un ruolo determinante nell'utilizzo efficace del *cloud:* assicurare che esista un processo di identificazione e gestione dei rischi, che i rischi valutati appartengano a tutte le categorie (organizzativi, tecnologici, di *compliance)* e che i controlli implementati siano relativi e proporzionali ai rischi identificati.

## Bibliografia

### ISACA:

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

*Cloud Computing Market Maturity*

*Controls and Assurance in the Cloud: Using COBIT 5*

*Guiding Principles for Cloud Computing Adoption and Use*

*ISACA Top 10 Technology Trends*

*Why Cloud Computing Should Be Part of Business Strategy*

### Altre fonti:

*Cloud Controls Matrix v3.0 Info Sheet (Cloud Security Alliance - CSA)*

*Cloud Controls Matrix v3.0.1 (Cloud Security Alliance - CSA)*

*Cloud Computing Risk Assessment (European Union Agency for Network and Information Security – ENISA)*

*GRC Stack (Cloud Security Alliance - CSA)*

*Secure Use of Cloud Computing in the Finance Sector (European Union Agency for Network and Information Security – ENISA)*

*Security Guidance for Critical Areas of Focus in Cloud Computing v3.0 (Cloud Security Alliance - CSA)*

*Survey and analysis of security parameters in cloud SLAs across the European public sector (European Union Agency for Network and Information Security – ENISA)*

*Top Threats to Cloud Computing (Cloud Security Alliance - CSA)*

## Ringraziamenti

Un sincero ringraziamento per aver realizzato questo documento, mettendo a disposizione il proprio tempo e le proprie conoscenze a:

Danilo Bottini (IT Auditor, Gruppo Enel)

Alessandro Gisolfi (Manager, KPMG Advisory)

Guido Milana (Senior Manager, KPMG Advisory)

Vincenzo Marrazzo (IT Auditor, Gruppo Enel)

Margherita Mezzacapo (Head of Audit Global ICT, Gruppo Enel)

Isabella Mittino (IT Auditor, UniCredit)

Nicola Paolino (Manager, KPMG Advisory)

Lino Piovesana (IT Auditor, Poste Italiane)

Corrado Pomodoro (Associate Partner, HSPI)

Luca Risi (Senior Manager, Protiviti)

Stefano Russo (Group Internal Audit Director, Luxottica)

Giovanni Taurisano (IT Auditor, Poste Italiane)

Giuseppe Zuccaro (IT Auditor, UniCredit)

Ringrazio inoltre Margherita Mezzacapo per aver promosso l'idea di questo lavoro nell'ambito dell'Associazione.

Simona Napoli

*Vice presidente AIEA*



Novembre 2016