Al servizio dei professionisti dell'IT Governance

Capitolo di Milano

Spett.le
BANCA D'ITALIA
Servizio Normativa e Politiche di Vigilanza
Divisione Normativa prudenziale
Via Milano 53
00184
ROMA

Milano, 2 novembre 2012

Oggetto: Osservazioni e commenti inerenti il "Documento per consultazione – Disposizioni di vigilanza prudenziale per le banche – Sistema dei controlli interni, sistema informativo e continuità operativa – Settembre 2012

Questa Associazione desidera sottoporre alla Vostra attenzione l'allegato documento di osservazioni e commenti inerenti il Capitolo 8..

Siamo naturalmente a disposizione per eventuali approfondimenti sulle osservazioni e commenti trasmessi. Per contatti con questa Associazione vogliate fare riferimento al Presidente Silvano Ongetta, o al Vicepresidente Enzo Toffanin delegato per la materia ai seguenti indirizzi di posta elettronica:

aiea@aiea.it
all'attenzione di ….

Oppure direttamente a:

silvano.ongetta@aiea.it
enzo.toffanin@aiea.it

Distinti saluti

Silvano Ongetta
Associazione Italiana Information Systems Auditors
Presidente

ALLEGATO

Disposizioni di vigilanza prudenziale per le banche – Sistema dei controlli interni, sistema informativo e continuità operativa – Settembre 2012 – Commenti al documento per consultazione

Commenti al **Capitolo 8, Sezione II, par. 1** (Interazione tra rischio informatico e rischi operativi) "box 4"

Il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico deve includere compiutamente oltre agli eventi di rischio che sono classificabili nel novero dei rischi di frode (event type 1 e 2) , gli eventi che nella tassonomia dei rischi operativi corrispondono alle "disfunzioni dei sistemi informatici" (event type 6), alle "carenze nel trattamento delle operazioni o nella gestione dei sistemi "(event type 7).[1] Tali sono i rischi associati alla regolarità della produzione informatica in esercizio, alla qualità dell'alimentazione e processazione delle banche dati e alla compliance alle norme di trattamento delle informazioni. Inoltre, dovrebbero essere considerate altre tipologie di rischio informatico i cui impatti sfavorevoli possono essere classificati secondo i casi in più tipi di eventi: E' il caso dei cosiddetti rischi dei processi di sviluppo e di manutenzione dei sistemi informatici (project management risk) corrispondenti ai rischi dei tempi di completamento, di economicità e di qualità del prodotto informatico la cui indagine appartiene alla categoria generale dei rischi nella produzione per commessa e dei rischi contrattuali ed extracontrattuali (reputazionali ad esempio) associati ai processi di acquisizione di risorse, di ricorso ai servizi di terze parti, di compliance rispetto alle attestazioni o dichiarazioni ad Autorità e/o terze parti.

Il livello di tolleranza al rischio informatico dell'intermediario con riguardo sia ai servizi interni che a quelli offerti alla clientela è validamente associabile ad un "grading" decrescente di impatti (sia pure indiretti, ma probabilisticamente credibili) sui ricavi e sui margini aziendali derivanti dall'accadere di eventi previsti. Nella definizione del "grading" l'Alta Direzione dell'intermediario è dominus in questa decisione trattandosi di una decisione di rischio di impresa; l'esperienza indica tuttavia che gli intermediari pongono tipicamente nella prima posizione il rischio di continuità dei servizi verso la clientela, a cui seguono il rischio reputazionale, e in posizioni successive i rischi di affidabilità, di

[1] Dalla lettura del paragrafo 2 Fonti normative del capitolo 8, Sezione I, ultimo periodo, che inizia con "si tiene conto dei seguenti documenti" non risulta con chiarezza che i 5 documenti riportati sono fonti metodologiche fra loro complementari, non alternative, ai fini della indagine sui rischi. Senza questa precisazione il lettore sarebbe autorizzato ad adottare una sola di quelle fonti, prendendo in considerazione una gamma limitata di rischi, in luogo del complesso dei rischi informatici.

continuità e di economicità dei processi informatici di supporto. Sebbene la nozione probabilistica di rischio e la misura della tolleranza (risk appetite) possano con talune approssimazioni formare oggetto di stime quantitative, il principio di generale accettazione della adozione di una metodica per l'analisi dei rischi e per la formulazione del grado di tolleranza si ritiene che sia rispettato qualora l'Alta Direzione abbia approvato una metodica di riferimento vincolante per il management aziendale, che nell'ambito della metodica le classi dei rischi siano dichiarate e dichiarata la loro priorità, che le soglie di tolleranza siano esplicitamente associate ad eventi misurabili e che i suddetti criteri siano effettivamente applicati.

La determinazione del rischio residuo, nella sua essenzialità, consegue alla valutazione di quanto del rischio identificato residua dopo l'applicazione di controlli e contromisure. L'appropriatezza del rischio residuo dipende a sua volta del grado di robustezza dei processi informatici che si intende raggiungere ovvero del grado di robustezza dei controlli che si applicano ai processi al fine di contrastare i rischi. Il framework COBIT raccomanda la valutazione del grado di robustezza dei processi e dei relativi controlli attraverso il modello di maturità dei processi.

Riguardo alla informazione periodica (almeno annuale) che deve essere resa all'organo con funzione di supervisione strategica sulla situazione di rischio informatico rispetto al livello accettato di tolleranza al rischio, si osserva che il complesso di valutazioni che vengono rappresentate in una relazione periodica di sintesi deve permettere sia all'organo di supervisione una immediata comprensione del dato di sintesi, sia la possibilità di comunicare tale valutazione ad Organismi esterni di vigilanza, sia di fondare tale valutazione su analisi e raccolte dati attendibili. Per quanto precede, nelle realtà aziendali di dimensione medio grandi è certamente buona prassi associare alla emissione della relazione periodica una valutazione di terza parte indipendente e di riconosciuta competenza professionale sulla attendibilità delle valutazioni espresse nella relazione periodica.

Commenti al **Capitolo 8, Sezione II, par. 4** (Interazione tra rischio informatico e rischi operativi)

La nozione di "*rischio informatico residuo*" dovrebbe essere emendata come segue:
"rischio informatico residuo" Il rischio informatico cui il sistema nel suo complesso è comunque esposto una volta applicati i controlli e le contromisure individuate in base alla strategia aziendale che recepisce ed interpreta i legittimi interessi di impresa ed extra-impresa (stakeholders needs) .

Commenti al **Capitolo 8, Sezione VI, par. 3** (L'esternalizzazione di sistemi e servizi ICT, Indicazioni particolari) – "box 5".

- Tassonomia del Cloud
- Aspetti tecnologici: la virtualizzazione
- Impatti operativi
- Nuovi rischi
- Buone prassi

1. **Tassonomia del Cloud**. In aggiunta alle tre tipologie di implementazione (privato, community e pubblico) è opportuno dare evidenza della tipologia "ibrida" che consiste della coesistenza con ruoli diversi o persino ridondati delle tre tipologie anzidette. Si comprende che la tipologia ibrida è funzionalmente più adattabile alle realtà aziendali, ma al tempo stesso espande e diversifica le regole di funzionamento e di conseguenza le esigenze di controllo sui rischi sottostanti). Oltre alle tipologie soggettive di fruizione dei servizi (soggetti utilizzatori e fornitori), andrebbero richiamate le tipologie

oggettive di servizi offerti (oggetti del servizio), così come riportate nel *NIST Special Publication 800-145* (*The Definition of Cloud Computing*) che, al momento, rappresenta lo standard di riferimento del settore di mercato:

- **IaaS**: *Infrastructure as a Service*. Servizi di outsourcing di infrastrutture di rete e sistemi in cui le risorse utilizzate sono gestite in modalità "pay per use"; tipicamente si tratta di risorse quali: Sistemi Operativi e capacità elaborativa (O.S., CPU, RAM), spazi di archiviazione dati (storage), banda trasmissiva.
- **PaaS**: *Platform as a Service*. Servizi di outsourcing di ambienti operativi completi di infrastrutture, sistemi operativi, librerie, compilatori, sistemi di controllo delle versioni, middleware, etc. per la progettazione, lo sviluppo, il testing, il rilascio e l'hosting di applicazioni software (es.: dot.net, java, php, etc.).
- **SaaS**: *Software as a Service*. Servizi di outsourcing di applicazioni fruibili attraverso interfacce web. Può trattarsi di applicazioni specifiche per settori di mercato, oppure di applicazioni di automazione d'ufficio, es.: servizi di posta elettronica, servizi di collaborazione, comunicazione, messaggistica, CRM, gestionali, etc.
- **BPaaS**: Business Process as a Service. Identificato come"Evoluzione del SaaS, definisce l'erogazione di servizi non esclusivamente riferiti ad ambiti applicativi ma direttamente alle funzionalità di business o di processo, potenzialmente trasversali rispetto alle piattaforme.

L'articolazione ha la sua importanza in quanto i rischi legati all'acquisizione di servizi di Cloud Computing sono connessi al diverso livello di "controllo tecnologico" relativo che si ha nei tre casi: più elevato nel caso IaaS, in cui il Cliente ha accesso diretto alle risorse condivise per attività di configurazione e monitoraggio, meno nel caso SaaS, in cui il Cliente ha accesso ai soli programmi eseguibili.

2. **Aspetti tecnologici: la virtualizzazione**. Sarebbe utile evidenziare che il Cloud Computing si avvale, nella maggioranza dei casi, di tecnologie di virtualizzazione; l'utilizzo di queste tecnologie, sebbene non rappresenti un requisito obbligatorio per un servizio di Cloud Computing, è spesso un fattore abilitante ma anche un fattore di rischio:
    a. il termine "virtualizzazione" si riferisce all'utilizzo di software specifici per creare piattaforme hardware simulate, vale a dire simulare l'esistenza di più componenti fisici dedicati quali: server, processori, schede grafiche, schede di rete, memorie RAM, memorie fisse, sistemi operativi, pur operando su un insieme più ridotto (al limite uno solo) di componenti reali;
    b. il software di virtualizzazione agisce "disaccoppiando" l'hardware fisico effettivo, dai software che lo utilizzano; il livello di astrazione così creato consente un'elevata flessibilità nell'utilizzo delle risorse fisiche disponibili;
    c. la virtualizzazione consente un'allocazione delle risorse al singolo cliente "flessibile"; vale a dire le risorse vengono allocate soltanto quando effettivamente servono; da qui le modalità di fruizione dei servizi Cloud che di norma prevedono il "pay per use";
    d. la virtualizzazione può interessare tutti i livelli di un sistema informativo:
        i. rete (connessioni fisiche suddivise in reti virtuali private)
        ii. sistemi server (server virtuali configurati all'interno di server fisici)
        iii. applicazioni (istanze multitenant)
    e. Grazie ai meccanismi di virtualizzazione si ottengono caratteristiche di flessibilità e tempi di set-up ridotti che, normalmente, non è possibile riscontrare nei modelli di Outsourcing tradizionale; inoltre gli stessi meccanismi consentono economie di scala e politiche di *oversubscription* che portano ad una riduzione dei costi di gestione e quindi dei prezzi al consumo.

3. **Impatti operativi**. L'adozione di un servizio Cloud Computing impatta sulle strutture organizzative e sui principali processi ICT in maniera analoga ma, se possibile, più incisiva rispetto ad un servizio di Outsourcing tradizionale:
    a. la struttura organizzativa IT viene modificata passando da un focus operativo a uno di gestione di processi;
    b. il personale operativo assume un ruolo focalizzato sul monitoraggio;
    c. la gestione del personale è rivolta a competenze e capacità in grado di gestire la relazione con il Cloud Service Provider;
    d. alcune attività IT sono trasferite alle funzioni di business;
    e. aumenta la possibile dipendenza da personale critico.

    Tutto questo accresce l'importanza delle capacità/competenze di Governance dell'Information Technology rispetto alle capacità/competenze più tecnologiche.

4. **Nuovi Rischi.** Gli indubbi vantaggi operativi dei servizi di Cloud Computing comportano anche un diverso profilo di rischio rispetto ai servizi di Outsourcing tradizionali. In particolare dovrebbero essere considerate e valutate le potenziali aree di rischio riportate nell'elenco che segue. Si deve comunque osservare che alcuni dei rischi elencati potrebbero esistere anche nei più tradizionali servizi di Outsourcing in funzione delle tecnologie utilizzate. L'elenco riportato non è esauriente rispetto a tutti i rischi che dovrebbero essere valutati; a tale scopo ed in funzione della criticità dei servizi esternalizzati, come già richiamato nelle indicazioni del documento di Banca d'Italia, dovrebbero essere condotte opportune e più contestualizzate attività di analisi del rischio.

La condivisione delle risorse (LAN, processori, ram e storage) implica i seguenti rischi potenziali:

<u>Rischi di "attacco informatico"</u> (intrusione, alterazione o diffusione non autorizzata di dati):

a. esistenza di un "collegamento", creato dal software di virtualizzazione, tra sistemi virtuali appartenenti a Clienti diversi ma serviti dalla stessa infrastruttura Cloud (il completo isolamento è possibile solo mediante una separazione fisica degli ambienti);
b. accesso non autorizzato a servizi e dati, da parte di utenti configurati nello stesso servizio Cloud, perpetrata attraverso l'uso di tecniche di intrusione informatica (lo stesso software di virtualizzazione, l'uso di controller DMA, gli strumenti di amministrazione concessi agli utenti, possono rappresentare nuove vulnerabilità oggetto di attacchi mirati);
c. possibile spostamento di settori di disco contenenti dati riservati da una VM (macchine virtuali) ad un'altra (dati rimossi, ma non cancellati in modo sicuro, potrebbero essere letti/recuperati da eventuali concorrenti)

<u>Rischi di compliance:</u>

d. archiviazione e gestione di dati al di fuori dei confini nazionali (nel caso di Cloud Service Provider esteri o multinazionali); in alcuni casi il Cloud Service Provider potrebbe non essere disposto a dichiarare l'ubicazione dei sistemi di archiviazione dei dati;
e. violazione delle norme sulla Privacy o delle Policy aziendali da parte del Cloud Provider (rischio comune all'Outsourcing tradizionale);

<u>Rischi di disponibilità:</u>

f. mancanza delle risorse richieste (interruzione o degrado del servizio), nel momento in cui occorrono, a causa di concomitanza di richieste e politiche di *oversubscription* eccessive da parte del Cloud Service Provider;

<u>Altri rischi nel caso SaaS:</u>

g. possibili difficoltà di migrazione dei dati verso altri fornitori (difficoltà di exit strategy);
h. possibili difficoltà di integrazione/interoperabilità con i servizi interni o di altre strutture che concorrono all'erogazione dei servizi di business;

i. perdita di know-how a vantaggio del Cloud Provider (maggiore rischio di lock-in).

5. **Buone prassi**. Si riportano di seguito a titolo indicativo alcune buone pratiche che possono essere attuate al fine di mitigare i nuovi rischi del Cloud Computing:
   Come già sottolineato i controlli da applicare dovrebbero essere valutati in base alle specifiche esigenze di sicurezza, che derivano da un'opportuna analisi del rischio, nonché da analisi costi/benefici, al fine di raggiungere il miglior rapporto tra sicurezza delle informazioni, prestazioni e costo dei servizi.
   Più in generale, le aree di controllo riguardano:
   a. la definizione e attuazione di adeguati **processi di Governance** (già richiamati nel documento di Banca d'Italia (Titolo V- Capitolo 8 - sezione II – par. 1) con chiari obiettivi di indirizzo e controllo dei servizi esternalizzati; in questo ambito, includere:
   b. la definizione ed attuazione di adeguati processi per la negoziazione e **gestione dei contratti**; di seguito alcune clausole da considerare nel caso di contratti di Cloud Computing;
      i. evidenza esplicita e visibilità delle procedure di sicurezza del CSP, possibilmente attraverso verifiche effettuate da una terza parte indipendente relative allo stato della sicurezza delle informazioni del CSP, rispetto a linee guida internazionali largamente riconosciute (p.e. ISO 2700x, CobiT, PCI-DSS, ecc.), tra cui ad esempio:
         - processi e risultati di analisi dei Rischi del CSP, soprattutto naturalmente per quanto riguarda i rischi per la sicurezza delle informazioni;
         - piano di Business Continuity del CSP richiedendo evidenze oggettive dell'esecuzione periodica dei relativi test;
         - processi di gestione degli incidenti, patching di sicurezza, sicurezza dell'ambiente di virtualizzazione;
         - caratteristiche di sicurezza fisica.
      ii. ricevere in modo regolare - e possibilmente senza intermediazioni ma mediante un sistema oggettivo con parametri replicabili - aggiornamenti sullo stato della sicurezza informatica dei propri sistemi o servizi (IaaS, PaaS, SaaS) erogati dal CSP;
      iii. policy di conservazione e di eliminazione dei dati;
      iv. obbligo di certificazione, da parte di una terza parte indipendente di riconosciuta competenza professionale, in merito al rispetto della normativa italiana;
      v. reporting sulla localizzazione geografica dei dati;
      vi. obbligo di notifica di eventi anomali, violazioni dei dati e/o delle informazioni trattate dal fornitore, vulnerabilità o minacce note entro termini predefiniti applicando le regole previste dal d.lgs 69/12 in tema di società che offrono servizi di comunicazione elettronica e mutuando quindi le regole ivi previste nel rapporto privatistico cliente/fornitore;
      vii. mantenimento di un registro delle violazioni dei dati personali e delle informazioni gestite dal fornitore per conto del cliente;
      viii. divieto di modifica della infrastruttura tecnologica utilizzata per erogare i servizi in assenza di assenso scritto della Banca in particolare qualora le applicazioni siano nella sfera giuridica del cliente;
      ix. livelli di servizio definiti end-to-end;
      x. previsione di penalità non esaustive del danno per perdita di informazioni o mancato rispetto dei livelli di servizio;
      xi. disponibilità di dati grezzi di monitoraggio;
      xii. divieto di subappalto salvo previo accordo scritto della Banca cliente;
      xiii. regolamentazione della proprietà dei log e della loro disponibilità da parte della Banca Cliente;

xiv. compartimentalizzazione e protezione contro la contaminazione dei dati tra clienti differenti e garanzie di riservatezza negli accessi ai dati da parte di personale e terze parti del CSP;
xv. portabilità del servizio e clausole di garanzia di continuità in caso di termine del contratto;
xvi. clausola sul mantenimento della proprietà dei dati
xvii. diritti di verificabilità con tempistiche e modalità, anche automatizzate, predeterminate.

c. **misure di sicurezza tecnologiche** specifiche da richiedere al CSP (e verificare da parte del Cliente), quali ad esempio:
   i. uso di reti e protocolli di trasmissione sicuri (uso di protocolli di comunicazione cifrati, es.: SSL)
   ii. crittografia dei dati a riposo negli archivi e nei file system del Cloud Provider;
   iii. uso di partizioni di disco isolate (storage non condiviso);
   iv. uso di forme di autenticazione federata;
   v. notifica immediata di eventi di sicurezza;
   vi. virtualizzazione controllata;
   vii. metodologie di sviluppo applicativo sicuro.

COBIT Regulatory and Legislative Recognition

La tabella seguente illustra alcuni riconoscimenti del COBIT da parte di Pubbliche Autorità come metodologia di riferimento adottati da normative nazionali anche al di fuori della Unione Europea.

Country	Regulatory Legislative Impact Summary
Turkey	In May 2006 the Banking Regulation and Supervision Agency of Turkey (BRSA) mandated that all banks operating in Turkey must adopt COBIT's best practices when managing IT-related processes. COBIT was the selected framework because its control objectives are internationally recognized and considered to be effective at controlling IT-related processes.
India	Risk IT recognized by the National Stock Exchange (NSE) when conducting assessments of IT and related risks
India	COBIT recognized by the Information Technology Department of the Government of Kerala as the standard for IT governance representing its national e-governance plan.
Japan	Risk IT and Val IT concepts included in "IT Optimization Guidelines", an evaluation of IT utilization in the country.
UAE-Dubai	COBIT accepted by His Highness' Rulers Court (HHRC) Financial Audit Department (Supreme Audit Institution of Dubai) as its IT governance framework and is used in within all government organizations.
Argentina	COBIT recognized and its use promoted in one or more circulars from Banco Central de la República – the country's Banking Regulator.
Argentina	COBIT adopted by the Mendoza Honorary Court as the control framework for all entities providing financial services in the province.
Brazil	COBIT recognized by the country's banking regulator, Banco Central do Brasil, as the control framework for self assessments and audit.
Colombia	COBIT required by the country's banking regulator, Superintendencia Financiera de Colombia, as a reference model for its evaluations. They are ensuring banks and other financial entities use COBIT.
Colombia	COBIT acknowledged by several governmental agencies as an acceptable framework. The ISACA Bogota chapter supports and promotes the government's knowledge of COBIT and ISACA certifications.