Clusit
Associazione Italiana per la Sicurezza Informatica

AIEA
ISACA
Al servizio dei professionisti dell'IT Governance
Capitolo di Milano

Gruppo di Ricerca
AIEA – CLUSIT

L'OUTSOURCING IT:
BEST PRACTICE
E AUDITING

L'**AIEA** è l'Associazione Italiana Information Systems Auditors.
Costituita in Milano nel 1979, l'AIEA riunisce e certifica coloro che in Italia svolgono professionalmente attività di Auditing e Controllo di sistemi ICT sia individualmente, sia come associati, partner o dipendenti di società.
Gli obiettivi dell'AIEA:

- ampliare la conoscenza e l'esperienza dei suoi aderenti nel campo dell'Information Systems Auditing, favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti;
- provvedere ad una adeguata informazione e comunicazione reciproca ai fini dell'aggiornamento nel campo delle tecniche di auditing nell'Information Technology and Communication;
- promuovere un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo di affidabilità dell'organizzazione e di sicurezza dei sistemi;
- facilitare i rapporti di scambio con analoghe associazioni estere;
- promuovere a livello nazionale la partecipazione degli Information Systems Auditor, alla certificazione C.I.S.A. (Certified Information Systems Auditor).

L'AIEA è membro dell'ISACA, International System Audit and Control Association, l'organismo che riunisce le associazioni professionali nazionali, che hanno lo scopo di rappresentare e certificare la figura professionale degli aderenti in quanto conforme alle caratteristiche richieste dai propri statuti

Il **CLUSIT** – Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli Studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.
Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazioneper la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

Copyright e Disclaimer

Composizione del Gruppo di Ricerca

Coordinamento

Claudio Bacchieri, CISM	AIEA	AEM

Gruppo di Ricerca

Alessandro Dellepiane, CISA	AIEA	UniCredit Audit
Alessandro Ierardi	AIEA	Consorzio Operativo Gruppo MPS
Guido Leone, CISA	AIEA	EDS Italia
Simona Napoli, CISA, CISM	AIEA	KPMG
Andrea Pasquinucci, Phd, CISA, CISSP	CLUSIT	UCCI.IT
Mihaela Popa, CISA, CISM	AIEA	UniCredit Audit
Massimiliano Rinalducci, CISA	AIEA	UniCredit Audit
Daniela Rocca	CLUSIT	Consulente Legale
Clarice Rosa, CISA	AIEA	Banca Intesa

Comitato di Qualità

Claudio Bacchieri, CISM	AIEA	AEM
Bruno Ghisu, CISA	AIEA	Banco di Sardegna
Guido Leone, CISA	AIEA	EDS Italia
Silvano Ongetta	AIEA	AIEA
Clarice Rosa, CISA	AIEA	Banca Intesa

Milano, dicembre 2006

INDICE

OBIETTIVI E STRUTTURA DELLO STUDIO

In questo studio ci siamo proposti di identificare alcune *best practice* pertinenti alla professione dell'IS Auditor quando essa sia esercitata per la revisione di realtà nelle quali il Sistema Informativo, o anche la sola gestione dell'infrastruttura IT, siano stati esternalizzati.

Obiettivo primario è descrivere e percorrere il processo di *outsourcing* informatico analizzandone il ciclo di vita, soffermandosi in maniera particolare sugli aspetti che legano sicurezza e contratto, e identificando i principali rischi potenziali ai quali le aziende committente e fornitrice dei servizi si espongono quando decidono di unire i loro interessi tramite un contratto. A tale obiettivo si associano quello di delineare una metodologia per valutare la consistenza delle eventuali situazioni in cui tali rischi sussistano, e quello di individuare alcuni strumenti che, utilizzati dagli IS Auditor, possano aiutare a mitigarli.

Più in particolare, lo studio è strutturato in tre capitoli:

- Nel primo capitolo si descrive il "fenomeno" *outsourcing IT* strutturandolo sotto forma di ciclo PDCA di vita del contratto e descrivendolo poi nelle sue pratiche più consolidate e diffuse;
- Nel secondo capitolo si affrontano e si approfondiscono due aspetti rilevanti dell'*outsourcing IT*: l'aspetto contrattuale, includendo i riferimenti agli SLA (*Service Level Agreements*), e quello della sicurezza, che comprende sia i servizi di outsourcing che l'aspetto legale e di gestione del contratto;
- Nel terzo e ultimo capitolo si affronta e si approfondisce il tema dell'IS Auditing in presenza di *outsourcing IT*, partendo dalla classificazione dei rischi per arrivare a proporre uno strumento valutativo dell'effettiva persistenza degli stessi.

Nel corso della ricerca ed in questo documento abbiamo scelto di evidenziare quegli aspetti che sono emersi dall'esperienza e dalla sensibilità dei componenti del gruppo di ricerca, aspetti che sono stati volutamente privilegiati rispetto alla consuetudine che, in un ambito come questo, ne vorrebbe invece vedere l'esposizione limitata al minimo.

Questo lavoro è stato svolto in collaborazione da AIEA e CLUSIT con l'intento di approfondire, come già evidenziato, sia le tematiche proprie dell'attività di Auditing che le tematiche relative alla sicurezza in particolare nella gestione del contratto. Pertanto una particolare attenzione è stata posta agli aspetti legali/contrattuali e agli aspetti della sicurezza, senza i quali risulta difficile una efficace gestione dei rischi di un processo di outsourcing.

Il mio ringraziamento va a coloro che hanno reso possibile questo risultato, al Presidente Silvano Ongetta, ai direttivi delle due Associazioni e alle Società di appartenenza dei partecipanti al Gruppo di Ricerca, per aver messo a disposizione le professionalità di coloro che hanno elaborato questo studio. Un ringraziamento particolare va poi a Luigi Vannutelli (CLUSIT) che ha contribuito alla fase di start-up di questa proficua collaborazione con AIEA.

Claudio Bacchieri

Coordinatore del Gruppo di Ricerca

DESTINATARI

I destinatari di questa ricera sono gli IS Auditor che, sempre di più, sono chiamati in prima persona a minimizzare e aiutare a gestire il rischio indotto da questa pratica ormai consolidata, anche se con forme e modalità molto diverse tra loro.

Anche le strutture di gestione della governance dell'outsourcing e le strutture del fornitore, a tutti i livelli, possono trarre indicazioni utili da questo lavoro: il ciclo di vita dell'outsourcing ha necessità di essere verificato continuamente per poterne gestire la dinamicità e i rischi che tale scelta sottende.

INTRODUZIONE

L'*outsourcing* è il meccanismo per mezzo del quale un'Azienda trasferisce all'esterno ("*esternalizza*") lo svolgimento di una funzione – come, per esempio, l'erogazione dei servizi del proprio Sistema Informativo – ricorrendo ad un fornitore con il quale stipula un contratto..

L'argomento è di attualità sia per la crescente quantità di Imprese che adottano l'*outsourcing* nelle sue varie forme che per la principale motivazione che porta ad adottarlo: consentire cioè all'impresa stessa di concentrarsi sul proprio *core business* mantenendo al proprio interno le sole competenze essenziali ad esso, e procedendo alla *terziarizzazione* di quelle attività che non sono direttamente riconducibili all'interesse primario dell'azienda.

La tendenza all'adozione dell'*outsourcing* è quindi la risposta all'esigenza di competitività che ogni Azienda, per essere vincente nel proprio settore di business e pronta a raccogliere le sfide della competizione globale, percepisce come di vitale importanza e traduce nella necessità di concentrarsi su ciò che costituisce il *cuore dell'attività principale*. È, infatti, ampiamente condivisa oggi la percezione di come il mantenere all'interno anche le attività di supporto al *core business*, come ad esempio il Sistema Informativo, si traduca in un dispendio di energie che il management è costretto a sottrarre dal perseguimento degli obiettivi primari dell'azienda a discapito, appunto, della competitività.

La scelta dell'*outsourcing* pone dunque all'Impresa il problema di definire e di delimitare il proprio *core business*, che è costituito dalle attività specifiche che la caratterizzano sul mercato e rispetto alle quali c'è l'obiettivo strategico di conseguire un vantaggio competitivo durevole sui concorrenti.

La tendenza a ricorrere all'esternalizzazione è così sostenuta, in definitiva, perché si dimostrano sempre più vitali gli stimoli ai quali tale strategia sa rispondere; uno di questi è l'opportunità di utilizzare gli investimenti e l'innovazione dei fornitori esterni e soprattutto le capacità specialistiche e professionali da loro messe a disposizione e che non sarebbe strategico sviluppare e mantenere all'interno. Inoltre c'è lo stimolo all'eccellenza dei risultati economici in mercati che cambiano rapidamente e caratterizzati da elevato grado di innovazione tecnologica, che si identifica con la riduzione del rischio, il controllo dei costi e la creazione delle condizioni per mettere in campo le migliori capacità per dare risposta ai bisogni dei clienti.

Tuttavia, l'azienda che valuta e decide di ricorrere all'*outsourcing* ha anche problemi, a volte consistenti, da affrontare.

Alcuni problemi si presentano nella fase di valutazione preliminare, altri sorgono una volta che l'azienda ha scelto di ricorrere all'*outsourcing*. Quelli di maggiore rilievo riguardano il processo di

selezione del fornitore, la definizione dei dettagli del contratto, i rapporti con il fornitore selezionato nella loro caratteristica di rapporti continuativi e prolungati, e l'organizzazione della struttura interna come sua controparte capace, informata e autorevole per negoziare e con esso operare.

In generale, la gestione stessa di un contratto di *outsourcing* presenta aspetti di sensibile complessità, ed alcuni di essi sono: la lunga durata, gli investimenti specializzati, l'incertezza sull'esaustività della materia coperta dal contratto e l'approccio verso le opportunità offerte dal progresso tecnologico. Aspetti come questi qualificano il contratto di *outsourcing* come un accordo di fornitura complesso con un'area di rischio, anche potenzialmente elevato, per il cliente costituito dal fatto di dipendere definitivamente dall'erogazione dall'esterno di un servizio essenziale per lo svolgimento di funzioni comunque critiche per la conduzione dell'Azienda.

Il punto cruciale per un'efficace gestione del contratto di *outsourcing IT* sta quindi nella sua negoziazione: un accordo di successo, raccomandano gli esperti, non può prescindere da contratti flessibili che prevedano durate contenute (3 - 5 anni) e revisioni periodiche, che contengano una chiara definizione di sistemi di misura delle performance, di livelli di servizio e di penali, e che prevedano meccanismi di condivisione sia del rischio che dei risultati di business.

Il numero elevato di variabili e la complessità delle problematiche che gravano intorno a questo tema rendono perciò difficile identificare uno schema generale che possa descrivere in modo semplice e univoco il ciclo di vita di un contratto di *outsourcing IT*, e rendono allo stesso modo particolarmente complesse ma di definitiva importanza le correlate attività di controllo e di gestione dei rischi.

1. ASPETTI GENERALI

1.1. CENNI SULLA STORIA E SULL'EVOLUZIONE DELL'OUTSOURCING

La nascita dell' outsourcing IT può farsi risalire alle prime offerte di servizi EDP, in genere costituite da applicazioni e da tempo di calcolo.

I primi casi di outsourcing IT, nelle forme in cui lo si intende oggi, risalgono agli anni '70 quando si afferma la tendenza alla ricerca di "flessibilità organizzativa" in grado di ottimizzare la dimensione delle unità aziendali e così soddisfare la spinta a concentrare le risorse e gli sforzi sul core business.

Gli anni '80 sono caratterizzati dalla costituzione, da parte di alcune imprese, di aziende autonome dedicate alla gestione delle attività informatiche allo scopo di controllare meglio i costi. Si diffondono in quel periodo i primi contratti di Facility Management per l'esternalizzazione della gestione operativa del sistema informatico.

Gli anni '90 hanno visto l'integrazione nelle strategie delle Imprese, e negli assetti organizzativi che ne derivano, dell' outsourcing IT come portatore di benefici che discendono dai seguenti aspetti:

- La focalizzazione sul "core business";
- La liberazione di risorse finanziarie, manageriali e operative per altri scopi aziendali;
- La reingegnerizzazione dei processi di servizio;
- L'accesso a competenze eccellenti esterne;
- L'accesso a risorse non disponibili internamente;
- La condivisione dei rischi e dei risultati (es. partnership).

A meta' degli anni novanta l'outsourcing IT era ritenuto essenzialmente uno strumento efficace nel contenere i crescenti costi del personale informatico e delle tecnologie (fu esempio di questo approccio l'industria aerospaziale che, come del resto anche altri settori in crisi, decise di ricorrervi pesantemente a causa delle difficoltà del settore derivanti dalla fine della guerra fredda e dai tagli governativi ai piani di sviluppo dei voli spaziali).

La seconda metà degli anni '90 ha visto poi il fenomeno dell'outsourcing IT evolvere in modo rilevante, con l'affermarsi di scelte più selettive rispetto al "full outsourcing" (se ne parlerà nel seguito), con l'avvio di una fase di riflessione sulle esperienze maturate, con una maggiore attenzione ai sistemi di controllo, e con la comparsa di nuove forme di "esternalizzazione" (ad esempio ASP – Application Service Provider).

Oggi la scelta dell'outsourcing IT deriva da considerazioni che vanno definitivamente oltre la sola riduzione dei costi, e che riguardano piuttosto le scelte strategiche tipiche dei momenti in cui alleanze e fusioni mettono in discussione e ridisegnano l'architettura dei gruppi presenti sul mercato.

In questo scenario non è comunque consueto oggi osservare, a parte poche eccezioni, che un'Azienda conferisca in outsourcing più del 70-80% dell'attivita' del reparto IT.

Pur essendosi ipotizzata una sua qualche forma di ridimensionamento strategico correlata all'espansione del ruolo del World Wide Web in Internet, l'outsourcing dimostra di rispondere ancora alle aspettative, tanto che il settore mantiene oggi un tasso di crescita maggiore di quello dell'economia americana e rappresenta ancora oltre il 20% del fatturato dei servizi IT gestiti da terzi. Nonostante questo, la sua crescita però è fra le più basse tra le attività del settore ICT, particolarmente

nelle aree delle elaborazioni gestionali (business processing), della contabilità, delle risorse umane e del Facility Management, e questo in relazione alla emergente concorrenza dei servizi alle aziende offerti dagli ASP, che si affermano come la "nouvelle vague" grazie alla caratteristica di essere forniti dall'esterno direttamente attraverso Internet a banda larga.

La crescita dei Servizi ASP è prevista mantenersi costante, e ciò sta inducendo alcuni operatori a spostare sull'ASP, dall'outsourcing IT, la propria offerta sul mercato che cominciano a percepire minacciata.

D'altra parte spesso si afferma che "… l'outsourcing è l'ultima cosa da fare se ci si preoccupa veramente della sicurezza informatica" o anche che "…i componenti software sono l'ultima cosa da utilizzare se si tiene veramente alla qualità del software".

I modelli emergenti di Servizio IT esterno, quali l'*utility computing*, sono considerati da molti ancora immaturi. I principali benefici economici ottenibili in questi casi sono ancora costituiti, essenzialmente, da una riduzione dei costi: queste offerte, quindi, risultano interessanti per predisporre configurazioni di emergenza nel caso si verificassero disastri e si tende a considerarle convenienti in quanto consistono nel pagare "a consumo" soluzioni che probabilmente non verranno mai utilizzate.

La barriera psicologica che rende tiepida l'accettazione del *computing on demand* - e quindi del trasferimento di dati fondamentali a gestori esterni - può essere ricondotta ad una diffusa forma di timore relativo alla sicurezza ed all'instabilità del mercato dei provider di servizi.

E' sempre presente, infatti, la preoccupazione di base dei professionisti ICT: che i fornitori possano, cioè, non essere in grado di occuparsi adeguatamente dei dati di vitale importanza per l'impresa.

A questa obiezione i sostenitori dei modelli basati sull'esternalizzazione replicano normalmente che l'affidare il proprio destino a terze parti è ormai una prassi costantemente praticata in molti altri ambiti, portando ad esempio le aziende di produzione che hanno implementato i sistemi just-in-time anche se questi le rendono potenzialmente vulnerabili a gestioni non ottimali da parte di loro fornitori. Di fatto le forze che trainano l'outsourcing IT e l'utilizzo dei componenti software sono aspetti dell'economia ai quali appare di fatto inutile tentare di opporsi.

1.2. CICLO DI VITA DEI CONTRATTI DI OUTSOURCING

In questa sezione illustriamo il ciclo di vita del contratto di outsourcing, inteso come la sequenza di eventi per esso rilevanti che accadono nel periodo di tempo che intercorre tra il momento in cui si manifesta l'esigenza di esternalizzare un servizio IT ed il momento in cui il contratto di outsourcing, stipulato con un fornitore per soddisfare tale esigenza, giunge al proprio termine e viene – o non viene – rinnovato con lo stesso o un altro fornitore.

Anche quando si intraprende il percorso verso l'outsourcing, con l'obiettivo di concretizzarlo in un contratto di servizio, occorre minimizzare il rischio di insuccessi, e ciò lo si deve perseguire assumendo l'ottica tipica della sana gestione dei progetti, e cioè dotandosi di una metodologia strutturata.

Il modello classico per tale genere di metodologia, che ispira anche questo documento, è quello adottato negli anni '50 da W. Edwards Deming come modello ciclico continuo, largamente conosciuto come modello PDCA (Plan-Do-Check-Act) e che si considera applicabile a tutti i processi aziendali.

Al centro del modello PDCA si colloca (vedi fig.1) il concetto di *miglioramento continuo* basato sul feedback che, identificando le ragioni per le quali i prodotti possono essere non conformi alle richieste dei clienti, permette ai manager di modificare le parti di un processo che necessitano di miglioramenti.

In particolare, il modello PDCA prevede:

- *una fase di pianificazione – PLAN –* in cui si progetta il processo definendone gli obiettivi;
- *una fase di attuazione – DO –* in cui si implementa il processo sulla base della pianificazione;
- *una fase di controllo – CHECK –* in cui si osserva il processo effettuando le appropriate misurazioni e raccogliendone i risultati;
- *una fase decisionale – ACT –* in cui si decidono i cambiamenti opportuni per migliorare il processo.

Nonostante nell'outsourcing IT il rapporto tra cliente e fornitore si stia caratterizzando sempre di più come una partnership, qui abbiamo preferito descrivere il ciclo di vita del contratto tenendo separati i due punti di vista, al fine di evidenziare i diversi ruoli del cliente e del fornitore e, nel capitolo 3, i diversi compiti delle rispettive funzioni di IS Audit. Al fine di facilitarne la lettura, questa sezione si apre quindi proponendo uno schema di sintesi che posiziona i momenti del ciclo di vita di un contratto di outsourcing IT secondo i due punti di vista, del cliente e del fornitore, evidenziando il parallelismo con cui le due parti svolgono, nell'ambito delle singole fasi, le attività dettagliate nel seguito (Tabella 1).

Il capitolo poi approfondirà, per le varie fasi del ciclo, le prassi più consolidate e diffuse.

Figura 1. Il modello PDCA di Edwards Deming

Tabella 1: Ciclo di vita del contratto di outsourcing

a. PUNTO DI VISTA DEL CLIENTE	**b. PUNTO DI VISTA DEL FORNITORE**
a.1. ANALISI (*Plan*)	**b.1. ANALISI (*Plan*)**
a.1.1. Individuazione esigenze e definizione strategie	b.1.1. Definizione del ruolo e delle strategie Identificazione delle esigenze Identificazione degli obiettivi Assegnazione responsabilità commerciali
a.1.2. Identificazione team di analisi	
a.1.3. Analisi dei rischi e delle potenzialità Valutazione dei processi interni Identificazione dei criteri di scelta Scelta dei processi da esternalizzare e degli obiettivi	b.1.2. Identificazione del cliente Individuazione delle opportunità di mercato Identificazione team di analisi Analisi dei rischi e delle potenzialità Sviluppo dell'offerta commerciale
a.1.4. Identificazione del fornitore Ricerca di mercato Identificazione forma di outsourcing Identificazione outsourcer	b.1.3. Definizione del progetto di attuazione e macro-plan
a.1.5. Definizione del progetto di attuazione e macro-plan	b.1.4. Definizione del contratto
a.1.6. Definizione del contratto	
a.2. IMPLEMENTAZIONE DEL CONTRATTO (Do)	**b.2. IMPLEMENTAZIONE DEL CONTRATTO (Do)**
a.2.1. Definizione del team misto cliente – outsourcer	b.2.1. Definizione del team misto cliente – outsourcer
a.2.2. Re-engineering del processo in outsourcing	b.2.2. Re-engineering del processo in outsourcing
a.2.3. Definizione strumenti di controllo ed indici	b.2.3. Definizione strumenti di controllo ed indici
a.2.4. Realizzazione del servizio Analisi organizzativa Adeguamento organizzativo Collaudo del servizio Accettazione del servizio	b.2.4. Realizzazione del servizio Progetto esecutivo Organizzazione del presidio al servizio Adeguamento organizzativo Collaudo del servizio
a.2.5. Formazione del personale	b.2.5. Formazione del personale
a.2.6. Migrazione al nuovo assetto	b.2.6. Migrazione al nuovo assetto
	b.2.7. Erogazione del servizio
	b.2.8. Supporto al cliente
a.3. GESTIONE E VERIFICA DEL CONTRATTO (Check)	**b.3. GESTIONE E VERIFICA DEL CONTRATTO (Check)**
a.3.1. Gestione del contratto e del fornitore	b.3.1. Gestione del contratto e del cliente
a.3.2. Monitoraggio dei livelli di servizio	b.3.2. Monitoraggio dei livelli di servizio
a.3.3. Le attività di Auditing	b.3.3. Le attività di Auditing
a.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (Act)	**b.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (Act)**
a.4.1. Miglioramento continuo	b.4.1. Miglioramento continuo
a.4.2. Valutazione economica e strategica del servizio di outsourcing	b.4.2. Valutazione del servizio di outsourcing
a.4.3. Rinnovo del contratto/ scelta diverso outsourcer	b.4.3. Rinnovo o termine del contratto

Si commentano, in quanto segue, le fasi e sottofasi indicate in tabella e si rinvia ai paragrafi successivi per un'analisi più approfondita delle tematiche che solitamente si affrontano nei diversi momenti che formano il processo di outsourcing.

a. PUNTO DI VISTA DEL CLIENTE

a.1. ANALISI (*Plan*)

a.1.1. Individuazione delle esigenze

L'emergere dell'esigenza di affidare ad una terza parte un processo aziendale, e la sua formalizzazione da parte del vertice aziendale, costituiscono l'inizio del ciclo di vita ed in particolare della fase di Analisi nella quale verificare la fattibilità e, in caso positivo, impostare il successivo progetto di outsourcing.

In generale, l'esigenza può manifestarsi in fase di revisione dei risultati e delle politiche aziendali (formulazione del piano strategico, redazione del budget annuale) oppure a seguito di nuove necessità quali, per esempio, quella di cogliere opportunità di mercato che impongono la realizzazione di nuove funzioni aziendali o l'uso di competenze non prontamente disponibili all'interno.

L'esigenza specifica e, quindi, gli obiettivi che l'azienda intende raggiungere mediante una soluzione di outsourcing, devono essere formulati sin dall'inizio in modo chiaro e, se gli obiettivi sono più di uno, è fondamentale associare a ciascuno di essi un grado di priorità. In questa prima fase devono essere anche individuati i rischi maggiori che la soluzione di esternalizzazione comporta (tipico nel caso dell'outsourtcing IT, ad esempio, è il vedere associato ad esso il rischio di perdere il controllo delle evoluzioni future a causa della mancanza di competenze interne).

Al termine di questa prima fase le esigenze aziendali, gli obiettivi e i rischi principali di una soluzione di outsourcing devono essere formalizzati e quindi condivisi dal vertice aziendale, che di conseguenza decide come conferire gli incarichi per costituire il team che procederà agli approfondimenti successivi.

a.1.2. Identificazione team di analisi

Il vertice dell'azienda individua un gruppo di persone responsabili di condurre le attività di approfondimento necessarie a verificare la praticabilità dell'iniziativa di outsourcing (nel nostro caso, d'ora in poi, s'intenderà "outsourcing IT"), analizzare i vantaggi ed i rischi associati, delineare la scelta di una specifica soluzione.

Il team è costituito da figure di livello dirigenziale e normalmente include almeno i responsabili delle seguenti aree aziendali: Servizio Informatico, funzioni utente interessate, Ufficio Legale (nel caso non sia presente sarà necessario avvalersi di legali esterni), Internal Audit, Risorse Umane.

a.1.3. Analisi dei rischi e delle potenzialità

Sulla base delle indicazioni ricevute dalla Direzione, è necessario definire, a livello generale, quali sono le potenzialità che derivano da una soluzione di outsourcing (ad esempio l'ottimizzazione dei canali di vendita grazie alla rapida acquisizione di nuove tecnologie), i rischi che potrebbero impedire il raggiungimento degli obiettivi aziendali (ad esempio

parziale perdita di controllo sui propri sistemi) ed il grado di rischio che l'azienda ritiene accettabile.

Parte dell'analisi dei rischi e delle potenzialità è costituita da una prima valutazione di costi/benefici nella situazione attuale e nei possibili scenari verso cui ci si rivolge, basata su consuntivi, stime e proiezioni delle principali voci di costo e di risparmio.

Per arrivare a delimitare il perimetro di applicazione della soluzione di outsourcing, il team di analisi esegue le seguenti macro-attività:

- Valutazione dei processi interni

  In questa fase l'analisi dei rischi e delle potenzialità è effettuata a livello generale sui processi aziendali.

  A partire da una macro-analisi tecnica, funzionale ed organizzativa dei processi interni candidati all'esternalizzazione, si definiscono gli scenari possibili (insourcing ed outsourcing nelle sue diverse forme) e si produce la mappa delle differenze tra le situazioni determinate da tali scenari e la situazione esistente, con i rispettivi rischi e vantaggi valutati rispetto agli obiettivi fissati dalla Direzione e secondo metriche opportunamente formalizzate.

  Questa fase permette di procedere ad un confronto oggettivo delle diverse ipotesi di esternalizzazione e, per i processi interni candidati all'esternalizzazione, richiede anche un'analisi più approfondita delle specifiche voci di costo e di risparmio.

- Identificazione dei criteri di scelta

  Per procedere alla definizione del perimetro, è necessario aver definito i criteri di scelta da applicare alle valutazioni appena descritte, una volta prodotte. Alcuni tra i principali criteri risultano essere i seguenti:

  - rilevanza aziendale del processo: solitamente le attività strategiche non possono essere oggetto di outsourcing, a differenza delle attività operative o di infrastruttura (ad esempio Facility Management, Disaster Recovery, ecc);
  - livello di rischio attuale/ futuro;
  - probabilità del rischio attuale/ futura;
  - grado di efficacia ed efficienza attuale/ futuro;
  - andamento stimato dei costi;
  - andamento stimato dei risparmi;
  - disponibilità di competenze esterne qualificate;
  - possibilità attuale/futura di assicurare il controllo dei processi.

- Scelta dei processi da esternalizzare e degli obiettivi

  Applicando i criteri di scelta alla valutazione dei processi, il team di analisi identifica l'ambito della soluzione di outsourcing e procede ad un ridisegno di alto livello dei processi aziendali.

  Sulla base del perimetro adottato, si deve procedere alla definizione attenta e precisa degli obiettivi che il servizio di outsourcing deve garantire, ed in particolare dei requisiti

minimi dello stesso, perché essi costituiranno la base per l'identificazione del fornitore, e per la definizione del servizio in sede di stesura e di negoziazione del contratto con il fornitore individuato.

L'esito di questa fase è formalizzato e sottoposto all'approvazione del vertice aziendale.

a.1.4. Identificazione del fornitore

- Ricerca di mercato

  La ricerca di mercato può essere informale e prendere direttamente in considerazione quelle aziende che risultino in grado di rispondere alle esigenze sulla base di elementi generici quali, ad esempio, l'aver fornito soluzioni analoghe ad altre aziende, l'avere determinate dimensioni e reputazione, l'essere già state coinvolte come fornitori nell'ambito di progetti precedenti, o altro.

- Identificazione della forma di outsourcing

  La forma di outsourcing (tra le possibili, ricordiamo qui: Joint Venture, Outsourcing globale, Outsourcing selettivo, Consorzio, ecc.) è determinante nella scelta del fornitore perché ne identifica il campo d'azione. In taluni casi questa fase di identificazione deve essere eseguita prima di effettuare la ricerca di mercato (ad esempio: se la necessità dell'azienda è quella di esternalizzare la sola gestione dell'hardware e del software di base, la ricerca sarà focalizzata sui fornitori di servizi di Facility Management).

  Rinviamo al paragrafo 1.2.1.2. per una trattazione più ampia delle possibili forme di outsourcing.

- Identificazione outsourcer

  Ai potenziali fornitori si invia una richiesta di offerta di servizio (solitamente indicata con l'acronimo RFP, Request For Proposal) che dovrà descrivere in dettaglio i requisiti sopra definiti, in termini di servizio richiesto, di livelli e di qualità del servizio stesso, di tempi di realizzazione. Il grado di formalismo di questa richiesta dipende dalla dimensione e dalla tipologia dell'azienda cliente e può richiedere l'apertura di una gara di appalto.

  La definizione di metriche in grado di tradurre in termini quantitativi i requisiti permette di predisporre una base oggettiva di confronto a partire dalla quale sarà possibile scegliere il fornitore sulla base della valutazione delle risposte ottenute.

Anche l'esito di questa fase dovrà essere documentato, formalizzato e sottoposto all'approvazione della Direzione, approvazione che costituirà l'autorizzazione a procedere con il fornitore selezionato.

a.1.5. Definizione del progetto di attuazione e macro-plan

Un aspetto importante del percorso verso l'outsourcing è l'impostazione del progetto di attuazione: la predisposizione, cioè, di un piano di massima che definisca le attività principali, le principali scadenze, le responsabilità ed i ruoli nel controllo e nel coordinamento, i vincoli principali da rispettare.

Questa attività, alla quale dovrebbe contribuire anche il fornitore, permette di raggiungere un maggiore livello di consapevolezza degli impegni cui l'azienda dovrà far fronte, e delle condizioni che il contratto con il fornitore dovrà contenere.

a.1.6. Definizione del contratto

La definizione dei termini contrattuali, a partire dagli obiettivi definiti e dalla proposta del fornitore scelto, è il risultato di una complessa e delicata trattativa che porta ad affinare al livello adeguato le varie condizioni.

In questa fase è fondamentale il diretto coinvolgimento dei legali, interni o esterni, per garantire l'aderenza delle clausole contrattuali alle esigenze del cliente e alla normativa vigente, nonché quelo dell' IS auditor per verificarne la compliance con le strategie e con i processi aziendali.

Il contratto deve essere il più possibile dettagliato, chiaro, completo nel descrivere le attività, i ruoli e le responsabilità di fornitore e cliente, i tempi di realizzazione della soluzione, i costi e gli eventuali incentivi, i livelli di servizio, la gestione della manutenzione ordinaria e straordinaria.

La qualità del contratto sarà infatti determinante per il successo del progetto e per la gestione corretta di eventuali situazioni critiche.

Per una trattazione esaustiva degli aspetti legali e di definizione del contratto si rinvia comunque al capitolo 2.

a.2. IMPLEMENTAZIONE DEL CONTRATTO (*Do*)

Questa è la fase operativa che traduce i termini contrattuali nel servizio IT e nell'assetto organizzativo che ne sosterrà l'erogazione. Questa fase, che vede cliente e fornitore svolgere in collaborazione le attività principali, si configura come un progetto a sé stante e, come tale, deve essere affrontata con una metodologia e misure organizzative adeguate.

a.2.1. Definizione del team misto cliente – outsourcer

Fattori critici per il raggiungimento degli obiettivi sono la definizione precisa dei ruoli e delle responsabilità, nonché la costituzione di un gruppo di lavoro "misto" con il compito di coordinare e controllare le attività svolte dai rispettivi gruppi operativi. Tale coordinamento e controllo dovrà esercitarsi sulla base del macro-plan redatto in precedenza che, a questo fine, dovrà essere sviluppato nelle attività di dettaglio per ciascuna delle quali saranno individuate le persone responsabili della loro realizzazione. Per meglio coordinare e controllare le attività comuni, cliente e fornitore dovranno necessariamente concordare tempi, scadenze e modalità realizzative nonché risolvere le eventuali reciproche dipendenze.

Una particolare attenzione deve essere posta alla valutazione della durata e alla gestione della complessità delle attività propedeutiche al passaggio a regime.

In questa fase cliente e fornitore dovrebbero anche concordare la programmazione delle attività di formazione da erogare prima del passaggio in esercizio della soluzione.

a.2.2. Re-engineering del processo in outsourcing

In questa fase viene analizzato in dettaglio il nuovo processo, definito ad alto livello nella fase di *Analisi dei rischi e delle potenzialità* (si veda punto *a.1.3*.): vengono determinate le specifiche funzionali e tecnologiche dello scenario futuro e di conseguenza vengono definite le strutture organizzative del cliente necessarie alla fruizione del futuro servizio.

Il completamento di questa fase rende possibile pianificare in modo definitivo attività, tempi, risorse e responsabilità del progetto di migrazione.

a.2.3. Definizione strumenti di controllo ed indici

In questa fase si definiscono gli strumenti per controllare l'effettivo raggiungimento degli obiettivi del contratto e gli indicatori in base ai quali misurare le prestazioni della soluzione di outsourcing e del fornitore.

In funzione delle diverse esigenze di evidenziare adeguatamente le eventuali carenze o situazioni critiche, si potranno definire strumenti ed indici da utilizzare in modo continuativo e/o su base periodica opportunamente determinata.

In particolare, è necessario definire il ruolo di Responsabile del Monitoraggio dei Livelli di Servizio e disegnare i processi di rilevazione, di comunicazione e di gestione degli esiti del monitoraggio stesso.

a.2.4. Realizzazione del servizio

- Analisi organizzativa

  In questa fase il cliente, in collaborazione con il fornitore, analizza e ridefinisce i propri processi organizzativi e le relative strutture di supporto.

  Inoltre, viene delineata la struttura organizzativa mista, cliente-fornitore, che gestirà la fruizione della soluzione di outsourcing durante tutto il periodo della sua durata.

- Adeguamento organizzativo

  Questa fase consiste nell'effettiva predisposizione delle strutture definite e nella gestione dell'eventuale ricollocazione del personale. Questo aspetto assume particolare rilevanza nei casi in cui il servizio di outsourcing implichi la transizione di personale dal cliente al fornitore.

  Ai fini dell'esecuzione della fase di collaudo, l'adeguamento organizzativo dovrebbe rendere operativa anche la struttura organizzativa mista cliente-fornitore per la gestione a regime del servizio.

- Collaudo del servizio

  Il collaudo del servizio consiste nell'esecuzione, da parte degli utenti, dei test volti a verificare che la soluzione allestita in fase realizzativa sia conforme ai requisiti specificati nel contratto e che i nuovi strumenti informatici siano aderenti a quanto definito nella fase di analisi (*Re-engineering del processo in outsourcing*, paragrafo *a.2.2*.).

  Il piano di test è sviluppato durante il progetto esecutivo e può essere predisposto anche in collaborazione con il fornitore.

- Accettazione del servizio

  Una volta accertato l'esito positivo dei test di collaudo, il Cliente dichiara l'idoneità del nuovo assetto formalizzandone l'accettazione .

a.2.5. Formazione del personale

L'avvio del servizio di outsourcing presuppone, sia per il cliente sia per il fornitore, l'adeguata formazione del rispettivo personale a qualsiasi titolo coinvolto nella nuova modalità di erogazione del servizio. Nel caso del cliente, il training metterà l'utente in grado di utilizzare il nuovo servizio focalizzando, a seconda del tipo di outsourcing, gli aspetti funzionali e/o sistemistici del nuovo assetto.

Può essere necessario svolgere attività di formazione anche prima del collaudo per fornire le competenze necessarie ad una efficace esecuzione dei test.

a.2.6. Migrazione al nuovo assetto

Con l'accettazione, si avvia la migrazione tecnica ed organizzativa al nuovo assetto. Ciò costituisce la fase conclusiva del progetto di implementazione del contratto, e comprende l'insieme di attività che permettono la chiusura del vecchio ambiente e l'avvio dell'erogazione dei servizi in outsourcing.

Ciò che segue descrive sinteticamente le principali attività che caratterizzano il periodo di fruizione del servizio.

a.3. GESTIONE E VERIFICA DEL CONTRATTO (*Check*)

a.3.1. Gestione del contratto e del fornitore

Durante il periodo di fruizione del servizio è opportuno che il cliente mantenga un controllo costante del rispetto delle clausole contrattuali e del corretto andamento delle relazioni con il fornitore. Queste attività, di responsabilità del team misto precedentemente costituito, saranno particolarmente importanti per gestire, ad esempio, il manifestarsi di esigenze interne diverse da requisiti iniziali, oppure il perdurare di carenze nel servizio fruito rispetto agli SLA, con modalità che possano evitare il deteriorarsi dei rapporti tra le due controparti.

a.3.2. Monitoraggio dei livelli di servizio

Grazie agli strumenti e agli indici sopra definiti si attivano i controlli concordati con il fornitore e si producono rapporti periodici ed estemporanei sull'andamento del servizio. Nei casi di scostamento dai livelli attesi, il Responsabile del Monitoraggio intraprende le opportune azioni correttive ed avvia i previsti processi di comunicazione verso l'azienda e verso il fornitore.

a.3.3. Le attività di Auditing

Attività di Auditing sono svolte durante tutto il ciclo di vita del contratto, come si vedrà in modo approfondito nel seguito; tuttavia le verifiche più significative e più numerose sono effettuate nel periodo di fruizione del servizio.

Molteplici possono essere la tipologia, gli obiettivi, la frequenza, le modalità di queste attività, così come lo possono essere i fattori che le determinano (controlli pianificati, controlli a fronte di eccezioni, ecc.).

Si rimanda al capitolo **3** per la trattazione approfondita di questo tema, che è il principale oggetto del presente studio.

a.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act*)

a.4.1. Miglioramento continuo

Anche se il servizio di outsourcing è regolato da termini contrattuali ben stabiliti, durante il periodo di fruizione normalmente si rendono necessari interventi correttivi o di ottimizzazione della soluzione informatica e della sua gestione. Questo, a seconda di quanto previsto nel contratto, può richiedere un regolazione economica separata.

In generale, con l'obiettivo di migliorare costantemente il servizio di outsourcing sulla base dell'evoluzione delle esigenze del cliente e delle potenzialità del fornitore, è possibile prevedere nel contratto una revisione periodica del servizio stesso, degli strumenti di controllo e degli indici di valutazione, fino ad una eventuale revisione dei corrispettivi economici.

a.4.2. Valutazione economica e strategica del servizio di outsourcing

Periodicamente (e non necessariamente allo scadere del contratto) il cliente deve rivalutare l'opportunità di mantenere quel servizio all'esterno con il medesimo fornitore, o di affidarlo ad un diverso outsourcer o di riportarlo all'interno dell'Azienda.

Questa valutazione deve prendere in considerazione, oltre alla qualità del servizio usufruito, anche l'evoluzione dei fattori interni ed esterni che, inizialmente, avevano determinato la decisione di esternalizzare.

a.4.3. Rinnovo del contratto / scelta diverso outsourcer

Le valutazioni appena considerate determineranno, quindi, la decisione del cliente in merito ad una delle seguenti alternative:

- rinnovo del contratto, in questo caso il ciclo di vita riprenderà dalla fase di Monitoraggio;
- rinegoziazione e riformulazione, in questo caso il ciclo di vita riprenderà dalla Definizione del contratto (fase di Analisi), ma la fase di Implementazione e Gestione non sarà necessariamente ripercorsa se non per gli adeguamenti di dettaglio;
- scelta di un diverso outsourcer, in questo caso il ciclo di vita riprenderà a partire dalla fase di Identificazione del fornitore;.
- rientro in Azienda del settore esternalizzato.

b. PUNTO DI VISTA DEL FORNITORE

b.1. ANALISI (*Plan*)

b.1.1. Defininizione del ruolo e delle strategie

L'esigenza di rafforzare la posizione nel mercato può condurre il vertice aziendale a valutare l'ipotesi di proporsi quale fornitore di servizi di outsourcing IT. L'analisi di opportunità e di fattibilità di una scelta di questo tipo deve includere uno studio delle caratteristiche interne dell'azienda, come ad esempio:

- le proprie capacità imprenditoriali;
- la propria solidità finanziaria;
- le competenze e le tecnologie disponibili o ragionevolmente acquisibili e quindi le forme di outsourcing più vicine all'attuale attività dell'azienda;
- la dimensione e la flessibilità delle proprie strutture;
- la possibilità di alleanze strategiche che permettano l'ampliamento dei servizi offerti;

ed un confronto con le concrete possibilità che il mercato dell'outsourcing IT offre, quali ad esempio:

- il livello di saturazione delle diverse forme di outsourcing e quindi il potenziale parco clienti disponibile;
- i costi derivanti dagli investimenti richiesti in termini di competenze, tecnologie e aspetti logistici;
- gli effettivi margini di guadagno, in rapporto agli attuali profitti dell'azienda, ecc.

L'analisi deve esaminare anche i rischi imprenditoriali legati alle diverse forme di outsourcing considerate in relazione alle caratteristiche dell'azienda.

Gli esiti dell'analisi di fattibilità devono essere condivisi con il vertice aziendale e, se è confermata la scelta di trasformare l'azienda in outsourcer per servizi IT, deve essere avviato uno studio per l'individuazione e la definizione degli obiettivi strategici.

A seguito della formulazione del nuovo piano di impresa, o parallelamente a questo, il vertice aziendale provvederà a dare incarico formale alle opportune strutture per l'avvio sia delle campagne di marketing per la promozione del nuovo ruolo che delle attività commerciali, organizzative ed informatiche necessarie al progressivo adeguamento interno e all'acquisizione dei Clienti.

Componente fondamentale della strategia dovrà essere l'attenzione all'aggiornamento continuo delle competenze e dell'infrastruttura tecnologica per tutelare e rafforzare la posizione dell'Azienda nel mercato.

b.1.2 Identificazione del cliente

- Individuazione delle opportunità di mercato

  Una nuova opportunità può presentarsi in seguito alle attività di promozione commerciale avviate per volontà della Direzione aziendale, oppure come richiesta esplicita formulata dal cliente. Questa, a sua volta, può pervenire tramite contatti informali, o manifestarsi come richiesta scritta indirizzata direttamente al fornitore, o come richiesta formale di una proposta di servizio (RFP), oppure mediante una gara di appalto.

  L'outsourcing potrebbe essere non ancora parte dell'offerta del fornitore, ed in tal caso la struttura che ha individuato l'opportunità deve coinvolgere il vertice aziendale che valuterà la fattibilità generale della risposta prima di autorizzarne la presentazione al Cliente.

  In ogni caso l'analisi dell'opportunità e l'eventuale risposta devono essere effettuate da una opportuna struttura commerciale.

- Individuazione team di analisi

  Il Responsabile designato per condurre l'attività commerciale, deve coordinare un gruppo di lavoro con l'obiettivo di approfondire la fattibilità dell'iniziativa, analizzandone ad alto livello i rischi ed i vantaggi, ed eventualmente predisporre la proposta di servizio da inviare al potenziale cliente.

  Il team deve includere tutte le competenze tecnico-funzionali necessarie e tutti i rappresentanti delle aree aziendali che lo specifico servizio di outsourcing, oggetto della proposta, coinvolge; se l'organizzazione aziendale non consente un gruppo di analisi sufficientemente ampio, il Responsabile deve farsi carico di consultare i referenti delle

aree aziendali coinvolte, quali ad esempio: Risorse Umane (in caso di acquisizione di personale del cliente), Servizio Informatico, Internal Audit, Ufficio Legale.

- Analisi dei rischi e delle potenzialità

  Una nuova iniziativa di outsourcing costituisce per il fornitore una importante opportunità, perché può permettere di acquisire nuovi clienti o ampliare la gamma dei servizi offerti, ma introduce fattori di rischio che devono essere valutati prima di dare corso alla formulazione della proposta commerciale e per esprimerla nei giusti termini, convenienti e cautelativi, per l'azienda.

  L'analisi dei rischi deve identificare e valutare sia i rischi inerenti all'attività di fornitura in sé, ad esempio il parziale o mancato rispetto dei livelli di servizio pattuiti, quelli che dipendono dall'operato e dalla situazione del cliente e qelli che dipendono dallo stato del suo servizio informatico.

  È, ad esempio, necessario individuare con precisione il perimetro del servizio di outsourcing, ossia le aree di competenza rispettive del cliente e del fornitore; in caso di acquisizione di asset del cliente, è necessario stimarne il valore, la qualità e la curva di svalutazione; a seconda del contesto e la forma cui si riferisce la richiesta di offerta, è necessario analizzare la composizione applicativa e tecnologica del servizio oggetto di trattativa, gli aspetti di proprietà o licenza d'uso, i principali contratti di manutenzione in essere e la dislocazione degli apparati tecnologici.

  D'altra parte, per il fornitore, i rischi derivanti dagli investimenti in nuove tecnologie e competenze si distribuiscono su più clienti e quindi, in ultima analisi, risultano più facilmente controllabili.

  I risultati dell'analisi devono essere formalizzati e sottoposti alla Direzione, che dovrà determinare l'effettiva convenienza dell'opportunità per lo sviluppo dell'azienda ed eventualmente autorizzare la prosecuzione delle attività di preparazione della presentazione dell'offerta al cliente.

  In tal caso, gli elementi sopra raccolti costituiscono la base per la formulazione dell'ipotesi di soluzione di outsourcing e per la stima sia dei costi che dei tempi di realizzazione.

- Sviluppo dell'offerta commerciale

  La formulazione dell'offerta commerciale, oltre a tenere in considerazione le valutazioni di rischio appena sviluppate, comprende un'approfondita attività di studio e di analisi per produrre una descrizione completa del servizio che si intende offrire.

  Questa fase richiede il coinvolgimento di legali, interni o esterni.

  Nei casi di acquisizione di risorse del cliente, la proposta deve contenere anche una prima ipotesi sulla loro collocazione e sulle modalità di transizione.

  Nello sviluppo dell'offerta si deve produrre una relazione precisa e completa del progetto di realizzazione ed erogazione del servizio richiesto dal cliente; si deve altresì descrivere la consistenza degli investimenti necessari per realizzare il servizio ed indicare puntualmente i relativi costi associati; devono essere definiti i tempi, i modi ed i costi di realizzazione e messa in produzione del servizio; si devono esporre con adeguato dettaglio le modalità ed i costi di gestione, nel tempo, del servizio stesso.

Per calcolare i costi di realizzazione e gestione del servizio, il fornitore può definire un business plan di massima che gli consenta di proiettare i risultati durante il periodo di durata proposto e simulare il punto di break even, a fronte dei costi stimati, del proprio impianto tariffario, dell'ammortamento degli investimenti previsti e dei ricavi attesi.

La formulazione dell'offerta è un passo molto importante e delicato perché la qualità e completezza della proposta commerciale, unitamente ai corrispettivi economici indicati, determinano la scelta del fornitore da parte del cliente; successivamente, i contenuti della proposta costituiranno la base di partenza per la definizione del contratto di outsourcing.

b.1.3. Definizione del progetto di attuazione e macro-plan

A seguito della firma, da parte del cliente, della proposta di servizio sopra formulata, il fornitore deve procedere alla predisposizione di un macro-plan che, sulla base della soluzione descritta nell'offerta, definisca le attività principali del progetto di realizzazione, consegna e gestione del servizio, in cui siano indicate le principali scadenze, i principali ruoli di controllo e coordinamento, i principali vincoli da risolvere o rispettare.

Questa attività può essere svolta congiuntamente al cliente (si veda l'analoga attività descritta nel paragrafo *a.1.6*.) e permette anche di affinare e completare le informazioni da cui derivare le clausole contrattuali.

b.1.4. Definizione del contratto

Anche questa fase si svolge in collaborazione con il cliente e con il coinvolgimento delle rappresentanze legali di cliente e fornitore.

La definizione del contratto è un processo che parte da quanto descritto nella proposta del fornitore e, percorrendo le necessarie fasi di negoziazione, giunge al consenso delle parti e alla firma del contratto.

Come descritto anche nel paragrafo *a.1.6*., il contratto deve descrivere con precisione attività, ruoli, responsabilità, tempi, costi, vincoli, livelli di servizio, penali ed eventuali incentivi, e quanto utile a prevenire l'insorgenza di situazioni di stallo o l'insuccesso del progetto stesso in caso di divergenze tra cliente e fornitore.

b.2. IMPLEMENTAZIONE DEL CONTRATTO (*Do*)

Come già indicato nella corrispondente sezione relativa al Cliente (v. paragrafo *a.2*), in questa fase il fornitore ha il compito di realizzare il servizio ed i relativi strumenti di gestione, secondo le specifiche definite dal contratto, nelle loro componenti tecniche ed organizzative. All'interno dell'unico progetto che coordina le attività comuni cliente-fornitore di questa fase, il fornitore sviluppa il piano di dettaglio e assegna alle proprie attività realizzative una tempistica coerente con le scadenze concordate con il cliente.

b.2.1. Definizione del team misto cliente – outsourcer

Questa fase è stata descritta nella corrispondente sezione relativa al Cliente (v. paragrafo *a.2*).

b.2.2. Re-engineering del processo in outsourcing

Questa fase è stata descritta nella corrispondente sezione relativa al Cliente (v. paragrafo *a.2*).

b.2.3. Definizione strumenti di controllo ed indici

Il fornitore dovrebbe disporre al proprio interno, o acquisire, metodologie e strumenti standard per il monitoraggio delle risorse IT che gestisce, nonché di processi di controllo della qualità dei servizi erogati.

In funzione dello specifico contratto, la definizione degli strumenti e degli indicatori di controllo, per la verifica del raggiungimento degli obiettivi, viene concordata con il cliente come indicato nella corrispondente sezione relativa al Cliente (v. paragrafo *a.2.3*).

b.2.4. Realizzazione del servizio

- Progetto esecutivo

  Essendo di fondamentale importanza per il buon esito complessivo dell'outsourcing, la realizzazione del servizio dovrebbe iniziare con una attenta pianificazione di dettaglio di attività, scadenze, risorse di riferimento e vincoli, nonché una prima formulazione di massima dei piani di collaudo, di formazione e di messa in produzione.

  Il progetto esecutivo ha per obiettivo la realizzazione delle componenti tecnologiche ed applicative del servizio e la predisposizione dei processi organizzativi interni ed esterni necessari all'attivazione del nuovo assetto; tutto ciò dipende dal tipo e dalla forma del servizio di outsourcing adottato, e può quindi variare dalla sola acquisizione e gestione delle infrastrutture hardware, alla acquisizione, o allo sviluppo, ed alla successiva manutenzione delle applicazioni.

  Per quanto riguarda il fornitore, il progetto esecutivo deve anche includere la predisposizione dell'ambiente tecnico per il collaudo utente e la relativa pianificazione di dettaglio dello stesso da effettuare in collaborazione con il cliente, nonché la pianificazione di dettaglio della fase di migrazione al futuro assetto. Prima del test di accettazione finale da parte del cliente, il fornitore può prevedere, se necessario, lo svolgimento di una fase di collaudo interno al fine di verificare l'assenza di anomalie ed, eventualmente, risolverle qualora ne emergessero.

- Organizzazione del presidio al servizio

  Questa fase è volta a definire sia le procedure e le strutture atte a gestire l'operatività giornaliera sia i meccanismi di controllo ed i piani di intervento per far fronte ad anomalie o situazioni di emergenza. Esempi di tali procedure e meccanismi sono:

  - documentazione operativa;
  - pianificazione dettagliata delle attività ordinarie e straordinarie;
  - adeguamenti organizzativi o definizione di nuove strutture dedicate alle attività di controllo e/o supporto al cliente con definizione e assegnazione puntuale di ruoli e responsabilità;
  - metodologie di controllo e tecniche di rilevazione degli indicatori di qualità del servizio;
  - strumenti di gestione e controllo da applicare agli apparati tecnologici e/o alle strutture organizzative;
  - sistemi automatici per la rendicontazione periodica al cliente, mediante i quali fornire misure oggettive e verificabili dei livelli di servizio erogati;

- piano di formazione del personale interno e del cliente.

In questa fase, inoltre, fornitore e cliente devono collaborare nell'analizzare i processi organizzativi comuni richiesti dal futuro assetto, definire e dimensionare le strutture miste a loro supporto.

- Adeguamento organizzativo

  In questa fase si attivano le strutture sopra definite e destinate a gestire il servizio e si determina l'opportuna destinazione del personale da ricollocare. Questo aspetto assume particolare rilevanza nei casi in cui il contratto di outsourcing preveda una transizione di dipendenti dal cliente al fornitore.

- Collaudo del servizio

  Questa attività è condotta congiuntamente da cliente e fornitore al fine di verificare, anche mediante simulazione della situazione di esercizio, che il servizio erogato dal fornitore sia conforme a quanto definito nelle clausole contrattuali.

b.2.5. Formazione del personale

Come anticipato nel paragrafo *a.2.5*, l'avvio del servizio di outsourcing presuppone anche per il fornitore, una adeguata formazione del rispettivo personale a qualsiasi titolo coinvolto nell'erogazione del servizio. Nel caso del fornitore, il training preparerà il personale addetto alla gestione del servizio a garantire l'adeguato supporto operativo, sistemistico e/o funzionale.

Può essere necessario svolgere attività di formazione anche prima del collaudo per fornire le competenze necessarie ad una efficace esecuzione dei test.

b.2.6. Migrazione al nuovo assetto

La migrazione al nuovo servizio è costituita dalle attività tecniche ed organizzative che permettono la transizione del processo interno al nuovo assetto nel quale diventa un servizio in outsourcing, garantendo la continuità operativa dell'azienda cliente.

In questa fase sono di fondamentale importanza la definizione dei ruoli, la corretta attribuzione delle responsabilità sia al personale del cliente sia a quello del fornitore, la predisposizione di un piano di dettaglio delle attività.

A seconda di quanto stabilito nel contratto, questa fase può anche prevedere che nel primo periodo di erogazione del servizio, e per una durata prestabilita, il fornitore metta in atto specifiche forme di affiancamento al personale del cliente.

b2.7. Erogazione del servizio

Questa fase consiste nello svolgimento di tutte le attività contemplate dal contratto di servizio alle condizioni stabilite, per il periodo di tempo e secondo il livello di qualità previsti dalle clausole contrattuali.

b.2.8. Supporto al cliente

La gestione del servizio si deve avvalere di una struttura di supporto al cliente che adotti processi e strumenti specifici per la gestione delle comunicazioni con il fornitore, e sia attiva nei tempi e nei modi definiti nel contratto. Il supporto al cliente può riguardare diversi ambiti, tra i quali:

- l'assistenza all'utilizzo del servizio;
- la gestione e la risoluzione delle anomalie;
- il supporto sistemistico ed operativo per la gestione e il controllo del funzionamento dell'infrastruttura tecnologica e applicativa;
- il controllo e coordimento delle richieste di manutenzione ordinaria ed evolutiva.

I metodi che il fornitore può adottare per fornire il supporto al cliente possono includere:

- la creazione di un call center e/o
- l'istituzione di una funzione di help desk, eventualmente strutturata su più livelli, a seconda della complessità del servizio di outsourcing;
- la predisposizione di documentazione utente e/o tecnica eventualmente accessibile in formato elettronico;
- l'erogazione di corsi specifici o di aggiornamento indirizzati sia al personale interno che opera per o presso il cliente, sia al personale del cliente;
- l'utilizzo di strumenti di monitoraggio dell'infrastruttura tecnologica e software, che permettano al fornitore di individuare e risolvere tempestivamente eventuali guasti o interruzioni di servizio;
- la predisposizione di procedure e strumenti per la gestione dei cambiamenti.

b.3. GESTIONE E VERIFICA DEL CONTRATTO (*Check*)

b.3.1. Gestione del contratto e del cliente

Il fornitore, per mezzo del team misto costituito con il cliente, nonché delle proprie strutture e processi organizzativi preposti alla gestione dei servizi erogati in outsourcing, dovrà sovrintendere al rispetto di tutti gli accordi contrattuali intercorsi, dalla fornitura del servizio alla consegna del reporting al cliente; inoltre dovrà provvedere a sostenere in modo proattivo la collaborazione con il cliente stesso, al fine di prevenire e/o limitare l'insorgere di situazioni di contrasto.

b.3.2. Monitoraggio dei livelli di servizio

Durante il periodo di erogazione del servizio il fornitore applica le procedure e i meccanismi precedentemente predisposti per la misurazione degli indicatori dei livelli di servizio, la formalizzazione degli esiti e la consegna al cliente nelle modalità e tempi stabiliti nel contratto. Nei casi di non rispetto dei livelli pattuiti, è responsabilità del fornitore intraprendere con tempestività tutti gli interventi necessari a ripristinare i livelli di servizio previsti. Il team misto cliente-fornitore per la gestione del periodo di esercizio dovrà includere una persona referente del fornitore responsabile per il coordinamento delle attività di controllo.

b.3.3. Le attività di Auditing

Per questa fase valgono le considerazioni contenute nella corrispondente sezione relativa al Cliente (v. paragrafo *a.3.3*).

b.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act*)

b.4.1. Miglioramento continuo

Per questa fase valgono le considerazioni contenute nella corrispondente sezione relativa al Cliente (v. paragrafo *a.4.1*).

b.4.2. Valutazione del servizio di outsourcing

In modalità e con obiettivi speculari rispetto al cliente, anche il fornitore dovrà valutare, con adeguato anticipo rispetto alla scadenza del contratto, se è opportuno attivare l'azione commerciale volta a favorire il rinnovo o la ridefinizione del contratto con quel cliente, oppure considerare l'ipotesi di interrompere la collaborazione a raggiungimento della scadenza. Per il fornitore una scelta in questo senso può scaturire, ad esempio, da significative variazioni nelle proprie strategie aziendali, oppure dal manifestarsi di criticità del contratto con lo specifico cliente.

b.4.3. Rinnovo o termine del contratto

Se, sulla base delle scelte e dell'esito di una eventuale trattativa, le parti decidono di proseguire nel rapporto commerciale, questo sarà oggetto o di un naturale rinnovo o, come più di frequente accade, di un processo di riformulazione che terrà conto delle nuove esigenze del cliente, delle nuove possibilità del fornitore, e del contesto di mercato. Il ciclo di vita riprenderà, rispettivamente, dalla fase Monitoraggio o dalla Definizione del Contratto, mentre l'esecuzione o meno di una nuova fase di Implementazione e Gestione, o di alcune sue parti, dipenderà dagli adeguamenti del servizio che il nuovo contratto comporterà.

1.2.1. ANALISI (*Plan*)

Iniziamo ad affrontare puntualmente le fasi del ciclo, partendo dall'Analisi, precisando che non verrà seguita puntualmente la distinzione tra cliente e fornitore vista poc'anzi.

1.2.1.1. Motivazioni e rischi

Le organizzazioni, siano esse società private o enti pubblici, ricorrono all'outsourcing IT allo scopo di sfruttare determinate opportunità o trasferire all'esterno alcuni dei rischi legati alla gestione e allo sviluppo del proprio sistema informativo. L'outsourcing introduce tuttavia anche nuovi rischi per l'organizzazione che vi ricorre: si pensi per esempio a quanto correlato con la materia contrattuale e legale ed all'ipotesi di veder deteriorare i servizi erogati dal sistema informativo.

Le motivazioni per il ricorso all'outsourcing si differenziano a seconda del profilo dell'organizzazione che vi ricorre (piccola o media impresa rispetto a gruppo multinazionale), del mercato in cui opera (banca rispetto ad azienda manifatturiera) e della tipologia di outsourcing scelta (facility management rispetto ad outsourcing globale).

E' possibile comunque considerare la seguente classificazione di tali motivazioni:

- ***Ricerca di efficienza e conseguente controllo dei costi***: il fornitore specializzato nello specifico ramo di attività esternalizzate, e con la possibilità di realizzare economie di scala e sinergie con analoghe attività svolte per altri clienti, è nelle migliori condizioni per conseguire una maggiore efficienza per il cliente e indurre per esso una riduzione dei costi IT;

- ***Concentrazione sul core business***: i sistemi informativi sono il core business del fornitore di outsourcing IT, ed il cliente, esternalizzando tale funzione, può dedicare le proprie risorse al proprio core business, minimizzando le risorse interne da dedicare all'IT;
- ***Conoscenze tecniche***: il cliente ha una conoscenza tecnica interna minore rispetto a quella che può avere un fornitore specializzato;
- ***Miglioramento della customer care***: un fornitore esterno ha una maggiore capacità di rispondere alle esigenze di supporto IT degli utenti, rispetto al fornitore interno.

Per quanto riguarda il fornitore stesso, la motivazione che lo riguarda è il fatto che l'outsourcing IT, in quanto tale, costituisce proprio il suo core business. Può fare eccezione a questo fatto il caso che la società di outsourcing, appartenente ad un Gruppo industriale, fornisca il servizio alle società del Gruppo stesso.

Giova ricordare che il ricorso all'esternalizzazione è andato crescendo nel corso degli ultimi anni in Italia, a conferma del fatto che i vantaggi o le motivazioni a ricorrervi sono da noi largamente condivisi. L'ISTAT, nelle sue analisi di settore, rileva come l'outsourcing sia uno dei principali fattori che hanno supportato la crescita del settore IT negli anni 90 (p.e. spesa per outsourcing nel settore bancario italiano cresciuta – in valore assoluto rispetto alla crescita totale della spesa IT – di circa 2,5 volte).

Così come le motivazioni che possono guidare il ricorso all'outsourcing, anche i rischi che esso introduce sono differenti a seconda delle diverse caratteristiche dell'organizzazione che vi ricorre.

Anche in questo caso, come per le motivazioni, riportiamo una possibile classificazione dei rischi introdotti dall'outsourcing:

- ***Riduzione della flessibilità operativa***: la presenza di un contratto che regola i rapporti tra le parti comporta una riduzione della flessibilità nei processi che implicano l'interazione tra utenti ed entità che eroga il servizio (che prima dell'outsourcing facevano parte della stessa organizzazione);
- ***Difficoltà a cambiare la strategia IT***: l'outsourcing è una scelta di livello strategico, e come tale difficilmente modificabile;
- ***Inadeguatezza del fornitore***: se il fornitore non è all'altezza dei livelli richiesti per i servizi da erogare, l'impatto sul cliente è immediato;
- ***Costi non pianificati***: il cliente pagherà corrispettivi aggiuntivi per quei servizi che non sono stati inclusi nel contratto ma che risulteranno poi necessari.

Nell'esperienza comune si sente spesso esprimere insoddisfazione rispetto all'outsourcing (dopo che vi si è ricorso), per l'eccessiva dipendenza che esso creerebbe nei confronti del fornitore, per la difficoltà di incidere sui livelli di servizio e per la mancanza di tempestività nell'effettuare le attività richieste.

È, infine, possibile identificare uno specifico rischio di transizione, il rischio, cioè, che nel corso della transizione dalle modalità operative legate ad un sistema informativo gestito (e/o sviluppato) in azienda a un sistema informativo gestito (e/o sviluppato) in outsourcing, si possa incorrere nella mancata, o insoddisfacente, erogazione del servizio.

Anche il fornitore, a sua volta, deve considerare alcuni rischi, tra i quali:

- Incapacità del cliente ad individuare con completezza i requisiti dei servizi richiesti;

- Incapacità del cliente a modificare il suo modo di lavorare a favore di quello del modello proposto dall'outsourcing;
- Conflittualità generata dalla trattativa economica indotta dall'erogazione di servizi aggiuntivi rispetto a quanto previsto dal contratto.

Le considerazioni sopra esposte sui benefici e sui rischi dell'outsourcing devono essere considerate almeno nei seguenti ambiti:

- Decisione di ricorrere o non ricorrere all'outsourcing;
- Scelta dello specifico outsourcer tra i possibili fornitori presenti sul mercato;
- Definizione delle modifiche da introdurre nel sistema di controllo interno a seguito della scelta di ricorrere all'outsourcing.

Per quanto riguarda la valutazione dei rischi illustriamo nel seguito un modello concettuale che permette di categorizzare i rischi e di valutarne la diminuzione o l'incremento.

Il modello prevede di considerare sette differenti **aree di rischio** – che vogliono essere rappresentative, seppure ad alto livello, dei maggiori rischi di business connessi con l'utilizzo dell'Information & Communication Tecnology – e valutare se il rischio inerente aumenta o diminuisce. A questo proposito si ricorda che per rischio inerente si intende il rischio potenziale che non considera gli eventuali controlli posti in essere al fine di mitigarlo (ad esempio la filiale di una banca è potenzialmente più esposta al rischio di rapine di un chiosco di giornali, prescindendo dai controlli – metal detector all'ingresso, guardie giurate, ecc. – posti in essere per contrastare tale rischio).

Nel seguito si riportano le aree di rischio riferite al cliente e alcune riflessioni, di puro carattere esemplificativo, circa la variazione che l'outsourcing può introdurre sui rischi aziendali:

- ***Dipendenza dal sistema informativo:*** Si tratta dei rischi correlati con l'impossibilità di operare in assenza del sistema informativo. Ovviamente tale rischio è direttamente proporzionale alla pervasività dei sistemi nell'operatività aziendale ed alla capacità dell'azienda di resistere nel tempo al fermo delle proprie attività.

  Per questo rischio valgono le considerazioni che seguono:

  a) se l'outsourcing si concretizza nell'affidare all'esterno attività prima gestite internamente e non comporta quindi cambiamenti di piattaforma, applicazioni, ecc., è verosimile che il rischio resti lo stesso. Si potrebbe al più ritenere che, nel lungo periodo, l'outsourcer cerchi di accrescere la pervasività dell'uso del'IT nei processi aziendali accrescendo, di conseguenza, il rischio potenziale.

  b) se l'outsourcing introduce, invece, anche l'utilizzo di nuove piattaforme, allora ciò che potrebbe aumentare è il grado di automazione dei processi, con conseguente aumento del rischio potenziale.

- ***Competenze e skill:*** Si tratta dei rischi correlati con la mancanza di conoscenze tecniche adeguate circa il sistema informativo in uso, ma anche in merito alle nuove possibilità offerte dalle tecnologie di nuova introduzione.

  L'outsourcer dovrebbe garantire l'aggiornamento delle competenze professionali del proprio personale. Conseguentemente il rischio di non avere competenze tecnologiche aggiornate decresce.

D'altronde il personale interno conosce meglio i processi dell'azienda ed ha solitamente un turnover più basso.

In questo caso si può osservare che il rischio cambia natura (dalla competenza tecnologica alla conoscenza delle peculiarità dell'azienda)

- ***Affidabilità del sistema informativo:*** Per questo rischio valgono le seguenti considerazioni:

  a) se l'outsourcing consiste nell'affidare all'esterno attività prima gestite internamente e non comporta quindi cambiamenti di piattaforma, applicazioni, ecc. è verosimile che il rischio resti lo stesso.

  b) se l'outsourcing corrisponde invece anche all'utilizzo di nuove piattaforme, allora il rischio potrebbe anche diminuire, qualora si passasse all'adozione di una piattaforma generalizzata

- ***Cambiamenti:*** E' il rischio legato al fatto che si possano introdurre errori o fermi dei sistemi in relazione all'introduzione di significativi cambiamenti negli stessi.

  Per questo rischio valgono le seguenti considerazioni :

  a) se l'outsourcing si concretizza nell'affidare all'esterno attività prima gestite internamente e non comporta quindi cambiamenti di piattaforma, applicazioni, ecc. è verosimile che il rischio sia basso. Nel medio periodo si deve comunque presumere che l'outosourcer tenda ad uniformare il sistema e i processi di gestione ai propri standard e che quindi ci sia un cambiamento da gestire e con esso l'emergere del conseguente rischio.

  b) se l'outsourcing corrisponde invece anche all'utilizzo di una nuova piattaforma, c'è ovviamente da gestire anche il rischio relativo ai cambiamenti che ciò introduce.

- ***Esternalizzazioni:*** Si tratta dei rischi correlati con la necessità di gestire un fornitore esterno, assicurando l'ottenimento dei servizi desiderati.

  L'outsourcing fa crescere questo rischio per definizione.

- ***Importanza del Sistema Informativo per il management della società:*** Il sistema informativo è una risorsa strategica per ciascuna azienda e come tale deve essere considerata dal management della società. Se ciò non avviene l'azienda nel suo complesso potrebbe non riuscire a raggiungere i propri obiettivi strategici, proprio per la scarsa adeguatezza dei sistemi nel supportare il raggiungimento di tali obiettivi.

  La scelta di ricorrere all'outsourcing è una scelta strategica ed è pertanto fondamentale che tale scelta venga operata dal management della società. Laddove il management della società non tenga in debito conto l'importanza del sistema informativo, il rischio che si corre aumenta perché si potrebbero infatti operare scelte esclusivamente basate su riduzioni di costi, senza considerare gli aspetti relativi alla qualità dei servizi erogati.

- ***Protezione delle informazioni:*** In caso di outsourcing il valore delle informazioni trattate resta lo stesso e, quanto più è elevato il loro valore o la loro rilevanza ai fini della normativa vigente, tanto maggiore è il rischio inerente relativo alle stesse.

  Con l'outsourcing cambiano, però, le modalità di gestione dei dati, e questo fattore deve essere definito all'interno del contratto e considerato nel momento in cui vengono definite le procedure per la gestione della sicurezza e i livelli di servizio richiesti al fornitore.

Il modello, opportunamente applicato nei casi specifici, serve a guidare l'organizzazione nella definizione dei controlli più appropriati per la riduzione dei nuovi rischi identificati e, d'altro

canto, l'IS Auditor dovrà considerare tali nuovi rischi nella definizione del proprio programma di audit e delle conclusioni del proprio lavoro, valutando l'importanza dei controlli in essere proprio in relazione ad essi.

1.2.1.2. Tipologie di Outsourcing dei servizi ICT

A coloro che intendono ricorrere all'outsourcing dei servizi informatici si presenta il duplice problema dell'individuazione della soluzione più adatta alle proprie esigenze e dell'effettiva capacità del mercato di soddisfarla pienamente.

Alla base della praticabilità di una forma di outsourcing si collocano i tipi di attività e gli ambiti del servizio informatico che si vorrebbero esternalizzare.

Se l'impresa matura l'idea di esternalizzare integralmente il servizio informatico, e cioè sia il supporto alle attività di core business sia l'infrastruttura tecnologica, allora l'obiettivo che si perseguirà sarà l'adozione di una soluzione in grado di garantire la copertura totale sia degli aspetti funzionali sia di quelli tecnici.

La copertura funzionale delle attività di core business può rendere problematica l'adozione dell'outsourcing, perché le peculiarità di uno specifico settore d'industria pongono il problema di reperire sul mercato le adeguate soluzioni preconfezionate.

Tra le soluzioni praticabili si possono annoverare quelle di tipo consortile, o gli accordi che prevedono la cessione degli asset al fornitore.

L'approccio graduale all'outsourcing potrebbe inoltre consistere in una strategia alternativa di minor rischio, che consideri ad esempio l'ipotesi di avviare un processo di esternalizzazione che prenda le mosse dalle componenti infrastrutturali, potenzialmente invarianti rispetto al settore merceologico.

L'outsourcing può essere classificato in relazione a:

- Orizzonte temporale, e cioè come tattico/temporaneo (in genere triennale) o strategico (uguale o superiore a 5 anni);
- Entità dei servizi esternalizzati, e cioè come globale (*full outsourcing)* o selettivo.

1.2.1.2.1. L'outsourcing globale

In questa forma di outsourcing le risorse del servizio informatico sono tutte, o quasi, gestite direttamente dal fornitore. Tali risorse, tra le quali si include il più delle volte anche il personale specializzato, generalmente sono le seguenti:

- Gli elaboratori e le loro periferiche;
- Le postazioni di lavoro, [1]
- L'infrastruttura di Networking;
- Le linee di telecomunicazione;
- Il software di sistema;

[1] Le postazioni di lavoro utente (workstation, personal computer o terminali) potrebbero non rientrare negli ambiti del contratto di outsourcing globale, e quindi gestite internamente dal cliente.

- Il software applicativo;
- I supporti: help desk e documentazione.

Con l'outsourcing globale l'azienda si propone di perseguire obiettivi strategici quali, ad esempio, l'aumento di efficienza operativa e la reale possibilità di concentrare le risorse interne sul *core business*, e cioè sul lancio di nuovi prodotti o di nuovi servizi.

In questo caso i contratti sono di lunga durata, dai 5 ai 10 anni, e possono prevedere clausole particolari mirate alla condivisione degli obiettivi e dei rischi attraverso politiche di incentivazione.

Riguardo il *full outsourcing* valgono le seguenti considerazioni:

a. quella di adottare la forma globale di outsourcing è una decisione di rilievo strategico presa e supportata dai massimi livelli aziendali;

b. usualmente l'outsourcing globale implica la presenza di un fornitore unico. Questa è la soluzione che, sul piano delle relazioni contrattuali ed amministrative, rende più lineare la pratica dell'outsourcing. Ciò non toglie che il cliente possa scegliere un approccio multiforme, configurandolo come un complesso di servizi di outsourcing selettivo;

c. un'impresa che delega totalmente a terzi lo sviluppo e la gestione del proprio servizio informatico necessita comunque ancora di risorse IT proprie, e supporre in linea di principio il contrario è un errore, peraltro comune, nel quale si rischia di incorrere. L'esperienza maturata presso molte società, che hanno adottato il *full outsourcing* con successo, ha infatti dimostrato che per il Cliente è necessario costituire uno staff di specialisti ed individuare una responsabilità manageriale preposta alla gestione delle relazioni con il fornitore;

d. l'aspetto umano e professionale può rappresentare uno degli elementi più complessi da gestire. Infatti se, in presenza di un servizio informatico interno, la scelta del Vertice è per l'outsourcing globale, allora le ripercussioni sul personale potrebbero essere significative: può accadere, per esempio, che il personale specializzato non possa essere riconvertito ad altre mansioni. Tal genere di aspetti necessita, per la sua delicatezza, di essere affrontato e gestito con la massima cura ed attenzione.

1.2.1.2.2. L'outsourcing selettivo

E' la forma di outsourcing che ha per oggetto parti del servizio informatico, oppure segmenti specifici dell'attività d'impresa.

Le varie soluzioni in cui l'outsourcing selettivo può esprimersi hanno in comune la caratteristica di consentire un accesso più diretto a particolari risorse, quali: specifiche competenze professionali, soluzioni applicative mirate, tecnologie di nicchia o particolarmente innovative.

La selettività privilegia quindi la specializzazione e alleggerisce l'organizzazione, ottimizzando l'impiego delle risorse e rendendone più agevole il reperimento.

Il beneficio economico, anche se non sempre evidente, è rappresentato dal fatto che i costi, anche in questo caso, da incerti diventano certi.

L'outsourcing selettivo può rilevarsi la strategia vincente in un contesto in cui l'esternalizzazione globale rappresenta il traguardo finale dell'impresa, traguardo verso il quale

si sceglie di procedere con un approccio graduale che può consentire di intervenire inizialmente e progressivamente sulle aree coperte da soluzioni consolidate.

Gli accordi contrattuali sono di media durata, dai 2 ai 5 anni, e si basano per lo più su livelli di servizio pattuiti e tariffe variabili in funzione del tipo di componente considerata.

Nell'ambito dell'outsourcing selettivo si possono distinguere alcune tipologie:

- *Outsourcing verticale*, che copre uno o più ambiti funzionali del portafoglio applicativo aziendale;
- *System management*, che copre l'area dei sistemi di elaborazione e del software di sistema;
- *Network management*, che riguarda le componenti dell'infrastruttura di comunicazione ;
- *Desktop management*, che riguarda le postazioni di lavoro;
- *End user computing*, che copre l'ambito della gestione degli ambienti elaborativi distribuiti;
- *Application management*, che riguarda la manutenzione, l'esercizio e lo sviluppo del software applicativo del cliente;
- *Outsourcing di funzioni IT*, quali la qualità, o altri servizi specifici anche professionali e consulenziali.

1.2.1.2.3. Insourcing (Società posseduta)

Il termine denota il caso in cui i servizi IT sono esternalizzati verso una società distinta da quella cui fornisce servizi stessi, ma da essa posseduta.

Tale società fornisce ed implementa i nuovi servizi e le architetture IT sulla base di accordi interni o contratti di servizio.

1.2.1.2.4. Joint Venture (Società partecipata)

Il termine, ai fini dell'outsourcing, denota il caso in cui i servizi IT sono delegati ad una società di servizi separata e indipendente dall'organizzazione a cui eroga servizi, in partecipazione con un fornitore. Tale società fornisce ed implementa i nuovi servizi e le architetture IT sulla base di un contratto di servizio.

1.2.1.2.5. Consorzio

Il termine, ai fini dell'outsourcing, denota il caso in cui i servizi IT sono stati delegati ad un raggruppamento di più fornitori esterni, che implementano i nuovi servizi ed architetture IT sulla base di un contratto di servizio

1.2.1.3. I principali servizi IT oggetto di outsourcing

I servizi IT oggetto di outsourcing hanno risentito, nel corso degli anni, sia dell'evoluzione del contesto economico sia di quella della tecnologia informatica.

Quando i sistemi informativi erano basati sul mainframe, i servizi oggetto di outsourcing erano riferiti solo a quel modello elaborativo e non avevano la varietà odierna.

I servizi spaziavano dalle varie forme di gestione del mainframe (housing dei sistemi, hosting delle applicazioni, ecc.) alla gestione della rete (privata o pubblica), alla gestione dei terminali periferici, alla fornitura di soluzioni per il disaster recovery.

Prima della diffusione dei personal computer, dei server midrange e delle LAN nei sistemi informativi aziendali, le diverse architetture sulle quali tali sistemi informativi si basavano, sia elaborative sia comunicative, erano limitate nell'interoperabilità. Con l'affermarsi dell'informatica distribuita e dell'*end user computing* sono nati, accanto a quelli già presenti sul mercato, i nuovi servizi quali il *LAN management* ed il *Desktop management*, e quelli tradizionali hanno visto ampliarsi la varietà dei sistemi supportati, dai mainframe IBM alle piattaforme basate su sistemi operativi Unix o di Microsoft.

Il prepotente affermarsi di Internet ha generato nuovi servizi e nuove modalità di erogazione, quali gli operatori di tipo *ISP* e *content provider* ed i servizi di *managed security*.

Si sta affermando oggi la tendenza all'erogazione di servizi "*on demand*", mirati a soddisfare i crescenti bisogni di flessibilità delle aziende. Esempi ne sono gli *ASP (Application Service Provider),* i *Web Services* o le *Certification Authority*.

I servizi professionali, dalla consulenza all'assistenza, hanno seguito poi l'evoluzione dei sistemi e delle applicazioni alimentata dalla diffusione di standard per lo sviluppo applicativo in ambienti tecnologici avanzati (XML, WSDL, SOA,…) e dalle razionalizzazioni prodotte dai sistemi ERP (Enterprise Resource Planning).

La norma UNI EN 29004-2 definisce il *servizio* come "*il risultato di attività svolte, sia all'interfaccia tra fornitore e cliente sia all'interno dell'organizzazione del fornitore, per soddisfare le esigenze del cliente*".

Se ne può derivare una definizione di *servizio IT* come **il risultato dell'insieme dei processi informatici svolti da una organizzazione, per un dato periodo, al fine di soddisfare le esigenze di un committente.**

La complessità crescente del mondo dell'IT e la sua carica innovativa ci pongono di fronte alla comparsa di sempre nuovi servizi e al mutamento di nomi e contenuti di quelli esistenti.

A conferma di questa continua evoluzione si può citare la varietà delle classificazioni dei servizi IT proposte in letteratura e delle loro descrizioni; analoga varietà si ritrova nell'aggregazione, secondo vari criteri o consuetudini, dei diversi servizi elementari in altri servizi o categorie di servizi.

Purtroppo allo stato attuale non esistono definizioni universalmente accettate dei diversi servizi IT, e spesso si verificano ambiguità nell'utilizzo dei termini.

Una delle possibili classificazione standard per i servizi IT, anche nell'ottica degli appalti pubblici, è rappresentata dalla delibera 49/2000 dell'AIPA (oggi CNIPA), che recepisce la classificazione CEE (oggi UE) "Common Procurement Vocabulary" (CPV) in vigore dal 1-1-1999.

Di seguito si riporta la "categoria 7" (Servizi informatici ed affini), con i relativi servizi, del CPV.

Figura 2. Classificazione “Common Procurement Vocabulary”

CPC prov.			CPV	
Categorie	Denominazione	Codice CPC	Codice CPV	Descrizione
		84250	50312510	Manutenzione di software di tecnologia dell'informazione
		84250	50312520	Riparazione di software di tecnologia dell'informazione
		84500	50312600	Manutenzione e riparazione di attrezzature per tecnologia dell'informazione
		84500	50312610	Manutenzione di attrezzature per tecnologia dell'informazione
		84500	50312620	Riparazione di attrezzature per tecnologia dell'informazione
		84500	50313000	Manutenzione e riparazione di macchine reprografiche
		84500	50313100	Servizi di riparazione di fotocopiatrici
		84500	50313200	Servizi di manutenzione di fotocopiatrici
		84500	50316000	Manutenzione e riparazione di distributori automatici di biglietti
		84500	50317000	Manutenzione e riparazione di macchinari per l'obliterazione di biglietti
		84250, 84500	50320000	Servizi di riparazione e manutenzione di computer personali
		84500	50321000	Servizi di riparazione di computer personali
		84500	50322000	Servizi di manutenzione di computer personali
		84500	50323000	Manutenzione e riparazione di unità periferiche
		84500	50323100	Manutenzione di unità periferiche
		84500	50323200	Riparazione di unità periferiche
		84250, 84500	50324000	Servizi di assistenza per computer personali
		84250	50324100	Servizi di manutenzione di sistemi
		84500	50324200	Servizi di manutenzione preventiva
		84100, 84210, 84990	72100000	Servizi di consulenza per attrezzature informatiche
		84100	72110000	Servizi di consulenza per la scelta di attrezzature informatiche
		84990	72120000	Servizi di consulenza per il ripristino di attrezzature informatiche
		84100	72130000	Servizi di consulenza per configurazione di stazioni informatiche
		84100	72140000	Servizi di consulenza per prove di accettazione di attrezzature informatiche
		84210-84250, 84990	72200000	Programmazione di software e servizi di consulenza
		84240	72210000	Servizi di programmazione di prodotti software in pacchetti

7	Servizi informatici ed affini			
		63309, 84250, 84500, 88650, 88660	50300000	Servizi di riparazione, manutenzione e servizi affini connessi a personal computer, attrezzature d'ufficio, apparecchiature per telecomunicazione e impianti audiovisivi
		84250, 84500, 88650	50310000	Manutenzione e riparazione di macchine per ufficio
		84500	50311000	Manutenzione e riparazione di macchine contabili da ufficio
		84500	50311400	Manutenzione e riparazione di calcolatori e macchine per contabilità
		84250, 84500	50312000	Manutenzione e riparazione di attrezzatura informatica
		84500	50312100	Manutenzione e riparazione di calcolatori centrali
		84500	50312110	Manutenzione di calcolatori centrali
		84500	50312120	Riparazione di calcolatori centrali
		84500	50312200	Manutenzione e riparazione di minicomputer
		84500	50312210	Manutenzione di minicomputer
		84500	50312220	Riparazione di minicomputer
		84500	50312300	Manutenzione e riparazione di attrezzature di reti per trasmissione dati
		84500	50312310	Manutenzione di attrezzature di reti per trasmissione dati
		84500	50312320	Riparazione di attrezzature di reti per la trasmissione dati
		84500	50312400	Manutenzione e riparazione di microcomputer
		84500	50312410	Manutenzione di microcomputer
		84500	50312420	Riparazione di microcomputer
		84250	50312500	Manutenzione e riparazione di software di tecnologia dell'informazione

CPC prov.			CPV	
Categorie	Denominazione	Codice CPC	Codice CPV	Descrizione
		84240	72211000	Servizi di programmazione di software di sistemi e di utente
		84240	72212000	Servizi di programmazione di software applicativi
		84210-84250	72220000	Servizi di consulenza in sistemi informatici e assistenza tecnica
		84220	72221000	Servizi di consulenza per analisi economiche
		84210, 84220	72222000	Servizi di revisione strategica e programmazione di sistemi o tecnologie dell'informazione
		84220	72222100	Servizi di revisione strategica di sistemi o tecnologie dell'informazione
		84210	72222200	Servizi di programmazione di sistemi o tecnologie dell'informazione
		84220	72222300	Servizi di tecnologia dell'informazione
		84220	72223000	Servizi di revisione dei requisiti delle tecnologie dell'informazione
		84220-84240	72224000	Servizi di consulenza per la gestione di progetti
		84240	72224100	Servizi di programmazione per l'implementazione di sistemi
		84230	72224200	Servizi di programmazione per l'assicurazione di qualità dei sistemi
		84230	72225000	Servizi di valutazione e revisione per l'assicurazione di qualità dei sistemi
		84240	72226000	Servizi di consulenza per prove di accettazione di software di sistema
		84220	72227000	Servizi di consulenza di integrazione software
		84220	72228000	Servizi di consulenza di integrazione hardware
		84230	72230000	Servizi di sviluppo di software personalizzati
		84230	72231000	Sviluppo di software per usi militari
		84230	72232000	Sviluppo di software per trattamento transazionale e software personalizzati
		84210, 84220, 84240	72240000	Servizi di analisi e programmazione di sistemi
		84220	72241000	Servizi di specificazione di obiettivi per progetti critici
		84240	72242000	Servizi di modellizzazione di progetti
		84240	72243000	Servizi di programmazione
		84240	72244000	Servizi di prototipazione
		84220, 84240	72245000	Servizi contrattuali di analisi di sistemi e di programmazione
		84210	72246000	Servizi di consulenza di sistemi
		84240, 84250	72250000	Servizi di manutenzione e assistenza sistemi

CPC prov.			CPV	
Categorie	Denominazione	Codice CPC	Codice CPV	Descrizione
		84250	72251000	Servizi di ripristino di programmi
		84250	72252000	Servizi di archiviazione dati
		84250	72253000	Servizi di assistenza informatica e di supporto
		84250	72253100	Servizi di assistenza informatica
		84250	72253200	Servizi di assistenza sistemi
		84240, 84250	72254000	Servizi di prova e di manutenzione di software
		84240	72254100	Servizi di collaudo di sistemi
		84210-84250, 84990	72260000	Servizi connessi al software
		84250	72261000	Servizi di assistenza software
		84240	72262000	Servizi di sviluppo di software
		84240	72263000	Servizi di implementazione di software
		84990	72264000	Servizi di riproduzione di software
		84240	72265000	Servizi di configurazione di software
		84210	72266000	Servizi di consulenza di software
		84250	72267000	Servizi di manutenzione di software
		84990	72268000	Servizi di fornitura di software
		75231, 84250, 84310-84400, 84990	72300000	Servizi di elaborazione dati
		75231, 84250, 84310-84390, 84990	72310000	Servizi di trattamento dati
		84320, 84330	72311000	Servizi di tabulazione informatica
		84320	72311100	Servizi di conversione dati
		84320	72311200	Servizi di trattamento a lotti
		84330	72311300	Servizi di time sharing informatico
		84310	72312000	Servizi di alimentazione dati
		84310	72312100	Servizi di preparazione dati
		84310	72312200	Servizi di riconoscimento ottico dei caratteri
		84310	72313000	Servizi di acquisizione dati
		84310	72314000	Servizi di raccolta e di collazione dati
		75231, 84250, 84990	72315000	Servizi di gestione e supporto di reti di trasmissione dati
		84250, 84990	72315100	Servizi di assistenza per una rete di trasmissione dati
		75231	72315200	Servizi di gestione di reti di trasmissione dati

CPC prov.			CPV	
Categorie	Denominazione	Codice CPC	Codice CPV	Descrizione
		84320	72316000	Servizi analisi di dati
		84390	72317000	Servizi di registrazione dati
		84310, 84320	72319000	Servizi di fornitura dati
		84400	72320000	Servizi di banche dati
		84400	72321000	Servizi di banche dati a valore aggiunto
		84400	72322000	Servizi di gestione dati
		84100-84990	72510000	Servizi di gestione connessi all'informatica
		84210-84250	72511000	Servizi software di gestione di rete
		84990	72512000	Servizi di gestione documenti
		84100-84990	72513000	Servizi di automazione di uffici
		84990	72514000	Servizi di gestione di attrezzature informatiche
		84990	72514100	Servizi di gestione di impianti mediante attrezzature informatiche
		84990	72514200	Servizi di gestione di attrezzature informatiche per lo sviluppo di sistemi informatici
		84990	72514300	Servizi di gestione di attrezzature informatiche per la manutenzione di sistemi informatici
		84100-84990	72520000	Servizi di consulenza e assistenza informatica
		84100-84990	72521000	Servizi di assistenza informatica
		84100-84990	72521100	Servizi di assistenza tecnica informatica
		75231, 75232, 84990	72530000	Servizi per rete informatica
		75231, 75232, 84990	72531000	Servizi di rete locale
		75231, 75232, 84990	72532000	Servizi di rete ad estensione geografica
		84250, 84500	72540000	Servizi di upgrade di computer
		84250, 84500	72541000	Servizi di espansione di computer
		84250, 84500	72541100	Servizi di espansione di memoria
		84220, 84990	72550000	Servizi di audit informatico
		84100, 84240	72560000	Servizi di collaudo informatico
		84250	72570000	Servizi di back-up informatico
		84250	72580000	Servizi di conversione informatica di cataloghi
		84100-84990	72590000	Servizi professionali connessi al computer
		84990	72591000	Elaborazione di accordi sul livello di assistenza

CPC prov.			CPV	
Categorie	Denominazione	Codice CPC	Codice CPV	Descrizione
		84230, 86761-86763, 86769	74323000	Servizi di controllo della qualità
		84230, 86761-86763, 86769	74323100	Servizi di garanzia della qualità

Senza pretese, che sarebbero velleitarie, di validità universale o di esaustività, nel seguito viene proposta una possibile e sintetica classificazione dei servizi IT in termini di *macro-servizi*, corredata in alcuni casi di esempi dei relativi servizi elementari. La lista intende coprire i principali servizi IT che sono, o possono essere, oggetto di outsourcing nella realtà italiana.

- *Facilities management*
- *Systems (server e mainframe) management*
  - Hardware
  - Software di base
  - Software di ambiente
- *Fleet (PCs) management*
- *Network management*
  - WAN e MAN
  - LAN
  - ISP
- *Application management*
  - Analysis
  - Development
  - Maintenance
  - Delivery (ASP, Web Services, ecc.)
- *Operations management*
- *Support services*
  - Help Desk
  - Contact center
- *Education services*
- *Security services (MSS, CA, antivirus, ecc.)*
- *Backup / Business Continuity / Disaster Recovery services*
- *Consulting services (ICT strategy, planning&organization, ICT architecture, ecc.)*
- *Service Level Management*

- Capacity Management
- Performance Management
- Configuration Management
- Change Management
- Problem Management
- Software distribution

- *IS auditing services*

Oltre a quella appena riportata, viene proposta, infine, una ulteriore classificazione, adottata nell'ambito della Pubblica Amministrazione, che raggruppa i servizi in quattro tipologie: quelli svolti dai fornitori in modo continuativo, senza che il committente li richieda volta per volta (una tipologia afferente alla gestione vera e propria dei sistemi informativi automatizzati), quelli finalizzati al cambiamento ed al miglioramento del funzionamento dei sistemi ed alla ottimizzazione del loro uso, quelli che assicurano agli utenti l'assistenza all'uso delle componenti del sistema e risolvono i problemi connessi con il loro utilizzo, ed infine i servizi svolti in maniera estemporanea o solo su richiesta esplicita, per risolvere determinate esigenze non prevedibili.

A) Servizi per la gestione
   1. Conduzione operativa dei sistemi di elaborazione
   2. Pianificazione delle elaborazioni
   3. Manutenzione degli ambienti software di sistema
   4. Gestione delle basi informative
   5. Gestione dei sistemi di supporto alle decisioni
   6. Gestione della sicurezza logica
   7. Web hosting
   8. Web housing
   9. Systems & Lan Management
   10. Gestione della documentazione
   11. Outsourcing delle postazioni di lavoro
   12. Monitoraggio dei livelli di servizio
   13. Gestione delle reti di telecomunicazione
   14. Servizi per la interoperabilità

B) Servizi per il cambiamento ed il miglioramento
   15. Gestione della configurazione e della modifica delle componenti del sistema
   16. Controllo ed ottimizzazione dei sistemi di elaborazione
   17. Capacity planning

C) Servizi per l'assistenza e la risoluzione dei problemi

18. Call Center di 1° livello, interno ed esterno
19. Supporto agli utenti nell'uso delle funzionalità dei sistemi di elaborazione (Call Center di 2° livello, interno ed esterno)
20. Manutenzione correttiva, adeguativa , migliorativa del software applicativo

D) Servizi su richiesta

21. Acquisizione e classificazione dati ed immagini
22. Archiviazione ottica
23. Direzione lavori e monitoraggio della attuazione dei contratti
24. Quality management
25. Formazione
26. Certificazione della firma digitale.

1.2.1.4. Il contratto e gli aspetti legali dell'Outsourcing

1.2.1.4.1. Gli aspetti contrattuali

A fronte delle molteplici forme di outsourcing, nel nostro ordinamento giuridico non esiste una forma tipica di *contratto di outsourcing*, tipicità peraltro non richiesta dalla legge (art. 1322 c.c.). Il rapporto contrattuale fra le parti si configura spesso come un insieme di contratti diversi, tra loro collegati e regolati, nel quale il fornitore del servizio IT acquisisce, ad esempio, strutture hardware, licenze software, ecc.

Si fa talvolta riferimento al *contratto di appalto di servizi*, con prestazioni continuative o periodiche, ma questa qualificazione giuridica è solo parziale e non abbraccia tutta la casistica che si manifesta nella pratica.

La durata, inoltre, è un elemento molto rilevante nei contratti di outsourcing, perché solitamente si tratta di contratti a durata medio-lunga, cosa che contribuisce a rendere più complesso il rapporto tra le parti.

Un ulteriore elemento di complessità si determina quando le parti decidono di creare una joint-venture, costituendo una società compartecipata per lo svolgimento delle attività di servizio. In questo caso, alla complessità del contratto di outsourcing si va ad aggiungere anche l'aspetto della costituzione societaria e della conseguente regolamentazione.

Il *contratto di outsourcing* assume pertanto una connotazione particolare che può sovvertire a volte i canoni tradizionali dei contratti di appalto di servizi.

Nel secondo capitolo saranno evidenziate in dettaglio le caratteristiche più salienti e peculiari del contratto di outsourcing del quale si introducono ora alcune definizioni e caratteristiche generali.

1.2.1.4.2. Una possibile definizione metagiuridica

Si vuole qui proporre una definizione di outsourcing che viene qualificata come *metagiuridica*, in quanto si basa sui contenuti – sull'*oggetto* – del contratto che, in quanto tale, determina una diversa natura del rapporto che viene ad instaurarsi tra le parti.

Secondo questa teoria, si ha outsourcing quando si verifichi l'affidamento all'esterno *di tutto – o parte sostanziale – un processo aziendale.*

Questo serve a distinguere l'outsourcing da un normale affidamento di un mero *servizio*. Valga per tutti l'esempio che segue. L'affidamento ad organizzazione esterna del servizio "paghe", si presenta come un normale appalto di servizi, anche se con caratteristiche di continuità o periodicità. Così, ad esempio, sarà sempre possibile, ogni 28 del mese, fare un collaudo e, se il numero di cedolini sbagliati dovesse superare una certa soglia, si applicheranno le conseguenze contrattuali previste. Se, invece, viene affidata all'esterno la "amministrazione del personale", un collaudo nel senso tradizionale del termine potrebbe essere eseguito con enorme difficoltà. Si dovrà pertanto ricorrere ad altre metodologie – ad esempio l'applicazione dei Service Level Agreement (SLA) – per verificare l'adempimento delle obbligazioni da parte del Fornitore.

E' evidente che l'outsourcing ed il servizio in appalto esterno, sono in questo caso due fattispecie di contratto ben diverse tra loro.

1.2.1.4.3. Caratteristiche dell'outsourcing: Gestire la *"Necessaria Incertezza"*

Le principali caratteristiche del rapporto di outsourcing nel settore ICT sono le seguenti:

1. coinvolgimento importante del Top Management: come già ricordato nei paragrafi precedenti, l'outsourcing è una scelta di strategia aziendale che può comportare grandi trasformazioni organizzative e di *mission* aziendale (concentrazione sul *core business*);

2. necessità di mantenere il controllo strategico dei processi affidati in outsourcing;

3. condivisione delle responsabilità, del monitoraggio e dei risultati – attuali e proiettati nel futuro – per assicurare l'adeguatezza dei servizi nel tempo;

4. esigenza di minimizzare la potenziale conflittualità tra le parti indotta dalle inevitabili variazioni che si renderanno necessarie nel corso della erogazione dei servizi.

Uno dei fattori che differenziano il contratto di outsourcing dai contratti di stampo "tradizionale", è quello delle *modifiche in corso d'opera* che, nei contratti "tradizionali", rappresentano delle eccezioni; e sono guardate con un certo sospetto da parte della committenza. In un rapporto di outsourcing, infatti, l'esigenza di *modifiche in corso d'opera* fa parte della normalità, tanto che una sistematica assenza di tale esigenza si dovrebbe considerare, semmai, come segnale di potenziali criticità.

Per la buona riuscita di un rapporto di outsourcing sembra quindi che le parti debbano predisporsi per poter gestire nel modo migliore quella che può essere definita come una *necessaria incertezza* insita nella natura stessa dell'outsourcing.

E' evidente l'impossibilità di regolare ex ante, tramite una specifica clausola, tutta la complessità del continuo adeguamento del rapporto tra le parti all'evoluzione aziendale ed alle dinamiche tecnologiche e di mercato. Esiste, piuttosto, una serie di predisposizioni e/o di clausole che nel loro insieme contribuiscono a determinare una sorta di *codice comportamentale* che, favorendo la collaborazione tra le parti, permette di gestire al meglio questa dinamica continua, in modo tale che il rapporto tra di esse si configuri come un *contratto quadro* suscettibile di aggiornamenti continui in relazione ai mutamenti delle esigenze.

Se, quindi, è vero che "*il contratto è l'accordo tra due o più parti per costituire, regolare o estinguere un rapporto giuridico patrimoniale*" (art. 1321 c.c.) e che *"il contratto ha forza di*

legge tra le parti" (art. 1372 c.c.), allora nulla vieta che le parti possano stabilire le regole cui esse stesse dovranno attenersi nella rinegoziazione delle condizioni contrattuali, in relazione alle mutate esigenze. Contribuiscono a questo obiettivo tutte le clausole che regolano il monitoraggio dei livelli di servizio concordati (SLA), la composizione, i poteri e le attività dei Comitati di Controllo, la reportistica, i check–point periodici, ed altro. Fondamentale, infine, è che le parti attribuiscano a tutte queste predisposizioni la dovuta rilevanza di fatto nell'indirizzare la conduzione delle attività operative e del rapporto contrattuale.

1.2.2. IMPLEMENTAZIONE E GESTIONE DEL CONTRATTO (*Do*)

1.2.2.1. L'implementazione del contratto

Le attività dell'azienda propedeutiche all'implementazione del contratto si possono identificare in quelle seguenti, alcune delle quali già citate nei precedenti paragrafi:

1. Definizione dei requisiti e dei livelli di servizio – Descrive cosa il cliente vuole (requisiti), e in base a quali parametri ed a quali valori di questi (i livelli di servizio) il contratto con il cliente sarà ritenuto adempiuto dal fornitore del servizio erogato; da qui discende l'importanza di stabilire con precisione ciò che ci si aspetta.

   L'enunciazione dei valori è necessaria, perché ha un riflesso diretto sul prezzo del servizio, o sui tempi necessari a fornirlo, che il fornitore chiederà.

   I requisiti dipendono fondamentalmente dalla natura e dall'ambito del servizio informatico che si intende esternalizzare e dalla forma di outsourcing che si intende adottare. Le categorie di requisiti che esprimono le caratteristiche di un servizio informatico sono riconducibili a:

   - Requisiti organizzativi
   - Requisiti funzionali
   - Requisiti tecnici
   - Requisiti dimensionali
   - Requisiti di qualità
   - Requisiti legati alla gestione del servizio.

2. La ricerca del fornitore – Le linee di indirizzo strategico tracciate dal vertice aziendale determinano i criteri di scelta della soluzione di outsourcing e determinano i vincoli di contesto dei quali tenere conto.

   I criteri di scelta possono essere determinati considerando fondamentalmente tre elementi: la qualità del servizio dichiarata, l'affidabilità del fornitore ed il prezzo dell'offerta, che andranno pesati in base alle caratteristiche peculiari del cliente ed alla tipologia del servizio da esternalizzare.

   La tattica di approccio, che convergerà poi nella selezione e nel confronto delle candidature, dipende dalla forma di outsourcing desiderata, dalla conoscenza del mercato, dai vincoli economici e di tempo che sono in gioco. In generale, l'identificazione del fornitore segue criteri indicati dalle direttive stabilite dal vertice aziendale, avendo quest'ultimo eventualmente disposto sondaggi di mercato oppure consultato una "preferred list" di candidati.

Una volta effettuata la ricerca e ricevute le offerte, queste vengono valutate secondo le prassi adottate all'interno della società, coinvolgendo figure tecniche e/o il vertice aziendale a seconda che si debbano approfondire aspetti di merito, come i Service Level Agreement, oppure di carattere economico/strategico.

3. Trattativa e firma del contratto – Questa attività di solito viene seguita dagli uffici legali: questa fase può richiedere anche un lungo tempo di messa a punto, perché si tratta di raggiungere un punto di equilibrio che soddisfi tutte le aspettative.
4. Realizzazione del servizio – Questa è la vera fase operativa, dove cliente e outsourcer lavorano insieme per costruire il miglior processo possibile (che è quello che soddisfa tutte le esigenze al costo più basso):

   - *Definizione del team misto cliente – outsourcer*

     Per ottenere il miglior risultato possibile, è importante che tutti gli aspetti siano chiariti e condivisi. Persone del cliente e dell'outsourcer (le figure operative che saranno quelle che dovranno gestire il processo, ciascuno sul proprio fronte) devono costituire, nel rispetto dei rispettivi ruoli, un unico team che dovrà avere obiettivi ben precisi.

   - *Re-engineering del processo in outsourcing*

     L'obiettivo prioritario di questo team è modificare il processo, in funzione del conferimento in outsourcing. Il processo, infatti, richiede una fase di dettaglio operativo congiunta, dove il disegno del cliente e gli adattamenti del fornitore trovino il necessario equilibrio attraverso la condivisione delle rispettive esperienze. Il processo va suddiviso quindi in sottoprocessi, di ognuno dei quali si deve chiaramente identificare un responsabile che ne garantisca il corretto funzionamento.

   - *Definizione strumenti di controllo ed indici*

     Vanno fissati gli strumenti per controllare l'effettivo raggiungimento degli obiettivi del processo, che sono stati già definiti nella fase di analisi e specificati nella Richiesta di Proposta all'outsourcer. Lo stesso vale per gli indici in base ai quali verrà misurata la performance dell'outsourcer. Va considerato, a questo proposito, che le assunzioni di partenza devono essere sempre verificate (ad esempio l'effettivo livello di servizio), monitorando costantemente l'andamento degli indici per intervenire rivedendo aspettative che si rivelassero non realistiche, secondo un approccio costruttivo che tenga ben presente che il successo, come il fallimento, dell'outsourcing sono tali sia per il fornitore che per il cliente.

   - *Migrazione al nuovo assetto*

     Vengono, come fase finale, trasferite le attività all'outsourcer prevedendo un periodo di avviamento che può articolarsi nelle seguenti attività: i) la predisposizione dell'impianto tecnologico, ii) la migrazione dal vecchio al nuovo sistema, iii) il collaudo utente, iv) lo start-up effettivo del servizio. Potrebbe anche essere prevista una fase di training del personale del cliente in funzione delle esigenze.

1.2.2.2. La gestione del contratto e gli aspetti organizzativi

La fase di gestione del contratto, pur essendo concettualmente semplice, è tuttavia molto delicata. Un progetto di outsourcing può generare tensioni negli individui, specialmente nel caso in cui

l'outsourcing preveda transizione di personale, o anche scetticismo rispetto alle scelte effettuate. Il coinvolgimento di tutte le persone, rappresentanti di tutti i livelli gerarchici, sin dalle fasi iniziali è una condizione irrinunciabile perché poi ciascuno contribuisca effettivamente al successo del progetto, e riconduca la gestione ad un fatto ordinario.

Gli aspetti legati alle persone sono i più complessi da trattare; qualsiasi forma di outsourcing venga scelta ci si troverà verosimilmente di fronte al problema dell'esubero di personale. Spesso si decide di utilizzare parte del personale IT nella gestione del governo dell'outsourcing. Questo può svilupparsi in due diverse fasi: il progetto di implementazione e la fruizione del servizio a regime.

Ognuna delle due fasi richiede un forte presidio organizzativo ed un controllo adeguato delle attività al fine del raggiungimento degli obiettivi.

Per la fase progettuale, della quale la durata limitata nel tempo è una caratteristica, possono senz'altro valere le consuete metodologie di project management; essa farà riferimento ad un comitato guida (steering committeee) che, con obiettivi di sostanza e temporali, sarà di indirizzo per un team composto da figure rappresentanti delle due parti con responsabilità paritetiche .

Anche per la fase di gestione del servizio a regime è indispensabile, non meno che per quella progettuale, un Comitato Guida formato da rappresentanti della direzione aziendale che ne rappresentino le linee strategiche. Questo ridurrà il rischio che prevalga la convinzione che sia unicamente l'outsourcer che debba farsi carico di tutte le problematiche. Fondamentale, inoltre, per mitigare il rischio di sottovalutazione della fase di gestione del servizio a regime è la cura della crescita della cultura professionale del management, e della conseguente consapevolezza aziendale che la *IT Governance* è parte integrante della *Corporate Governance*.

La crescita della cultura aziendale nel senso appena indicato garantisce la sensibilità verso la necessità di un adeguato presidio strategico e, nello stesso tempo, gestionale, garantendo che all'organismo responsabile di tale presidio sia assegnata l'adeguata collocazione organizzativa nella gerarchia aziendale, e che in esso assuma rilevanza determinante il contributo dell'Information Sytems Auditing.

Un'ulteriore considerazione relativa a questo argomento è che l'operare in regime di outsourcing ha sempre influenza sull'organizzazione interna, anche perché può portare alla variazione sia delle attività che dei ruoli e delle responsabilità. Ciò diviene particolarmente evidente quando si consideri il fatto che la fornitura dei servizi IT all'utenza finale è erogata da una struttura esterna, il che modifica sensibilmente le caratteristiche delle relazioni umane con il personale addetto. Se poi con la transizione all'outsourcing si avvia un processo di trasformazione del servizio informatico in chiave evolutiva, i processi operativi potrebbero dover essere ridefiniti, con impatti di rilievo sulla modalità di lavorare. Anche questo conferma l'attenzione particolare che deve essere posta alla definizione della funzione preposta al governo dell'outsourcing.

In questo contesto si ricordano, infine, i tre elementi chiave del controllo di ogni ciclo di produzione, che guideranno la conduzione del rapporto tra cliente e fornitore:

- Il monitoraggio,
- Il miglioramento continuo,
- Il re-engineering del processo ed aggiustamento degli indici caratterizzanti.

1.2.3. I CONTROLLI E LE VERIFICHE DEL CONTRATTO (*Check*)

1.2.3.1. Monitoraggio dei livelli di servizio

I servizi IT sono sempre una combinazione di attività interne ed esterne e le interazioni di fatto tra cliente e fornitore, in caso di Outsourcing, sono certamente più complesse di quanto descritto nel contratto.

Esternalizzare i servizi informatici non significa necessariamente sopprimere la funzione IT interna, ma rende necessario modificarne la missione al fine di attribuire ad essa compiti che salvaguardino la responsabilità finale dell'azienda.

Tra le attività di Governance, quella di esercitare i controlli sull'erogazione del servizio da parte dell'outsourcer è sicuramente strategica ai fini del soddisfacimento delle aspettative aziendali.

Alla base di questa attività c'è la definizione del livello del servizio[2] atteso, ed è importante che il committente e l'outsourcer condividano l'identificazione degli indicatori, delle modalità di misura e di un sistema di monitoraggio che fornisca rapporti di sintesi dello stato dei livelli dei servizio, sulla base dei quali disporre, quando necessario, interventi o azioni correttive.

Il confronto tra outsourcer e committente sullo stato del livello del servizio dovrà avvenire con regolarità e secondo forme stabilite dal contratto[3]; a supporto della Direzione, in tale adempimento dovrà partecipare una adeguata rappresentanza delle funzioni professionali ed operative, al fine di intercettare con tempestività e accuratezza i problemi o le potenziali criticità.

Per indirizzare le eventuali difficoltà di valutazione del servizio nel primo periodo di erogazione, quando l'assenza di dati storici rende impossibile l'analisi di tendenza dei livelli di servizio e si potrebbe evidenziare la necessità di affinare alcuni parametri di misurazione, è buona prassi prevedere un periodo di osservazione al quale segua una revisione del contratto.

1.2.3.2. Le attività di auditing

L'attività di controllo precedentemente descritta riguarda in particolare le strutture operative. Accanto a questa è necessario che l'azienda svolga periodiche verifiche sui processi di gestione dei servizi IT esternalizzati, tramite audit effettuati dalla propria funzione di Audit Interno o commissionati ad un Auditor Esterno, con l'obiettivo primario di assicurare che ruoli e responsabilità delle terze parti siano chiaramente definiti, ed in grado di soddisfare i requisiti.

La verifica dovrebbe essere mirata alle procedure atte a gestire gli aspetti contrattuali ed i livelli di servizio.

È quindi opportuno includere nel contratto una clausola che assicuri la possibilità di svolgere audit presso l'outsourcer, che specifichi quali tipi di audit sono da prevedere (Audit Interno o Esterno) e preveda l'eventuale diritto, per il committente, di accedere ai risultati dell'attività di audit interno dell'outsourcer e dei conseguenti piani di correzione delle carenze riscontrate.

1.2.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act*)

[2] Livello al quale determinate caratteristiche di un servizio soddisfano i requisiti del committente.

[3] A livello contrattuale è opportuno che le singole controparti si accordino con precisione riguardo alle modalità di rapportarsi, indicando reciprocamente i soggetti che interverranno e come saranno gestiti gli scambi informativi.

Il rapporto contrattuale tra cliente e fornitore, perché sia garantita la soddisfazione reciproca ed il mantenimento del rapporto per tutta la durata prevista, deve essere gestito con opportune politiche di revisione, tenendo conto dell'evoluzione delle caratteristiche del cliente e dei servizi informatici da questo erogati, dell'evoluzione delle strategie societarie, degli andamenti del mercato.

Il cliente è responsabile dell'identificazione dei driver indicanti le evoluzioni tecnologiche, di business e industriali, concorda con il fornitore i punti focali da considerare ed individua gli obiettivi di quello che si identifica come un *relationship change plan*.

Il *relationship change plan* definisce la struttura e i processi finalizzati all'identificazione ed alla gestione dei cambiamenti e delle evoluzioni nel rapporto di lungo periodo fra il cliente ed il fornitore di servizi di outsourcing e, una volta implementato dal cliente, è gestito congiuntamente con il fornitore e agisce secondo livelli di controllo, verifica e rilascio.

Viene così contrastata la percezione, da parte delle unità di business, che l'accordo conseguito sia poco flessibile se non, in alcuni casi, addirittura di ostacolo alla realizzazione del business stesso.

La capacità di stabilire un'efficace politica di *change management* è, quindi, business-critical.

Un piano di gestione dei cambiamenti potrebbe comprendere, tra gli altri, i seguenti argomenti:

- Responsabilità del piano di gestione dei cambiamenti,
- Chiara definizione delle categorie chiave del cambiamento (per esempio, il costo per le modifiche dei volumi),
- Ruoli, responsabilità e procedure decisionali per il cliente e per il fornitore per ciascuna classe di categorie chiave,
- I principali driver per le modifiche (prospettive a tre, sei e nove mesi), rivisti mensilmente,
- Potenziali implicazioni dei principali driver con i referenti chiave per parte del cliente e del fornitore,
- Obiettivi attuali delle principali iniziative (per esempio le prime tre in rilevanza) in ciascuna categoria di modifica (con una prospettiva almeno a tre mesi), il referente ed il rischio associato.

Una situazione che, in mancanza di un approccio orientato alla gestione proattiva dei cambiamenti, rischia di provocare una rottura con il fornitore, e può essere quella che si determina nella vita di quei tipici contratti di outsourcing strategico (con caratteristiche di durata di 5-7 anni, di cessione degli asset esistenti e di transizione del personale IT) che hanno il solo obiettivo di un'immediata riduzione dei costi. Alla soddisfazione per il raggiungimento dei reciproci obiettivi, scontato dopo il primo anno, può sopraggiungere nel periodo successivo l'esigenza di trovare una soluzione alternativa che superi i limiti indotti al business dalla struttura statica dell'accordo originario e argini la probabile tendenza negativa dei livelli del servizio erogato.

1.2.4.1. Come funziona la pianificazione delle modifiche

L'accordo può essere costruito sulla base del raggiungimento di una condizione di "stato costante" per i primi 12 mesi di transizione e trasformazione. Il contratto può includere meccanismi per modificare i volumi utilizzati (per esempio: costi aggiuntivi o riduzioni per modifiche ai *mips* erogati e, per i desktop, le postazioni di lavoro impegnate). Può essere inclusa anche una certa quantità di aggiornamento tecnologico (per esempio, la sostituzione del 33% di PC ogni anno), con il risultato che le modifiche tecnologiche sono dovute a nuovi requisiti che non erano normati nelle

specifiche d'uso piuttosto che ad aggiornamenti tecnologici effettivi (per esempio, integrare una nuova soluzione per un'area di business); di solito le clausole che prevedono questi tipi di modifica sono deboli e complesse nello stesso tempo.

Ne consegue che un tipico contratto di outsourcing è strutturato sulla base di un anno di trasformazione continua seguito da sei anni di evoluzione statica; questa situazione non segue la reale necessità che è spesso di un anno di "trasformazione continua" seguito da sei anni di ulteriori "trasformazioni continue".

1.2.4.2. Il Piano di innovazione

Una società segue un ciclo naturale di nascita, crescita, maturità e declino, e durante tutto questo ciclo gestisce interventi di innovazione ed iniziative di trasformazione. Ciò potrà riflettersi negli accordi di outsourcing includendo Piani di innovazione direttamente nei contratti. Sostanzialmente, un Piano di innovazione conterrà meccanismi per permettere al cliente e al fornitore di identificare insieme le opportunità e di tradurre le idee e le previsioni in azioni concrete.

Il Piano di l'innovazione descrive perciò i metodi e le procedure che un cliente e un fornitore devono utilizzare per introdurre nuovi servizi all'interno degli accordi di outsourcing, definirne i risultati attesi ed i metodi per le valutazioni economiche dei corrispettivi.

Molti sono gli argomenti che dovrebbero essere parte del Piano di innovazione e collegati con gli obiettivi strategici:

- Un processo per l'innovazione, inclusa le modalità di implementazione e le priorità;
- Un processo per l'evoluzione architetturale;
- Un processo di miglioramento del business;
- Un programma di adeguamento economico riferito all'innovazione.

L'importanza che assume la capacità di interagire con il fornitore, nel gestire le opportunità di innovazione, cresce con la strategicità del rapporto che l'azienda stabilisce con il fornitore stesso, fino anche a dipenderne. Perciò l'inclusione di Piani di innovazione nei contratti di outsourcing è la base fondamentale per poter cogliere i vantaggi delle evoluzioni architetturali e delle iniziative di business che si vengono a concretizzare nel tempo.

1.2.4.3. Valutazione dell'efficacia del servizio

In un rapporto di outsourcing, gli effetti della relazione contrattuale devono essere misurati durante tutto il ciclo di vita del contratto per verificare se l'accordo iniziale rimane rispondente alla realtà in evoluzione.

In un contratto della durata di 5-7 anni, i requisiti di business del cliente e la capacità dell'outsourcer di erogare i servizi è probabile che cambino sostanzialmente, e può essere opportuno avvalersi di una valutazione indipendente che verifichi a che punto è la loro relazione.

A fronte del risultato, che si ottiene identificando le aree di attrito o di debolezza, si svilupperanno dei piani di facilitazione al dialogo su basi concrete (i *measurement charter*) che permetteranno anche di rendere le parti consapevoli delle rispettive strategie.

I *measurement charter* contengono quindi misure tattiche delle performance del servizio e le metriche derivanti dal piano strategico del cliente. Le risultanze vanno usate come base di partenza per migliorare la relazione fin dall'inizio e, poi, per tutta la durata del rapporto contrattuale.

1.3. FATTORI CRITICI DI SUCCESSO

Si possono individuare cinque condizioni che consentono di verificare preliminarmente la compatibilità aziendale con una scelta di IT Outsourcing, e quindi le condizioni per conseguire realmente i benefici attesi o evitare potenziali rischi:

1. Il ruolo e gli obiettivi assegnati al SI aziendale

   Laddove gli obiettivi assegnati alla funzione IT siano fortemente orientati al perseguimento dell'efficienza e dei risparmi dei costi operativi aziendali è opportuno effettuare alcune considerazioni. Il modello di equilibrio economico degli outsourcer è orientato alle economie di scala nell'erogazione di servizi il più standardizzati possibile: il risparmio sui costi è quindi realistico perseguirlo in quei servizi che sono basati principalmente sul consumo di risorse tecnologiche (cpu, dischi, etc..).

   In questo senso è quindi il Facility Management quello che sembra più omogeneo con le premesse di economicità del servizio. Il contesto cambia quando nell'outsourcing si include l'evoluzione applicativa, perché la difficoltà nel prevedere la dinamicità e nello specificare le esigenze applicative si potrebbe scontrare con rigidità sia del contratto che del modello operativo dell'outsourcer, questo più orientato alle standardizzazioni che alle personalizzazioni.

2. Il clima aziendale generato dalla funzione SI

   Si riferisce alla verifica di un eventuale clima conflittuale tra la funzione dei Sistemi Informativi interna ed il resto dell'Azienda. Si tratta dei casi in cui la funzione SI non è riuscita a diventare un reale partner interno delle funzioni utenti, e questa situazione potrebbe compromettere la capacità di generare una reale partnership con l'outsourcer, fondamentale per gestire una relazione complessa e dinamica quale è quella dell'outsourcing. E' stato dimostrato che l'Outsourcing funziona bene laddove si possa riscontrare la realizzazione del concetto di "extended staffing" della funzione SI interna: in altri termini dove l'outsourcer diventa una estensione sinergica e complementare della funzione SI interna.

3. Il grado di descrivibilità oggettiva e di conoscenza interna dei servizi informatici da esternalizzare

   Le *best practice* e la letteratura e l'esperienza insegnano che esternalizzare attività critiche, poco documentabili e spesso poco conosciute, aumenta i rischi dell'operazione. Un basso grado di conoscenza interna dei servizi informatici da esternalizzare è spesso la causa di una scarsa descrizione dei servizi nonché dei livelli attesi degli stessi, con le ovvie conseguenze sulla descrizione dell'oggetto stesso del contratto e sul Service Level Agreement: il rischio qui è che questi perdano il ruolo di strumento di regolamentazione paritetica del rapporto. La soluzione, in questo caso, potrebbe essere quella di riconoscere la propria difficoltà nel descrivere i servizi in oggetto e nel farsi aiutare da esperti nello specifico settore.

4. La capacità di impostare e gestire sofisticati sistemi di controllo della relazione con l'outsourcer

   Un requisito fondamentale è la capacità di impostare e gestire sistemi complessi di controllo. Vi è la necessità di pensare non solo al controllo dei fattori di input (es. budget economico) o output (es. verifiche su SLA, penali), ma anche e sopratutto del comportamento e del processo di erogazione del servizio. E' importante progettare non solo gli istituti sanzionatori, ma anche e

soprattutto quei sistemi di controllo che permettano di prevenire il verificarsi del disservizio. Sono esempi di questi: i sistemi di normazione (raccolta e formalizzazione della documentazione, dei registri, certificazione della qualità etc..), di standardizzazione (es. delle procedure, del project management etc..), di benchmarking e di soluzioni organizzative (team, comitati etc..).

Certamente i sistemi di controllo aumentano i costi organizzativi dell'outsourtcing e questi devono essere consapevolmente condivisi dalle parti, sia perché costituiscono una seria forma di condivisione dei risultati e degli oneri, sia perché sono una forma di tutela reciproca nell'ambito del rapporto.

5. La capacità di definizione del contratto di outsourcing

   Ultimo prerequisito da verificare è la capacità di definizione del contratto che diventa il momento più critico della corretta impostazione dei servizi dell'outsourcing e dei relativi sistemi di controllo. Il contratto è di fatto il documento formale dove consolidare in forma definitiva e chiara tutte le idee, i meccanismi di controllo creati, le attività richieste e i livelli di servizio, le clausole accessorie e sanzionatorie, nonché i costi di setup del servizio. La particolare attenzione che va posta ai costi di setup, è necessaria perché spesso questi sono di impatto significativo sull'economicità concreta dell'operazione; per garantire, infatti, gli stessi livelli di servizio all'utenza aziendale, inizialmente si devono attivare in parallelo sia le risorse sia le competenze del cliente sia quelle dell'outsourcer, con un aggravio di costi nel breve termine. È evidente quindi che nella fase di start-up del servizio, la definizione del contratto deve ben riflettere una realtà nella quale generalmente l'outsourcer non è del tutto efficace (non raggiunge tutti gli obiettivi stabiliti) e l'azienda cliente non è del tutto efficiente (impiega ancora le proprie risorse mentre paga già risorse dell'outsourcer in avviamento).

2. LA SICUREZZA ED IL CONTRATTO

In questa seconda parte analizzeremo in dettaglio alcuni aspetti del processo di outsourcing focalizzandoci sulla relazione tra sicurezza ICT ed aspetti contrattuali.

Le due materie usano linguaggi assai diversi ma sono strettamente legate ed è assolutamente vitale per la buona riuscita del processo di outsourcing dare ad entrambe il dovuto peso e ruolo, anche nella fase di assessment del rischio, tramite adeguate risorse umane ed economiche.

Questa parte della trattazione è organizzata in cinque sezioni.

Nella prima sezione descriveremo alcuni aspetti legali relativi ai contratti di outsourcing ICT e alle problematiche di "sicurezza".

Nella seconda sezione descriveremo i caratteri essenziali di un contratto di outsourcing e proporremo un modello di contratto di outsourcing.

Nella terza sezione, approfondiremo il tema della riservatezza dei dati e delle informazioni, in quanto argomento di grande rilevanza.

Nella quarta sezione riprenderemo le considerazioni fatte nell'introduzione e ci soffermeremo sugli aspetti pratici e tecnici del processo di outsourcing ICT così da comprendere appieno la struttura del contratto.

Nella quinta ed ultima sezione discuteremo con un paio di esempi come è possibile formulare degli SLA che forniscano sufficienti garanzie di essere funzionali alla buona riuscita del contratto.

2.1. ASPETTI LEGALI DEI CONTRATTI ICT E DELLA SICUREZZA INFORMATICA

Parlare degli aspetti legali della sicurezza informatica significa parlare di quell'insieme di norme (leggi, decreti, regolamenti) che il legislatore nazionale e sovranazionale pongono a salvaguardia della sfera privata della persona fisica e del patrimonio informativo di aziende e istituzioni.

Possono essere inclusi in questo concetto generale anche gli standard nazionali o internazionali, che sebbene con valore non cogente, concorrono a integrare le norme vigenti in materia di sicurezza. Così come pure i codici di comportamento e di autoregolamentazione e le norme di deontologia professionale sviluppati dalle istituzioni o da gruppi organizzati (ad esempio gli ordini professionali).

Quando si parla di norme sulla sicurezza informatica si toccano i settori di Internet, del commercio elettronico, della validità e rilevanza del documento informatico, della conservazione dei documenti in formato digitale, di invoicing, della protezione dei dati personali, della tutela del software e del diritto d'autore, dell'editoria web, dei reati informatici.

Alcune di queste materie hanno visto una recente produzione legislativa e hanno suscitato enorme interesse nella dottrina. Molti sono stati i convegni e i seminari sui temi della firma elettronica e della privacy, in considerazione dell'impatto evidente di tali normative sulle procedure aziendali (implementazione delle misure di sicurezza, rapporti telematici con il Registro delle Imprese tramite la smart card distribuita ai legali rappresentanti delle società, fatturazione elettronica e conservazione digitale dei libri contabili).

Meno evidente è l'impatto che le problematiche attinenti alla sicurezza hanno nella formazione (negoziazione) e nell'esecuzione dei rapporti tra le parti di un contratto di outsourcing. Questo è l'argomento della nostra trattazione.

2.1.1 LA FORMULAZIONE DEL CONTRATTO

Il contratto è *"l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale"*. Così si esprime il nostro legislatore nell'art. 1321 c.c., che introduce il titolo II del Libro IV del Codice Civile dedicato ai contratti in generale.

Il nostro legislatore ha regolato in questa sezione del nostro Codice Civile una materia da sempre esistita: tutti i rapporti tra esseri umani, gruppi, istituzioni si basano e si sono sempre basati su un tessuto di consensi, di accordi, di contratti, appunto, che per essere tali non per forza devono essere scritti. La forma scritta è infatti prevista a pena di nullità solo per un numero chiuso di contratti tipizzati per legge (art. 1350 c.c.).

Il contratto è quindi uno degli elementi portanti della c.d. "Società Civile". Tutte le attività umane si basano su questo fondamentale istituto giuridico, al punto tale che l'esistenza dello stesso non viene talvolta neppure percepita. Solo nel momento in cui sorgano situazioni di conflitto, le parti cercano nel contratto le basi per far valere le proprie ragioni. Ed infatti lo stesso legislatore afferma il principio fondamentale secondo il quale "*il contratto ha forza di legge tra le parti"* (art. 1372 c.c.).

Spesso non esiste alcun documento scritto che comprovi l'accordo raggiunto, oppure si stipulano contratti talmente usuali e convalidati dalla prassi corrente che si utilizzano formulari standard, reperibili in commercio o predisposti dalle società venditrici, le cui "clausole" contrattuali non vengono neppure discusse tra le parti contraenti.

Esistono però alcuni contratti per i quali, sia per la loro rilevanza economica, sia per altri motivi quali una lunga durata del rapporto o una particolare complessità dei servizi, le parti contraenti negoziano accuratamente i contenuti del rapporto contrattuale in fase di costruzione, in modo tale da regolare con accuratezza i rispettivi obblighi, prestazioni e benefici e prevenire al meglio possibile eventuali controversie.

In particolare, i contratti che hanno per oggetto prodotti e servizi attinenti all'informatica hanno assunto un ruolo di notevole importanza.

Esistono già alcune clausole che si stanno stabilizzando, determinate dalle prassi che si va man mano instaurando tra gli operatori. In questo settore si assiste al fenomeno, abbastanza usuale e comprensibile, di un tentativo di standardizzazione da parte dei fornitori volto a imporre condizioni a loro favorevoli, contrapposto al tentativo dei committenti di "difendere" le proprie esigenze. Ne deriva che, in contratti di particolare rilevanza quali ad esempio quelli di outsourcing, si sviluppano spesso negoziazioni di particolare complessità, con risultati benefici per la creazione di prassi equilibrate.

2.1.2. "SICUREZZA" IN QUALI CONTRATTI?

Il tema della sicurezza si pone, in tutta la sua rilevanza, in tutte le situazioni in cui si è costretti a fidarsi di un terzo. Si può trattare dell'imbianchino, del muratore, dell'elettricista oppure di un tecnico informatico… La prima preoccupazione è: "Chi è ? Mi posso fidare ?"

Le problematiche di sicurezza si pongono alle parti contraenti in tutte quelle situazioni in cui vi sia almeno uno dei seguenti elementi:

1. accesso fisico e/o "virtuale" al domicilio dell'altra parte;
2. intromissione / permanenza all'interno dei processi aziendali;
3. sviluppo di applicazioni / nuove procedure / implementazione di know-how;
4. durata a medio o lungo termine.

Le situazioni in cui è lecito preoccuparsi della sicurezza sono quindi numerose .

Questo non significa che, automaticamente, in *tutte* queste situazioni si debba arrestare la negoziazione ed intervenire pesantemente con clausole "capestro" a tutela della sicurezza. Significa, molto più semplicemente, che l'argomento sicurezza deve essere preso in esame, magari per decidere poi che, nel caso specifico, non vale la pena di ricorrere a particolari protezioni.

E' importante essere consapevoli che una corretta valutazione dei rischi è già un notevole passo in avanti verso la prevenzione: questa attività si chiama, con terminologia ormai usuale, *"risk assessment*".

Le tipologie di contratti nei quali si pone più spesso il tema della sicurezza sono le seguenti.

L'elenco che si propone è meramente esemplificativo.

a) Contratti di fornitura di beni

Entrano in questa categoria tutti i rapporti contrattuali che hanno per oggetto la vendita di prodotti.

Se la consegna e la messa in opera/installazione dei beni acquistati richiedono l'intervento del fornitore presso i locali dell'acquirente, ecco che si possono presentare problemi che possono divenire tanto più delicati e sensibili quanto più, nei locali in questione, siano presenti dati o informazioni di natura riservata o che abbiano natura di segreto industriale o tecnologico.

Sarà quindi necessario, in questi casi, far sì che il contratto contenga opportune clausole di salvaguardia e/o precisi impegni di "non disclosure" da parte del fornitore, oppure che siano redatti distinti accordi di riservatezza nel caso in cui si utilizzino contratti standard, o non siano stati redatti contratti scritti.

b) Contratti di appalto

L'**appalto** è definito dall'art. 1655 c.c. come il contratto con il quale una parte assume, con organizzazione dei mezzi necessari e con gestione a proprio rischio, il compimento di un'opera o di un servizio verso un corrispettivo in denaro.

E' una categoria molto ampia che può comprendere attività di scarsa rilevanza e complessità, ad esempio l'imbiancatura dei locali o la pulizia degli uffici. Ma può altresì ricomprendere attività molto più complesse ed articolate, quali ad esempio la costruzione o la ristrutturazione di edifici o l'integrazione di sistemi informatici. In questi casi gli aspetti relativi alla sicurezza assumono una rilevanza notevole.

I **contratti di appalto di servizi** fanno parte della categoria dei contratti di appalto e sono caratterizzati dalla maggiore incidenza delle problematiche attinenti alla sicurezza.

Nel caso dell'appalto di servizi in generale, il tema della sicurezza può essere visto principalmente in funzione della durata o della periodicità del servizio oggetto del contratto. Ad esempio, il servizio di pulizie affidato ad una impresa esterna determina non pochi rischi legati alla sicurezza.

I servizi di sorveglianza pongono problemi ancora maggiori perché entrano nel vivo dei sistemi di sicurezza fisica, come parte integrante della stessa.

Se si parla di **appalto di servizi professionali di consulenza**, il più delle volte il problema "sicurezza" dovrebbe essere risolto all'origine quando si tratti di figure appartenenti a Ordini o Albi professionali. Il segreto professionale dell'avvocato, del commercialista o del medico, sono previsti e tutelati dal diritto positivo e dai codici di deontologia professionale degli stessi ordini. E' però da considerare con attenzione il caso in cui ci si debba rivolgere a professionisti non appartenenti a specifici ordini professionali o albi, come ad esempio il consulente marketing o di organizzazione aziendale. In questi casi sarà assai opportuno negoziare specifiche clausole di riservatezza sulle materie oggetto della consulenza.

Quando si parla di **appalto di servizi informatici**, il problema della sicurezza si pone in tutta la sua ampiezza e profondità.

Un elenco non esaustivo di servizi informatici potrebbe essere il seguente:

- *Servizi di assistenza tecnico – applicativa (spesso noti con l'efficace termine di "body rental");*
- *Servizi di manutenzione hardware;*
- *Servizi (impropriamente) definiti di"manutenzione software", che vanno dalla correzione errori fino all'implementazione di nuove funzioni;*
- *Servizi di sviluppo e/o personalizzazione del software;*

Per tutti questi servizi i problemi relativi alla sicurezza si pongono in maniera decisamente evidente.

Quando l'oggetto del contratto d'appalto è la predisposizione e/o la gestione di sistemi di sicurezza, si parla di contratto d'**appalto di servizi di sicurezza**. In questo caso si raggiunge il massimo della rilevanza dei problemi in questione. Basti solo considerare che spesso questi contratti prevedono l'intrusione a scopo di test nel sistema informatico del committente, per verificarne le difese. Il nuovo termine "ethical hacker*"* è stato coniato appositamente per definire coloro che svolgono tali tentativi di intrusione a fin di bene.

Il contratto di outsourcing di servizi informatici ricade normalmente nella disciplina prevista per l'appalto. L'outsourcer *(*appaltatore) assume l'obbligo di prestare a favore del cliente (committente), i servizi concordati con organizzazione dei mezzi necessari e gestione a proprio rischio. Si tratta quindi di un contratto con obbligazione di risultato, anche se ci sono casi molto limitati in cui, nel tentativo di limitare le responsabilità dell'appaltatore, prevalgono le obbligazioni di mezzi e il contratto si trasforma in appalto atipico.

2.2. IL CONTRATTO DI OUTSOURCING DI SERVIZI INFORMATICI

Nei contratti di outsourcing di servizi informatici, le obbligazioni assunte dal fornitore comportano, nella quasi totalità dei casi, l'accesso e l'uso di sistemi e di informazioni del committente.

Che cosa il committente può ragionevolmente pretendere? -- Che cosa il fornitore deve ragionevolmente garantire?" Queste domande possono essere considerate come i quesiti di base che ciascun contraente deve porsi. La discussione potrebbe talvolta accendersi sul concetto di ragionevolezza.

Il rapido evolvere delle tecnologie e dei mercati, la necessità di raggiungere una sempre maggiore economicità, una sempre maggiore concorrenza tra le imprese sono solo alcune fra le cause che hanno

spinto le aziende a procedere verso una sempre maggiore esternalizzazione delle strutture/funzioni informatiche.

Questa esternalizzazione sembra creare un rapporto sbilanciato a favore del fornitore, per via dell'enorme difficoltà a cambiare fornitore nel caso in cui non sia raggiunta la soddisfazione del committente. Infatti, se da un lato chi offre i servizi rischia di perdere il corrispettivo e pagare anche danni ingenti, chi esternalizza rischia di restare privo dei fattori produttivi di cui necessita, oltre a subire un danno di proporzioni difficilmente quantificabili a priori.

Per strutturare al meglio un contratto e quindi ridurre al minimo i rischi per le parti, è necessario inquadrare giuridicamente la situazione.

La struttura dei contratti può essere molto varia, in funzione delle differenti esigenze che dovessero presentarsi. Di conseguenza, alcuni contratti posso presentarsi molto lineari, altri essere più complicati ed avere al loro interno molti aspetti da disciplinare.

Il modello di contratto che proponiamo contiene alcune clausole di carattere generale (oggetto, durata, inadempimento, esonero dalle responsabilità, risoluzione delle controversie,…) e una parte speciale, contenente la descrizione degli aspetti economici e operativi più strettamente legati al servizio posto in essere.

Il contratto è accompagnato da un disciplinare tecnico (allegato), contenente la descrizione degli aspetti più strettamente tecnici e anche i livelli di servizio attesi (SLA) che descriveremo in un paragrafo successivo.

Al contratto di outsourcing potrebbero collegarsi contratti per la cessione dell'hw, del sw, del personale, ma ciò non rientra negli obiettivi di questa trattazione.

Il modello di contratto suggerito è passibile di modifiche e integrazioni legate alle esigenze del caso concreto e non si pretende di fare un elencazione esaustiva di tutto ciò che è opportuno inserire nel contratto.

L'articolato si suddivide in "n." articoli, a ciascuno dei quali potrà corrispondere un allegato tecnico che dovrà contenere la descrizione tecnica di tutto ciò che ha attinenza con l'articolo di riferimento.

Tali allegati, la cui numerazione è opportuno sia la stessa degli articoli ai quali si riferiscono, sono dominio del personale tecnico che dovrà descrivere, nel maggior dettaglio possibile, i contenuti specifici delle tematiche di riferimento. I citati allegati potranno contenere grafici, diagrammi, algoritmi e matrici e tutte quelle rappresentazioni grafiche del linguaggio tecnico che contribuiscono alla corretta rappresentazione ed interpretazione di ciò che si vuole esprimere.

2.2.1. IL CONTENUTO DEGLI ARTICOLI

Lo schema di contratto che si propone è di seguito sintetizzato:

Articolo 1 – Oggetto del Contratto

Articolo 2 – Passaggio delle consegne/Avviamento dell'attività

Articolo 3 – Decorrenza/Durata del contratto

Articolo 4 - Condizioni per la corretta esecuzione dei servizi/Garanzie per le parti

Articolo 5 – Dovere di informazione

Articolo 6 – Livelli di servizio e parametri quantitativi

Articolo 7 – Reports / Deliverables

Articolo 8 – Tutela della proprietà intellettuale

Articolo 9 – Criteri di completamento dei servizi

Articolo 10 – Risoluzione per inadempimento

Articolo 11 – Cause di esclusione dalle responsabilità

Articolo 12 – Responsabilità delle parti ed obblighi di indennizzo e manleva

Articolo 13 – Cessione del contratto e facoltà di sub-appalto

Articolo 14 – Riservatezza e protezione dei dati

Articolo 15 – Sicurezza dei dati

Articolo 16 – Facoltà di *auditing* e di accesso ai locali ed agli impianti

Articolo 17 – Corrispettivi – Fatturazione – Pagamenti

Articolo 18 – Composizione delle controversie e/o clausola arbitrale

Altre clausole generali possono contenere previsioni usuali quali la legge applicabile o eventuali accordi di esclusiva.

Vediamo nello specifico quale dovrebbe esserne il contenuto.

Articolo 1 – Oggetto del Contratto

Nell'oggetto del contratto dovrà essere descritto con precisione il contenuto dei servizi dati in outsourcing. Quindi, schematizzando, è necessario descrivere:

- cosa viene dato in outsourcing
- quali strutture informatiche sono messe a disposizione (hw e sw)
- la gestione tecnico-operativa
- la gestione sistemistico-operativa
- la prestazione di attività di manutenzione correttiva e adattativa
- l'eventuale presenza di attività di sviluppo
- l'aggiornamento tecnologico
- i servizi di interconnessione tra committente e fornitore
- la messa a disposizione della manualistica (opzionale)
- il training degli utenti (opzionale)
- i report informativi su attività di manutenzione e aggiornamento dei sistemi (opzionale)
- la pianificazione degli interventi di evoluzione dei sistemi (opzionale)

Articolo 2 – Passaggio delle consegne/Avviamento dell'attività

E’ necessario inserire tempi certi relativi al periodo di migrazione dei servizi dal committente al fornitore, definendo quindi il passaggio di consegne e l’avviamento dell’attività da parte del fornitore. E’ necessario stabilire le attività a carico delle parti e le modalità di esecuzione.

Sarebbe opportuno regolamentare anche il passaggio inverso, ovvero il ritorno eventuale dei servizi dal fornitore al committente o ad un altro fornitore alla scadenza del termine o in caso di risoluzione del contratto, per evitare spiacevoli disagi per le parti.

Articolo 3 – Decorrenza/Durata del contratto

Devono essere inserite le disposizioni relative alla decorrenza (per stabilire con esattezza il momento a partire dal quale il servizio di outsourcing viene preso in carico dall’appaltatore) e alla durata del contratto. La durata del contratto dipende da molti fattori, anche se la stabilità nel tempo è auspicabile, vista la complessità dell’esternalizzazione. Altro elemento che entra in gioco per valutare l’opportuna durata del contratto, può essere la scelta di cedere immobili o il proprio personale al fornitore.

In questa clausola possono altresì essere descritti i check-point eventualmente previsti come tappe intermedie, nonché le norme relative alla fine del contratto e le modalità di trasferimento delle attività ad altri soggetti (committente o altro fornitore subentrante).

Articolo 4 - Condizioni per la corretta esecuzione dei servizi/Garanzie per le parti

Si tratta di una clausola molto importante. Di solito contiene tutte le circostanze che vengono portate a conoscenza della controparte, sulle quali si fonda l'assetto e l'equilibrio dell'accordo. Ad esempio:

- adeguatezza delle strutture informatiche alla prestazione dei servizi;
- impiego di personale adeguato (dotato eventualmente di particolari certificazioni);
- possesso di tutte le necessarie autorizzazioni ad operare ed a prestare i servizi in oggetto;
- assenza di limiti o impedimenti derivanti da terzi per la stipula del contratto;
- esistenza di tutte le necessarie condizioni e dei necessari presupposti di sicurezza per la corretta esecuzione delle prestazioni, ecc.;
- possesso di eventuali certificazioni quali ISO, BS7799, SAS70 per l’espletamento dei servizi richiesti.

L'eventuale venire meno delle condizioni descritte o la scoperta che non erano veritiere o non lo sono più fa sì che a carico dell'inadempiente siano dovuti indennizzi e manleve, solitamente indicate in altra clausola apposita.

Articolo 5 – Dovere di informazione

Potrebbe essere opportuno inserire una clausola nella quale si prevede un obbligo di informazione per entrambe le parti in caso di modifiche legislative che obbligassero ad effettuare cambiamenti delle procedure di sicurezza e nelle modalità di prestazione dei servizi. In tal caso, potrebbe essere possibile aggiornare il contratto in corso d’opera, anche nei suoi aspetti economici, se necessario, per ottemperare agli obblighi di legge.

Articolo 6 - Livelli di servizio e parametri quantitativi

L'esattezza della prestazione da parte dell'appaltatore è subordinata al puntuale rispetto di orari e modalità di erogazione dei servizi. I parametri entro cui sono contenuti i quantitativi minimi e massimi sono stabiliti in apposito allegato disciplinare (livelli di servizio e parametri quantitativi, detti anche Service Level Agreement o SLA). In alcuni casi, ad esempio quando i servizi dell'appaltatore sono forniti tramite infrastrutture informatiche del committente, è necessario che siano stabiliti anche i livelli di servizio che il committente garantisce al fornitore sulla propria infrastruttura e/o servizi. Questi accordi sono del tutto paralleli agli SLA e sono chiamati Operation Level Agreement od OLA. I livelli di servizio possono essere espressi in percentuali minime per garantire l'erogazione dei servizi (es.: continuità del servizio, disponibilità minima del servizio tollerata in relazione a periodi definiti, tempo di presa in carico di errori/malfunzionamenti, tempo di correzione di errori/malfunzionamenti, …). Possono essere previste eventuali penalità per il mancato rispetto dei livelli di servizio dei parametri quantitativi.

E' opportuna, a questo riguardo, una annotazione: si sta sempre più diffondendo anche una clausola tipo "bonus – malus", nel senso che può essere uno strumento utile per entrambe le parti in quanto costituisce una forma di incentivazione al miglioramento di determinati livelli di servizio, impostando una sorta di *strategic leverage* per ottenere migliori risultati là dove siano ritenuti rilevanti.

Articolo 7 – Reports / Deliverables

E' necessario che siano descritti i tempi e le modalità di redazione di rapporti periodici sullo stato di avanzamento delle prestazioni, i risultati di studi di fattibilità e/o attività consulenziali (ove siano previste), come pure sviluppi e/o personalizzazioni del software esistente e preso in carico dal fornitore e relativa documentazione.

Sarebbe opportuna la creazione di commissioni congiunte che tengano monitorata l'attività di outsourcing e valutino la necessità di modifiche del contratto in corso d'opera, con incontri periodici a cadenza annuale o semestrale propedeutici alla redazione dei reports di cui sopra.

Articolo 8 – Tutela della proprietà intellettuale

In questa clausola sono fornite una serie di garanzie circa il rispetto dei diritti della proprietà intellettuale e di altri diritti di privativa industriale di terzi. Possono essere stabiliti una serie di obblighi a carico delle parti in riferimento alla tutela della proprietà intellettuale della controparte. Sono stabilite le regole per la gestione di eventuali rivendicazioni della proprietà intellettuale da parte di terzi. In questa clausola possono anche essere disciplinate eventuali modifiche o evoluzioni del software dell'appaltatore eseguite dal committente oppure esclusivamente a favore del committente e pagate interamente da quest'ultimo.

Articolo 9 – Criteri di completamento dei servizi

Si vuole, di proposito, evitare il termine di "collaudo". Questo potrà ovviamente essere incluso sotto questo articolo per tutti quei casi in cui vi sia un'attività di sviluppo di un'opera per la quale sia prevista una "conclusione".

Articolo 10 – Risoluzione per inadempimento

Questa clausola riporta casi di particolare importanza nei quali la parte non inadempiente può richiedere la risoluzione del contratto di outsourcing. Si tratta di solito di una clausola risolutiva espressa ai sensi dell'art. 1465 c.c.; è una clausola molto delicata in quanto non può essere generica, a pena di nullità. Può essere prevista una diffida ad adempiere, che contiene di solito le modalità ed i termini per intimare l'esatto adempimento alla parte inadempiente, ai sensi dell'art. 1454 c.c., pena la risoluzione del contratto di *outsourcing.*

Articolo 11 – Cause di esclusione dalle responsabilità

Questo articolo disciplina se esistono casi in cui la responsabilità delle parti è limitata o esclusa. La portata e l'estensione delle cause di esclusione e limitazione di responsabilità è soggetta ai limiti imposti dall'art. 1229 c.c.[4]

Articolo 12 - Responsabilità delle parti ed obblighi di indennizzo e manleva

Stabilisce eventuali obblighi di indennizzo e manleva delle parti e la diligenza dovuta da ciascuna nell'adempimento. In alcuni casi, per particolari settori di attività, o laddove ci si voglia riferire a criteri maggiormente impegnativi, la determinazione della diligenza è riferita a prassi particolari di settore, sia a carattere nazionale, sia anche a carattere internazionale.

Articolo 13 - Cessione del contratto e facoltà di sub-appalto

Può contenere eventuali limitazioni alla cedibilità del contratto da parte del committente o dell'appaltatore e per quest'ultimo la facoltà o meno di sub-appalto. Può contenere una clausola di recesso unilaterale a favore del committente in caso di cambio dell'assetto proprietario dell'appaltatore per evitare che si creino situazioni difficili da gestire (ad esempio nel caso in cui il nuovo fornitore sia un concorrente dell'appaltante).

Articolo 14 – Riservatezza e protezione dei dati

Oltre all'obbligo di riservatezza delle informazioni, questo articolo disciplina tutti gli aspetti relativi alla protezione dei dati personali (D. Lgs. 196/2003): contiene l'informativa ed il consenso al trattamento dei dati e, di solito, include anche la nomina del fornitore a responsabile del trattamento unitamente alle relative istruzioni scritte. Appare opportuno allegare al contratto la documentazione relativa.

Articolo 15 – Sicurezza dei dati

Questa clausola contiene tutte le procedure relative alla sicurezza (backup, disaster recovery, …) previste come minime/idonee dal D. Lgs. 196/2003.

[4] Art. 1229 Clausole di esonero da responsabilità. — È nullo qualsiasi patto che esclude o limita preventivamente la responsabilità del debitore per dolo o per colpa grave. È nullo altresì qualsiasi patto preventivo di esonero o di limitazione di responsabilità per i casi in cui il fatto del debitore e dei suoi ausiliari costituisca violazione di obblighi derivanti da norme di ordine pubblico.

Articolo 16 - Facoltà di auditing e di accesso ai locali ed agli impianti

E' importante stabilire se e con che modalità il committente può controllare, anche presso i locali dell'appaltatore, l'adeguatezza delle strutture, delle procedure e di tutto ciò che è predisposto al fine della buona esecuzione degli obblighi contrattuali.

Articolo 17 - Corrispettivi – Fatturazione – Pagamenti

Sotto questo titolo, nell'Articolato, dovranno essere riportate solamente le norme generali sulla tematica, quali ad esempio, quelle che disciplinano il calcolo dei corrispettivi (canone annuo, tariffe, prezzi unitari per singole attività compiute, addebiti "cost plus", ecc., ma senza inserire nell'Articolato i valori numerici. Questi ultimi dovranno essere riportati tutti – e solo – nell'Allegato, eventualmente anche mediante l'ausilio di formule, matrici o tabelle.

Articolo 18 - Composizione delle controversie e/o clausola arbitrale

Questa clausola contiene la disciplina dei meccanismi di consultazione tra le parti volti ad assicurare una rapida soluzione ad eventuali controversie sorte tra le parti circa le modalità di esecuzione del contratto.

Altre clausole generali

Possono contenere previsioni usuali quali legge applicabile ed eventuali accordi di esclusiva.

Lo schema proposto è una guida logica non solo per la redazione del contratto, ma anche per la conduzione della negoziazione.

Nei casi in cui uno dei due team riesca ad impostare, a livello di contrattazione, la sequenza delle tematiche da discutere e risolvere secondo lo schema descritto, il risultato può essere coerente con le posizioni delle due parti. La rigorosa suddivisione tra Articolato ed allegati tecnici aiuta a coordinare tra loro i due diversi "linguaggi", legale e tecnico, facilitando la comprensione dell'accordo.

La stessa rigorosa suddivisione permette la flessibilità e la dinamica contrattuale. Appare infatti evidente che una buona parte – forse la maggior parte – dei necessari adeguamenti o modifiche in corso d'opera, possono essere realizzati attraverso la modifica dei soli allegati, senza necessità di revisioni contrattuali che, per loro natura, comportano procedure molto più lunghe e laboriose.

2.3. LA RISERVATEZZA DEI DATI E DELLE INFORMAZIONI

Stante la rilevanza della problematica, si ritiene opportuno ragionare in particolar modo sul tema della riservatezza di cui all'articolo 14 del modello contrattuale proposto.

Ai soli fini di questa trattazione – senza cioè pretendere di darne un valore assoluto – si propongono le seguenti due definizioni:

- con il termine "**Dati**" si intende un insieme di elementi alfanumerici (in gergo, "stringhe") suscettibili di essere inseriti in un sistema di elaborazione, per essere memorizzati, elaborati, gestiti, trasmessi, ecc.;
- con il termine "**Informazioni**" si intende un insieme aggregato di dati tale che chi ne entra in possesso viene a conoscenza di una o più nozioni con un significato.

Due esempi possono meglio chiarire quanto sopra indicato.

Una stringa di 8 – 10 numeri ed un'altra di caratteri alfabetici che corrisponda al nome e cognome di una persona ("Dati"), di per sé non dicono molto. Ma se le due stringhe in questione vengono aggregate in un certo modo, chi ne prenderà visione potrà conoscere, ad esempio, il numero telefonico di una persona ("Informazione").

Altro esempio: un elenco di "N" nominativi di Società non costituisce di per sé alcuna informazione di carattere riservato, essendo tutti nomi noti e reperibili in qualsiasi elenco telefonico. Se, però, questo elenco viene presentato con il titolo di "Lista dei clienti della Spett. DITTA", l'elenco in questione costituisce un'informazione altamente riservata della società "DITTA".

Sia i "Dati" che le "Informazioni" dovranno quindi essere protetti e salvaguardati.

2.3.1. SICUREZZA E PROTEZIONE DEI "DATI" E DELLE "INFORMAZIONI"

I Dati e il sistema che li contiene (Sistema Informativo) dovranno essere protetti contro tutte le cause (agenti esterni o interni al sistema) che ne possano pregiudicare l'integrità, l'accessibilità, l'uso ed i risultati attesi dal proprietario e/o da chi, legittimamente, debba fruire dei risultati delle elaborazioni svolte.

La protezione dovrà riguardare le intromissioni dolose e gli attacchi da virus; ma anche i casi di deterioramento o perdita di dati determinati da errori umani dovuti a imperizia o negligenza, inconvenienti tecnici, fatti accidentali o fortuiti. Con la conseguente necessità di proteggere il sistema e di creare procedure di backup, recovery, ecc., allo scopo di limitare le perdite e/o gli accessi indesiderati e consentire la ripresa o la prosecuzione delle attività in corso nel più breve tempo possibile. La protezione dei Dati deve essere attiva naturalmente non solo quando essi risiedono sui supporti di memorizzazione, ma anche nei momenti in cui essi transitano su linee di trasmissione dati.

I fornitori di tecnologia hanno sviluppato e continuano a sviluppare ed aggiornare una serie di strumenti di sicurezza fisica e logica, quali sistemi di crittografia, sistemi di autenticazione, firewall, sistemi antivirus e antispyware con lo scopo di rendere massima la sicurezza dei dati.

Per "Riservatezza delle Informazioni" intendiamo in questo contesto uno step successivo alla sicurezza del dato puro: parliamo di una riservatezza di carattere soggettivo.

Ci spieghiamo meglio: il fornitore dei servizi deve poter accedere a informazioni di proprietà del committente. È evidente che chiunque debba, per contratto, effettuare un determinato servizio (ad esempio sviluppare o personalizzare un software applicativo) deve conoscere quali siano gli obiettivi di risultato finale, le metodologie, le modalità di funzionamento: in definitiva, ciò che potrebbe essere definito come "l'intimità" aziendale del servizio di cui si tratta e i legami del servizio stesso con gli altri processi aziendali. Quindi ciò che si richiede al fornitore di servizi è una confidenzialità ulteriore rispetto alla limitazione degli accessi al dato puro e semplice, che potrà essere garantita solo tramite appropriate clausole di riservatezza e non tramite strumenti di sicurezza fisica e logica. La protezione potrà essere garantita da qui in avanti, solo a livello contrattuale. Inoltre, il contenuto delle

obbligazioni che dovranno essere richieste/pretese dal fornitore si riferisce esclusivamente a comportamenti umani delle persone del fornitore stesso e dei suoi eventuali sub-fornitori.

Per quanto riguarda la "Sicurezza e protezione dei Dati", l'oggetto delle protezioni da definire e da tradurre in clausole contrattuali si riferisce in prevalenza a specifiche e requisiti di tipo tecnico, la cui gestione e responsabilità compete primariamente al "proprietario" del sistema. Al fornitore dovranno quindi essere date le specifiche tecniche alle quali esso dovrà attenersi nello sviluppo delle attività di sua competenza.

Quando si parla di sicurezza dei dati non è possibile non fare cenno a quanto previsto dal Codice in materia di protezione dei dati personali (D. Lgs. 196/2003). Gli obblighi di sicurezza sono previsti negli artt. 31 a 36 e nell'Allegato B al Codice.

L'art. 31 è posto come norma generale a garanzia dei dati personali oggetto di trattamento. Tali dati devono essere custoditi e controllati, in base alle conoscenze acquisite mediante il progresso tecnico e all'importanza dei dati trattati, in modo da ridurre al minimo, tramite l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta. Le "idonee e preventive misure di sicurezza" sono quelle che preservano il titolare del trattamento dalla responsabilità civile (art. 15 del D. Lgs. 196/2003).

Per garantire il livello di sicurezza "idoneo" difficilmente basta mettere in opera le misure minime di sicurezza previste dall'art. 33. Le misure minime di sicurezza infatti prevedono il livello minimo di protezione dei dati personali, quello considerato essenziale dal legislatore al di sotto del quale non è possibile scendere a pena di sanzioni penali. Tali misure sono descritte nel disciplinare tecnico (Allegato B).

Il livello idoneo di sicurezza dei dati sarà tanto maggiore quanto maggiore sarà l'importanza dei dati trattati.

La protezione dei dati, quindi l'adozione delle misure di sicurezza, è compito primario del titolare del trattamento dei dati personali. Nei casi in cui il titolare del trattamento si avvale della collaborazione/assistenza di persone fisiche/giuridiche in outsourcing, esse saranno nominate "responsabile del trattamento dei dati in outsourcing", in quanto accedendo a dati personali, dovranno dare garanzie sul corretto trattamento dei dati stessi. In tal caso, il titolare del trattamento dovrà dare istruzioni scritte e vigilare sull'adozione delle misure da parte del responsabile.

Nel momento in cui, quindi, il committente decide di rivolgersi ad una terza parte per lo svolgimento di attività o servizi attinenti al suo sistema informatico, bisognerà valutare a priori quali misure devono essere attivate, con che modalità, che controlli il titolare può/deve effettuare e come suddividere le responsabilità (se possono essere suddivise). Le misure di sicurezza dipendono infatti, per la maggior parte dei casi, dal servizio posto in essere. Potranno esserci alcuni aspetti relativi alla sicurezza a carico del committente. Il più delle volte vi saranno aspetti a carico del committente e altri a carico del fornitore. Sarà molto importante cercare di attribuire alle parti le eventuali responsabilità derivanti da un errato trattamento dei dati. La domanda da porsi è: *a chi spetta cosa*? In alcuni casi potrà non essere facile rispondere a questa domanda.

Ai sensi degli articoli 42- 45 del nuovo codice in materia di privacy, è necessario prestare particolare attenzione nel passaggio dei dati (supponendo che tra i dati siano contenuti dati considerati "personali") quando l'outsourcer è straniero.

Infatti, se per quanto riguarda i Paesi della Comunità Europea non esistono limitazioni alla circolazione dei dati, il trasferimento di dati (anche solo temporaneo) in Paesi non UE è concesso solo

in determinati casi (consenso dell'interessato, obblighi contrattuali, salvaguardia dell'interesse pubblico, ecc., di articolo 43 D. Lgs. 196/2003), oppure deve essere autorizzato specificamente dal Garante. Il fine è quello di garantire che il livello di tutela della privacy sia lo stesso di quello previsto in Italia.

A tale proposito si segnala che la valutazione sull'adeguatezza della tutela è già stata sancita per i seguenti Stati non europei:

- Argentina
- Canada
- Svizzera
- US
- Guernsey
- Isola di Man

L'UE ha predisposto alcune clausole tipo da utilizzare nel trasferimento di dati personali verso Paesi Terzi consultabili all'indirizzo:

http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm.

2.3.2. LA DEFINIZIONE DELLE SPECIFICHE TECNICHE

Nella fase di negoziazione di un contratto sarà compito del titolare del trattamento dei dati definire in modo preciso ed inequivocabile le specifiche tecniche del sistema di sicurezza, così da garantire il livello idoneo di sicurezza in base alla natura e all'importanza dei dati trattati. Naturalmente è auspicabile che ci sia la massima collaborazione tra le parti così da comprendere appieno quali potrebbero essere i punti di debolezza del sistema.

Il fornitore, chiamato a svolgere attività di servizi professionali o di sviluppo o comunque interventi nelle strutture informatiche ed organizzative del titolare, dovrà quindi attenersi a tali specifiche ed operare in modo che i risultati del lavoro svolto siano coerenti con le specifiche stesse, a meno che il titolare stesso deleghi al fornitore proprio lo studio e la messa in opera delle misure di sicurezza. In tal caso il fornitore avrà un ruolo più rilevante e non dovrà limitarsi al puro rispetto delle specifiche del titolare ma dare vita alle migliori soluzioni di sicurezza possibili. In caso di outsourcing del sistema informatico del titolare presso i locali del fornitore, è necessario che il titolare ritenga adeguate le misure di sicurezza del fornitore.

Le specifiche tecniche possono riguardare aree o campi di natura diversa. Esse potranno riguardare requisiti attinenti alla sicurezza fisica, cioè a tutto quanto riguardi il controllo degli accessi, l'identificazione delle persone, le procedure di accesso e di conservazione di determinati documenti e supporti, etc; ma anche requisiti attinenti alla sicurezza logica cioè specifiche riguardanti le misure in atto per la salvaguardia del sistema e dei dati in esso contenuti (ad esempio firewall, sistemi di intrusion detection, etc.).

Sarà compito specifico del titolare far sì che il fornitore riceva tutte le specifiche alle quali il personale del fornitore dovrà attenersi nell'esecuzione del contratto e dare ogni supporto affinché tali specifiche vengano implementate nel modo corretto.

E' quindi chiaro che il cliente potrà "pretendere" la formalizzazione di determinate condizioni solo se il fornitore sarà messo nella condizione di conoscere ed accettare le specifiche che dovranno regolare le attività di esecuzione delle obbligazioni contrattuali. In prevalenza si tratterà di specifiche di natura tecnica, che il fornitore si impegnerà a rispettare.

Nella prassi comune si deve purtroppo riconoscere che la negoziazione di molti contratti, anche importanti, si focalizza spesso sull'aspetto economico ("…quanto mi costa"), e sui "precedenti" ("…abbiamo fatto sempre così"), senza prendere in considerazione gli aspetti di novità che lo sviluppo della tecnologia e del "business" continuano a proporre come sfide a chi ha la responsabilità delle strategie aziendali e soprattutto senza prendere in adeguata considerazione i fattori di rischio legati alla scelta e alla tipologia di contratto.

Il comportamento irrinunciabile a tale riguardo è quello di prevedere sempre una fase di "risk assessment", anche di carattere legale (il rischio legale è pressoché sempre dimenticato!), in quanto è molto importante agire preventivamente per non rischiare di causare danno a sé stessi o a terzi.

Si è già detto che, a differenza della protezione dei dati, nel caso delle informazioni l'elemento saliente è dato dalla necessità di regolare i comportamenti umani.

Il problema della riservatezza delle informazioni si pone in quanto esse sono, per definizione, o già conosciute, o comunque accessibili, da parte di persone nei confronti delle quali tale protezione deve essere attuata. I comportamenti umani sono quelli più difficili da regolare per contratto, in quanto l'azione preventiva delle clausole contrattuali può funzionare solo se:

- l'informazione è comunicata a tutti coloro che devono mantenere la riservatezza (il fornitore in primo luogo, ma altresì i dipendenti/collaboratori/consulenti esterni del fornitore, eventuali subfornitori, eventuali terzi che per qualsiasi motivo dovessero intervenire operativamente);
- esistono delle precise responsabilità per coloro che non dovessero rispettare gli accordi di riservatezza previsti;
- esistono delle sanzioni (civili oppure disciplinari) previste per l'inottemperanza degli obblighi ed esiste la percezione che le sanzioni saranno applicate.

In mancanza anche soltanto di uno di questi elementi, le clausole contrattuali non funzioneranno e il comportamento umano potrà costituire davvero l'anello debole della catena.

La prassi contrattuale, soprattutto per le influenze derivanti dai contratti nordamericani, ha sviluppato una certa serie di clausole che, nella maggior parte dei casi, riescono a realizzare una protezione accettabile. Il paragrafo successivo ne fornisce una descrizione sintetica.

2.3.3. LA CLAUSOLA SULLA RISERVATEZZA

La clausola di riservatezza disciplina in dettaglio tutti gli aspetti, molto delicati, relativi a:

- quali informazioni siano da considerare riservate
- quali limitazioni alla riservatezza esistono e i casi in cui le limitazioni alla riservatezza possono essere considerate non applicabili
- periodo durante il quale tali informazioni devono mantenersi riservate
- eventuale penale prevista in caso di mancato rispetto dell'obbligo di riservatezza.

1. Un primo punto consiste nello stabilire *quali siano le Informazioni Riservate*

   Affermare che *"tutte le informazioni"* acquisite durante lo svolgimento del contratto sono riservate equivale, in pratica, a dire che nulla è riservato. In molti casi, l'eccesso di "protezione" si risolve, nel momento in cui si debba interpretare il contratto in sede di contenzioso, in una assenza di protezione, dando spazio a diatribe legali lunghe ed estenuanti.

   E' quindi buona norma stabilire, almeno per macro–categorie, quali siano le informazioni che debbano essere qualificate come "riservate". Questo può essere realizzato attraverso due diverse metodologie:

   a) Definire riservate, tutte quelle informazioni che:

   - siano definite, nei supporti cartacei od altro, come "Riservate", "Confidenziali", o altre indicazioni consimili, e/o
   - tutte le informazioni riguardanti determinate materie, quali ad esempio: i processi produttivi del committente, le informazioni sulle strategie commerciali, i dati numerici e/o statistici riguardanti l'attività commerciale, quelli relativi al personale, eccetera.

   b) Definire riservate tutte le informazioni derivanti da particolari situazioni per le quali sia opportuno stipulare un apposito "non disclosure agreement" per attività da parte di terzi fornitori (o comunque coinvolti) che comportino l'accesso a veri e propri segreti industriali. Questo "non disclosure agreement" si concretizza in un accordo scritto che deve essere firmato, prima che venga concesso loro accesso alle informazioni riservate di cui trattasi.

2. Deve essere precisato quali informazioni non dovranno essere considerate come riservate. In linea generale, non sono informazioni riservate quelle che abbiano le seguenti caratteristiche:
   - siano già, o divengano – ma non a causa di violazione – di dominio pubblico;
   - siano già in possesso della controparte:
   - vengano in possesso della controparte con regole basate su concetti di "non" confidenzialità che coinvolgono anche fonti esterne.

   Viene spesso inserita la precisazione che l'obbligo di riservatezza decade nel caso di richiesta da parte di autorità pubblica (forze dell'ordine). Tale precisazione è opportuna ma non è indispensabile in quanto non ci si può sottrarre all'obbligo di comunicazione alle forze dell'ordine. Si può regolare contrattualmente un obbligo di comunicazione/informazione all'altra parte di tale richiesta da parte della autorità pubblica.

   Le clausole sulla riservatezza comportano l'obbligo in capo al fornitore di trasferire validamente tali obblighi di riservatezza ai propri dipendenti/collaboratori/consulenti esterni o sub-fornitori impegnati nell'esecuzione dei servizi.

   Questo trasferimento si dovrebbe concretizzare in opportune dichiarazioni da far sottoscrivere ai dipendenti/collaboratori/consulenti esterni o sub-fornitori, che il committente deve (*dovrebbe*) pretendere di avere in copia.

   Molte aziende descrivono il contenuto nella clausola contrattuale sulla riservatezza enunciando il principio che *"le informazioni verranno trattate con lo stesso grado di cura e riservatezza impiegato per le informazioni riservate della Azienda Fornitrice"*.

   E' un parametro di riferimento che può funzionare se l'azienda fornitrice ha al suo interno validi metodi di controllo e procedure di gestione delle problematiche che dovessero nascere

sull'argomento. Da questo punto di vista, una certificazione di qualità che preveda tali procedure è certamente un elemento qualificante poiché dà al rapporto contrattuale un riferimento interpretativo certo.

3. E' infine opportuno stabilire un termine per l'obbligazione di riservatezza. L'impegno a rispettare tale obbligo deve esistere durante lo svolgimento degli obblighi contrattuali e deve sopravvivere al termine del contratto. Di norma, un periodo dai tre ai cinque anni è sufficiente a tutelare il committente.

4. Può essere previsto il pagamento di una penale in caso di mancato rispetto degli obblighi. Tale penale prescinde dal risarcimento del danno. E' importante che la penale prevista sia economicamente commisurata all'importanza delle informazioni riservate, per evitare che la penale stessa diventi motivo di contestazione.

   La penale sarà accettata solo se il fornitore percepirà che tutti gli elementi della clausola di riservatezza (contenuto, durata, limitazioni, ecc.) lo tutelano da un livello di responsabilità troppo elevato.

2.4. LA SICUREZZA NEI SERVIZI DI OUTSOURCING ICT

Cerchiamo di chiarire meglio ora cosa si intende per *Sicurezza* nell'ambito dell'Outsourcing ICT, in modo da completare il quadro delineato nei suoi aspetti legali.

Abbiamo visto che i punti caratteristici di un servizio di outsourcing ICT sono:

- l'affidamento all'esterno di tutto – o di una parte sostanziale – di un processo aziendale;
- per un periodo di durata medio-lunga.

Cosa significa *sicurezza* quando tutto un processo aziendale è affidato ad altri?

Uno degli aspetti fondamentali della sicurezza è il controllo in modo da poter istituire le regole, verificarne l'attuazione e così via. Tutto ciò è molto difficile, se non impossibile, quando tutto il processo aziendale da controllare è gestito da altri, perché di norma non si ha la possibilità di accedere direttamente alle strutture di imposizione e controllo.

Segue un esempio per chiarire la problematica:

Supponiamo che una azienda dia in outsourcing il processo aziendale "Amministrazione", compresa la gestione di tutti i documenti elettronici relativi ai contratti di acquisto e vendita (Gestionale, Supply Chain, Budget, CRM, etc.).

Per far questo, l'azienda esternalizza funzionalità che sono realizzate attraverso l'utilizzo di software (programmi), utilizzato dagli operatori del cliente, eseguito su hardware (elaboratori) che è gestito, controllato e mantenuto da operatori tecnici. Vi sono alcuni elaboratori su cui sono eseguiti dei programmi che vengono dismessi o trasferiti in blocco ad altri e vi sono nuove funzioni introdotte in azienda offerte da programmi eseguiti su elaboratori altrui.

Un servizio in outsourcing è generalmente realizzato nel seguente modo:

- il fornitore ha (in proprietà, leasing, comodato d'uso, ecc.) gli elaboratori;

- il fornitore ha le licenze per eseguire su questi elaboratori dei programmi;
- il fornitore ha il personale tecnico per configurare, gestire, controllare e mantenere sia gli elaboratori sia i programmi, nel caso anche tramite servizi sub-appaltati a terze parti;
- gli operatori del cliente collegano i propri terminali agli elaboratori del fornitore per eseguire le operazioni necessarie al processo aziendale in questione.

I terminali del cliente possono essere connessi agli elaboratori del fornitore direttamente, se questi ultimi sono in loco, oppure in via remota con linee di trasmissione dati dedicate o via internet (con accessi protetti quali VPN cifrate); per utilizzare le applicazioni spesso è necessaria la presenza di un programma client installato sui terminali del cliente per l'accesso alle applicazioni del fornitore.

Ciò che preme sottolineare è che il cliente ha un "client", cioè di norma un PC sul quale è installato un programma apposito (anche auto-installato via web, ad esempio nel caso di applicazioni Java) sul quale non vi sono né dati né vengono realizzate elaborazioni e che quindi funziona solo da terminale. Tutti i dati risiedono sull'elaboratore del fornitore, sul quale avvengono tutte le elaborazioni.

Dal punto di vista della sicurezza, il cliente ha delle esigenze minimali, tra cui, ad esempio, le seguenti:

1. il cliente vuole che alcuni dei propri operatori possano accedere ad alcuni dati, altri ad altri dati, altri ancora possano leggere ma non modificare dei dati, altri possano utilizzare alcune funzioni ma non altre, e così via;
2. il cliente vuole sapere chi, fra i propri operatori, ha fatto alcune operazioni e quando;
3. il cliente vuole sapere chi tra il personale tecnico che gestisce gli elaboratori e gli applicativi può avere accesso ai dati ivi contenuti ed in quali modalità, quando questo succede, ecc.;
4. il cliente vuole sapere e controllare come vengono assegnate e gestite le credenziali di tutti coloro che possono accedere in qualunque modo ai propri dati;
5. il cliente vuole sapere il livello di manutenzione dei programmi, le patch applicate, le versioni utilizzate, ecc.;
6. il cliente vuole essere informato di attacchi al sistema, di violazioni dello stesso, oltre ovviamente a problemi tecnici, guasti malfunzionamenti eccetera che possano avere conseguenze dirette o indirette sulla sicurezza, intesa anche come interruzione del servizio o corruzione di dati.

L'elenco non è esaustivo: si potrebbe parlare anche di backup dei dati, continuità di servizio, disaster recovery ecc..

Il punto essenziale è che tutte le funzioni di gestione, verifica e controllo sugli elaboratori, sugli applicativi e sui dati sono saldamente nelle mani del fornitore ed il cliente generalmente non ha nessun accesso diretto ad essi. Come fa il cliente a verificare che la gestione degli accessi e delle credenziali di accesso sono conformi alle proprie politiche di sicurezza? Come fa a verificare che la configurazione dei sistemi operativi e degli applicativi soddisfano requisiti di sicurezza sufficienti? Come fa a verificare che le patch sono applicate nei tempi e nelle modalità migliori?

Nel caso di outsourcing di un servizio ICT è impossibile gestire o anche solo controllare *direttamente* la sicurezza perchè non si ha il controllo né sull'hardware né sul software.

Inoltre, visto che un contratto di outsourcing è di durata medio-lunga, il cliente non ha interesse a mantenere presso di sé personale tecnico specializzato per una funzione che non ha più al proprio

interno e quindi provvede alla dismissione dell'intero ramo di azienda relativo, passando il personale all'outsourcer. In alcuni casi le varie aziende decidono di creare una terza società a cui ognuna cede il proprio ramo di azienda, personale incluso, in modo da far confluire tutte le risorse in un unica società esterna, compartecipata.

Anche nel caso in cui il personale non venga trasferito all'outsourcer ma mantenuto al proprio interno, il personale viene adibito ad altre funzioni e con il tempo il know-how specifico relativo alla funzione dismessa viene perso.

A questo punto l'azienda non solo non ha più il controllo sull'hardware e sul software, ma non ha più neppure le competenze interne per poter valutare la sicurezza, in tutti i suoi aspetti, e la qualità del servizio ricevuto. In una tale situazione la dipendenza del cliente dal fornitore è totale. La situazione può aggravarsi ulteriormente poiché vi è il rischio reale che le politiche di sicurezza dell'azienda cliente finiscano per non considerare più i possibili problemi relativi ai servizi esternalizzati. Così, non solo l'azienda non valuta la sicurezza e la qualità dei servizi dati in outsourcing, ma potrebbe venir meno altresì la percezione della necessità di valutare e controllare il servizio ricevuto. Questa conclusione potrebbe sembrare catastrofica, ma il rischio è reale nei casi in cui il management si concentri solo sull'effetto economico positivo dell'outsourcing.

2.4.1. UNA SOLUZIONE NON REALIZZABILE …

La soluzione potrebbe essere quella di dare al cliente la possibilità di avere alcune funzioni di controllo e verifica diretta presso il fornitore. Ad esempio, dargli la possibilità di accedere direttamente alle macchine del fornitore in qualità di amministratore oppure di auditor. Questa soluzione, tecnicamente possibile ma talvolta di non semplice implementazione, si scontra con alcuni ostacoli che la rendono praticamente non realizzabile.

Innanzitutto questa soluzione richiede che il cliente mantenga delle figure professionali tecniche qualificate in grado di fare le verifiche. Anche se per queste funzioni può essere richiesto meno personale che per la gestione interna dei servizi, questo è un onere che il cliente non è disposto a sostenere in quanto l'abbassamento dei costi è uno dei motivi che l'hanno spinto a ricorrere alla soluzione di outsourcing.

In secondo luogo, la ragione per cui il fornitore di outsourcing dovrebbe offrire un servizio conveniente e migliore rispetto a quello gestito internamente, sta nel fatto che lo stesso servizio è offerto a più clienti e si realizzano delle economie di scala. Inoltre, il fornitore può offrire servizi più avanzati e qualitativamente migliori perchè si specializza nella fornitura di servizi che per i clienti sono solo servizi di supporto, seppur importanti, al core-business. Non è quindi possibile che il fornitore dia ad ogni cliente la possibilità di accesso diretto alle proprie macchine secondo le procedure e le politiche di sicurezza di ciascuno di essi. Al contrario, il fornitore deve stabilire le politiche che devono essere applicate a tutti i propri clienti. Inoltre, le risorse presso il fornitore sono condivise e ciò è necessario per poter realizzare le necessarie economie di scala. Se le risorse sono condivise è necessario che il fornitore limiti fortemente le possibilità di accesso dei clienti, non solo per evitare che uno di questi sottragga risorse agli altri, ma anche per evitare che si possano creare situazioni di accesso ai dati non autorizzato. Il fornitore ha quindi il difficile compito di gestire risorse condivise mantenendo al contempo una netta separazione fra i clienti. Questo è un compito delicato, non semplice e in totale contraddizione con la possibilità di autorizzare ogni cliente ad effettuare direttamente le proprie attività di gestione e verifica.

Un ultimo ostacolo alla soluzione indicata è dato da possibili contrasti tra fornitore e cliente. La possibilità che un cliente possa verificare direttamente le configurazioni, le procedure e la gestione dell'hardware e del software del fornitore è sicuramente una fonte di conflitti fra le parti e renderebbe sicuramente più difficile la gestione del servizio di outsourcing.

2.4.2. …E LA SOLUZIONE CONTRATTUALE

Un'alternativa valida a quanto sopra esposto è che tutto ciò che riguarda la sicurezza dei servizi dati in outsourcing sia regolato dal contratto tra le parti, come esposto nei paragrafi precedenti.

E' molto importante che ci sia chiarezza sul contenuto del contratto: deve essere chiaramente indicato l'oggetto dei servizi e le procedure di erogazione degli stessi.

Bisogna tenere conto del fatto che un contratto di outsourcing è normalmente di lunga durata e che quindi sia le esigenze del committente sia le modalità di fornitura del servizio cambieranno nel tempo adeguandosi alle nuove tecnologie del fornitore e nuove attività del committente. Per questo motivo il contratto deve esser sì specifico sull'oggetto dei servizi, ma al contempo sufficientemente elastico da prevedere modifiche future.

Un punto che troppo spesso viene sottostimato, è la complessità del processo di *TakeOver*, nel caso di dismissione di un processo già esistente in azienda o di avvio del nuovo servizio.

E' quasi sempre necessario realizzare un modello di prova utilizzando dati reali e simulando l'attività e le normali transazioni. E' inoltre necessario pianificare dettagliatamente i tempi del processo di transizione, i tempi e le modalità di verifica che la transizione sia stata effettuata correttamente. Bisogna immaginare il verificarsi di problemi imprevisti e la possibilità di ritornare al servizio interno (*RollBack*) qualora nel *TakeOver* si rilevassero problemi non immediatamente risolvibili. Questo ovviamente richiede una dettagliata pianificazione dei backup dei dati, delle configurazioni delle macchine, delle procedure di *TakeOver* e di *RollBack* del processo di avvio (transizione al nuovo fornitore) in modo che nessun dato venga perso. Ovviamente bisogna tenere conto dell'eventuale interruzione dei servizi con conseguente valutazione dei rischi associati e degli eventuali danni.

Ma se il *TakeOver* è importante, ancora più importante è il ri-trasferimento dei servizi al termine del contratto.

Ciò può avvenire in almeno tre situazioni.

Nella prima si arriva alla risoluzione del contratto a causa di un contenzioso tra le parti. In questo caso l'altra parte si limiterà a svolgere le azioni strettamente indispensabili, ovvero ciò a cui è obbligata per contratto, senza concedere *favori.*

Nella seconda situazione il contratto si conclude naturalmente con il favore e la soddisfazione delle parti. Tuttavia, essendo il contratto concluso, il fornitore non ha interesse ad impegnarsi per un cliente che ha perso ed il committente non ha interesse a lavorare in sinergia con un fornitore che non lo interessa più. In entrambi i casi, quindi, il rischio che questa fase possa produrre danni anche gravi ad entrambi è notevole e spesso sottostimato.

Vi è un terzo caso, il più rischioso, nel quale una delle due parti fallisce ed interrompe, spesso quasi senza avviso alcuno, di erogare o usufruire del servizio. In caso di fallimento del cliente, il rischio per il fornitore è quasi essenzialmente economico e facilmente valutabile; in caso di fallimento del

fornitore invece, la situazione è molto più critica poiché l'interruzione di un servizio essenziale per il funzionamento dell'azienda potrebbe portare al fallimento anche del committente![5]

Ovviamente sia il committente sia il fornitore devono considerare questi scenari, valutarne i rischi ed inserire nel contratto clausole che possano evitarli o almeno ridurli. Ad esempio, dal punto di vista del committente può essere utile farsi consegnare periodicamente i backup di tutti i dati ed avere le licenze degli applicativi che li trattano in modo, in caso estremo, da poter ricreare il servizio altrove. Nel contratto devono essere indicate le procedure con cui i servizi ed i dati sono riconsegnati al committente al termine del contratto o trasferiti al nuovo fornitore, con esplicita menzione delle responsabilità di entrambe le parti in questo processo. Vanno regolamentate anche le tempistiche in cui ciò deve essere fatto. Anche questa parte del contratto deve essere rivista periodicamente tenendo conto di tutte le modifiche che durante il trascorrere del tempo verranno apportate al servizio.

E' pertanto utile stabilire a priori una periodica revisione del contratto in corso d'opera per evitare che, con il passare del tempo, il servizio effettivamente erogato ed utilizzato si discosti da quello effettivamente descritto nel contratto.

2.4.3. I SERVIZI E GLI SLA

E' opportuno approfondire la problematica della descrizione dei servizi, soprattutto dal punto di vista della *sicurezza*.

In linea di principio, committente e fornitore potrebbero accordarsi unicamente su come dividersi le responsabilità per il corretto funzionamento del servizio. Questo potrebbe realizzarsi nell'impegno del fornitore a fornire il servizio sempre nei tempi accordati e nelle modalità accordate ed analogamente il committente ad utilizzarlo nei modi dovuti e solo per gli scopi descritti. Una divisione chiara delle responsabilità è assolutamente necessaria, ma spesso non è sufficiente. Infatti l'interpretazione delle norme può essere problematica.

Per rendere più concreti i principi generali è sicuramente consigliabile riferirsi a norme internazionali, standard e certificazioni.

È buona cosa che le parti abbiano certificazioni di qualità dei servizi secondo le norme ISO e processi di trattamento delle informazioni quali BS7799/ISO17799/ISO27001, ma anche certificazioni del personale sia per il software sia per l'hardware utilizzato, per l'amministrazione dei sistemi e così via. È utile che il personale del committente sia certificato, od almeno abbia seguito dei corsi di addestramento, nell'utilizzo delle applicazioni del fornitore. È necessario che nel contratto vengano specificate le certificazioni sia a livello aziendale sia del personale, i corsi di addestramento necessari e la loro periodicità.

Ma questo, anche se molto utile, ancora non basta.

Ogni contratto di outsourcing ha alcune caratteristiche specifiche che dipendono dai servizi erogati da quel fornitore a quel committente. E' necessario pertanto che committente e fornitore individuino dei parametri che siano chiari, non ambigui, per entrambi sui quali valutare i servizi erogati e le modalità di realizzazione degli stessi: da qui nascono i Service Level Agreement, detti comunemente SLA.

[5] Al lettore che si chieda cosa questo abbia a che fare con la sicurezza ICT, ricordiamo che queste sono tematiche affrontate dalla Business Continuity e Disaster Recovery.

Anche se gli SLA sono spesso offerti dai fornitori in modo quasi propagandistico a garanzia dei servizi che offrono, il vero ruolo che possono giocare in un contratto di outsourcing è quello di formulare delle precise regole qualitative e quantitative di misura.

Ciò che ci proponiamo di fare in questa sede è dare alcuni esempi e indicazioni di massima di come gli SLA dovrebbero essere impostati.

I parametri che possono essere inseriti negli SLA sono, a titolo non esaustivo:

- il numero di operatori che possono accedere contemporaneamente al servizio
- i tempi di risposta del sistema a seconda del tipo di operazione
- le quantità di dati che il servizio accetta e può memorizzare
- le prestazioni delle apparecchiature hardware e delle reti di telecomunicazione

ma anche

- l'utilizzo di hardware e software di particolari produttori
- la messa in opera di particolari procedure di backup dei dati, recovery, manutenzione ed i loro tempi
- la periodicità dell'aggiornamento del software e hardware
- la disponibilità di hardware e di backup ed i tempi della loro eventuale attivazione
- la disponibilità e l'efficienza del personale di supporto tecnico
- i tempi tra la segnalazione di un guasto o problema tecnico (apertura del ticket), la presa in carico dello stesso e la sua risoluzione
- le prestazioni dei sistemi di sicurezza fisici e logici, dal controllo accessi alle sale macchine, ai firewall, anti-virus, IDS, ecc.

e così via.

È importante notare come gli SLA possono essere modulari ed agganciati direttamente ai corrispettivi economici in una logica di Bonus/Malus. Può essere ad esempio stabilito che il corrispettivo dovuto al fornitore aumenta (Bonus) se una particolare misura di un servizio o gruppo di servizi è superiore ad una certa soglia; ad esempio se nell'arco di un mese il tempo di risposta medio dell'applicazione è stato inferiore a 5 secondi ed il servizio è stato disponibile più del 99,99% del tempo. Viceversa, se i parametri sono al di sotto di un'altra soglia, il corrispettivo viene ridotto (Malus) ed in caso di più gravi inadempienze da parte del fornitore si possono considerare anche penali economiche. Anche se è più raro, vi possono essere anche vincoli o misure imposte al committente, ad esempio nel caso in cui particolari comportamenti del personale del committente possano essere causa di un degradamento del servizio o addirittura procurare danni alle apparecchiature o servizi del fornitore. È molto importante che i parametri indicati negli SLA siano effettivamente significativi del servizio e della sua qualità, e che quindi misurino le aspettative del committente e le prestazioni del fornitore. Non è facile trovare parametri che veramente riescano a valutare se gli interessi delle parti sono soddisfatti ed è compito della trattativa tra le parti, soprattutto a livello tecnico, trovarli ed aggiornarli periodicamente.

A proposito delle penali di carattere economico spesso previste nei confronti del fornitore, si noti come queste vengano spesso utilizzate dai fornitori per limitare le proprie responsabilità e specificare il massimo grado di rischio economico a cui possono essere soggetti.

Infatti la penale diventa una protezione per il fornitore quando stabilisce la sua massima perdita possibile. A livello di contrattazione, deve pertanto essere chiaro ad entrambe le parti il significato e il valore delle penali previste.

2.4.3.1. Le verifiche degli SLA

La verifica degli SLA è un aspetto fondamentale da tenere in considerazione e deve poter essere effettuata in modo indipendente dalle parti.

Quando questa verifica richiede l'accesso a sistemi di terzi, nel contratto devono essere descritte regole chiare e precise su come questo deve essere fatto in pratica. In alcune situazioni conviene anche che siano team congiunti ad effettuare le verifiche degli SLA. Queste verifiche possono essere fatte in modo periodico e predeterminato, ma si deve anche permettere a ciascuna delle due parti di attivare una procedura di verifica non predeterminata nel caso in cui ritenga che ci siano dei problemi. Nel caso di meccanismi Bonus/Malus è importante che nel contratto siano chiaramente indicati le soglie che fanno scattare il meccanismo di premio/penalizzazione, chi è deputato alla misurazione e quali parametri sono utilizzati nella misurazione.

I problemi sorgono in caso di contestazione sul rispetto degli SLA.

Per evitare che in questi casi si giunga a contenziosi tra le parti, potrebbe essere utile nominare una terza parte di cui entrambi si fidano alla quale affidare la verifica degli SLA secondo procedure predefinite. Questa terza parte deve essere indicata inizialmente nel contratto e devono essere indicate le procedure per l'invocazione della stessa, gli obblighi di entrambi verso di essa e le rispettive incombenze economiche.

L'intervento di una terza parte può impedire che una contestazione degeneri subito in un vero e proprio contenzioso con la possibilità di risoluzione anticipata del contratto, ma non può esserci una garanzia assoluta che ciò possa essere evitato.

Anche in presenza di un contratto di outsourcing completo e di SLA ben formulati con le relative procedure di verifica, è sempre consigliato mitigare il problema dei controlli mancanti con la cosiddetta *Clausola di Audit*, ovvero la possibilità per il committente di effettuare un Audit sui sistemi del fornitore in qualità di Auditor esterno. Ovviamente la procedura di invocazione di questo Audit e la sua pianificazionesuo devono essere concordati e stabiliti a contratto.

Spesso però i fornitori non acconsentono a tale richiesta perché nel caso in cui il fornitore abbia un numero elevato di clienti, il suo carico di lavoro per permettere gli Audit potrebbe diventare elevato e tradursi in perdite economiche.

Pertanto il fornitore oppone spesso alla Clausola di Audit specifica per ogni cliente, un Audit esterno effettuato da una terza parte indipendente e riconosciuta da tutti i clienti, oppure una certificazione quale SAS 70 che è specifica per i servizi di Outsourcing.

La certificazione SAS 70 non è molto diffusa in europa (è una certificazione americana) e spesso i fornitori la sostituiscono con la certificazione BS7799/ISO17799/ISO27001 la quale però, anche se utile, non copre in maniera specifica il controllo e la verifica degli SLA e non può quindi essere considerata quale una certificazione specifica per i servizi di Outsourcing.

2.4.4. I SERVIZI DI OUTSOURCING DELLA SICUREZZA ICT

Al giorno d'oggi molti servizi di sicurezza sono offerti da ditte specializzate perché sono servizi molto tecnici e richiedono personale dedicato con addestramento e conoscenze particolari che difficilmente un'azienda si può mantenere internamente.

I *Vulnerability Assessment* e i *Penetration Test* sono esempi di servizi di sicurezza.

I primi sono misurazioni del livello di sicurezza dei sistemi operativi ed applicativi, delle versioni e delle patch presenti, ecc., per verificare l'eventuale presenza di bug. I secondi sono attacchi autorizzati e concordati, interni e/o esterni ai sistemi, per verificare la resistenza e la sicurezza dei sistemi testati.

Tali servizi sono servizi ICT commissionati ad esterni qualificati e affidabili, ma non possono essere considerati come servizi di outsourcing in senso stretto, perché di solito sono svolti saltuariamente e non prevedono il coinvolgimento del fornitore del servizio nelle procedure di gestione del sistema informatico. Inoltre sono servizi che, se anche svolti con periodicità prestabilita, non comportano la "cessione" di una attività dell'azienda.

Quando si parla di outsourcing si intendono invece i casi in cui la gestione del proprio sistema informatico è demandata totalmente o parzialmente ad una società esterna.

Nell'outsourcing dei servizi di sicurezza il servizio di sicurezza dei sistemi informatici di un'azienda è affidato ad una ditta specializzata esterna. In questo caso il fornitore formula le politiche di sicurezza ICT conformi alle politiche generali di sicurezza del committente, includendo eventualmente le procedure per adeguarsi a norme o certificazioni. Il fornitore formula altresì le procedure di applicazione delle politiche, i progetti informatici a livello di macchine e di reti, le relative configurazioni, manutenzioni, monitoraggi, patch di sicurezza, servizi di emergenza, backup, recovery, reporting etc..

Anche se l'infrastruttura informatica è di proprietà del cliente e da lui gestita direttamente, il fornitore di sicurezza ICT provvede, per quanto gli compete, alla configurazione dei Sistemi Operativi e degli applicativi dei server; indica le modalità di configurazione ed uso dei client; installa, configura, gestisce e monitorizza tutti gli applicativi e le macchine dedicate alla sicurezza quali firewall, proxy, intrusion detection, sniffer, ma anche server web e di posta elettronica; configura e monitorizza le connessioni ad internet e con altre aziende anche tramite circuiti privati cifrati (VPN cifrate) etc..

Il problema cruciale in questo tipo di servizi, è che essi riguardano il cuore della sicurezza informatica dell'azienda, anzi sono la sicurezza informatica dell'azienda e quindi giustamente devono essere affidati ad aziende specializzate se non si può disporre di personale interno e di strutture adatte a svolgere questi compiti.

Al giorno d'oggi la sicurezza dell'azienda e la sicurezza informatica si sovrappongono in buona parte, in quanto la maggior parte delle informazioni e quasi tutte le funzioni aziendali sono gestite o monitorate o archiviate nei sistemi informatici. Anche i sistemi di controllo degli accessi, i cedolini orari, la vigilanza notturna e molte altre attività sono oggi basati sull'infrastruttura informatica dell'azienda. La conclusione è quindi che la sicurezza aziendale va di pari passo con la sicurezza informatica.

Ma se la sicurezza informatica è la sicurezza aziendale, perché un'azienda dovrebbe affidare ad esterni questa funzione così importante? La risposta è semplice: efficienza ed economicità. Una attività molto tecnica e specializzata, che non si può improvvisare o implementare in parte, è da affidare a chi ha competenze specifiche in materia.

Vista l'importanza e delicatezza di questo *servizio*, è ancora più importante che esso sia visto non come un appalto esterno quale potrebbe essere un servizio per la riparazione/sostituzione di guasti hardware, bensì come un servizio di outsourcing di una funzione molto importante dell'azienda.

In particolare possiamo pensare al ruolo particolare del comitato di controllo, delle commissioni miste, ai report, agli SLA che comprenderanno le descrizioni delle politiche di sicurezza da implementare, alle verifiche fatte da esterni (Vulnerability Assessment e Penetration Test) per verificare gli SLA, alle attività periodiche e le revisioni periodiche del contratto e così via.

In questo ambito segnaliamo in modo particolare i servizi di *Business Continuity* e *Disaster Recovery*.

Molto spesso infatti questi servizi, a causa della loro natura particolare, sono affidati a fornitori esterni. Data la loro criticità, è molto importante che le misure di verifica e di controllo periodico siano appropriate, per ridurre il rischio che al momento del bisogno qualcosa non funzioni o non sia adeguato alle vere necessità del committente. E' quindi molto importante che le revisioni del contratto, dei dettagli tecnici e degli SLA, siano fatte regolarmente e siano approfondite. Infine, è anche necessario che siano previsti ed effettuati test periodici della loro messa in opera.

Un contratto di outsourcing ben costruito e gestito può veramente rendere efficace e *sicuro* un servizio di outsourcing della sicurezza informatica di un'azienda.

2.4.5. ASPETTI ESSENZIALI DI UN CONTRATTO DI OUTSOURCING ICT

In questa sezione presentiamo una tabella il cui contenuto è derivato rispetto alla struttura del contratto descritta nella sezione 2.2. Con questa tabella vogliamo riassumere gli aspetti principali che caratterizzano un contratto di outsourcing ICT e che riteniamo possa essere utile per una compilazione completa del contratto.

Tabella 2. Aspetti essenziali di un contratto di outsourcing ICT

Oggetto e tempistiche • elenco dei servizi • procedure di take-over • tempi di take-over • tempi di verifica e test del take-over • durata del contratto • verifica tappe intermedie attivazione • trasferimento al termine del contratto • tempi di trasferimento al termine del contratto • condizioni per la corretta esecuzione • criteri per il completamento dei lavori • periodicità delle revisioni del contratto in corso d'opera	**Procedure di controllo** • modalità di accesso ai dati, informazioni, hw, sw, locali, strutture ecc. • livelli di servizio • nomina responsabili • nomina comitato controllo/team misto, compiti e procedure • modalità di reporting dei responsabili e del comitato di controllo
Reportistica • rapporti sullo stato di applicazione del contratto (SLA, ecc.) • figure referenti e periodicità dei rapporti • formato dei rapporti • proprietà intellettuale di documenti, dati, informazioni, hw/sw, invenzioni ecc.	**Verifiche tecniche** • procedure di verifiche SLA • procedure verifiche di attività non periodiche • modalità di contro-verifiche, contestazioni, mediazioni di terze parti • clausola di Audit
Elementi economici • corrispettivi • tempi e modalità di fatturazione • tempi e modalità di pagamento • condizioni e modalità di rimborso • clausole bonus – malus • calcolo e modalità di pagamento penali/bonus • sanzioni per inadempienze	**Clausole generali** • risoluzione per inadempimento • foro competente • subappalti • riservatezza informazioni, privacy • procedure di arbitrato • clausole di esonero dalle responsabilità

2.5. IL CONTRATTO DI OUTSOURCING ICT E GLI SLA

In un contratto di outsourcing, la stesura degli SLA segna sicuramente uno dei passaggi più difficili. Gli SLA infatti devono garantire che il servizio offerto dal fornitore soddisfi veramente le esigenze, tecniche, economiche, di business del cliente. Purtroppo spesso gli SLA sono formulati dal fornitore ed accettati dal cliente con ben pochi controlli se non una valutazione grossolana del rapporto servizi/costi. Perché un contratto di outsourcing abbia successo è necessario:

- che il cliente mantenga sufficienti competenze tecniche, anche tramite il supporto di consulenti esterni, per poter stendere e valutare gli SLA

- che nella fase di stesura del contratto vi sia una commissione paritetica tra cliente e fornitore composta da esperti legali e tecnici, che formuli gli SLA relativi ai servizi in oggetto; gli SLA possono essere definiti a partire dalle indicazioni espresse dal cliente nella RFP (Request for Proposal) e/o a partire dagli SLA proposti dal fornitore

- che entrambi, cliente e fornitore, valutino gli SLA in modo indipendente sia a livello tecnico sia commerciale prima della loro approvazione;

- che nel contratto esistano procedure per poter rivedere gli SLA periodicamente od a richiesta di uno dei contraenti.

Purtroppo non è possibile dettare come devono essere costituiti gli SLA nel settore ICT, utilizzare standard o norme predefinite, anche perché essi dipendono troppo dai dettagli dei servizi in oggetto e dagli obiettivi di business che questi servizi mirano a soddisfare. Infatti la maggior parte dei servizi ICT non sono (ancora) classificabili come *commodity*, e pertanto non è possibile una standardizzazione delle loro caratteristiche. Quello che possiamo fare in questa sede è dare delle indicazioni su cosa potrebbe essere contenuto negli SLA e come essi potrebbero essere formulati.

Nell'approccio alla stesura degli SLA bisogna tenere presente che il punto di vista del fornitore e quello del cliente sono molto diversi:

- il fornitore considera gli SLA principalmente dal punto di vista tecnico, tenendo conto delle ottimizzazioni e delle economie di scala che può offrire e che permettono il miglior impiego possibile dei propri sistemi;

- il cliente dovrebbe invece considerare gli SLA principalmente come strumento per garantire il raggiungimento dei propri obiettivi di business, da questo punto di vista le caratteristiche tecniche sono significative solo se utili al business.

Si noti che non è compito esclusivo dei fornitori individuare quali siano i parametri che devono essere garantiti negli SLA per garantire il raggiungimento degli obiettivi del cliente: tuttavia per servizi molto comuni spesso i parametri proposti dai fornitori sono di generale utilità.

Per sottolineare l'importanza di questo punto, riportiamo un esempio dal *Manuale sui livelli di servizio nel settore ICT*[6], considerando la disponibilità temporale del servizio durante un periodo fissato di tempo, quale potrebbe essere tre mesi. Possono essere date formulazioni molto diverse del livello di servizio che a prima vista potrebbero sembrare simili:

1. nessuna interruzione del servizio deve superare 30 minuti consecutivi

2. non devono verificarsi più di 5 interruzioni del servizio, di qualsiasi durata, nell'arco del periodo

3. la media delle interruzioni deve essere inferiore a 30 minuti

4. il 95% delle interruzioni deve essere di durata inferiore a 30 minuti, il 3% a 35 minuti, il 2% a 45 minuti

[6] I Quaderni dell'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA), volume 7, gennaio 2002.

5. la somma di tutte le interruzioni deve essere inferiore a 180 minuti.

Dipende ovviamente dal tipo di business supportato dal servizio, scegliere la formulazione corretta. Inoltre, laddove possibile, è spesso conveniente che il cliente svolga in via preliminare delle misure sul sistema che ha già in essere da cui dedurre i livelli di servizio da richiedere, ed è opportuno rieseguire queste misure nel periodo di attivazione del servizio per poter perfezionare gli strumenti e le metriche di valutazione e, se previsto da contratto, i parametri stessi degli SLA.

È necessario a questo punto considerare brevemente gli OLA, ovvero gli *Operation Level Agreement*. Gli OLA sono la controparte degli SLA e sono richiesti in contratti di outsourcing particolarmente complessi o quando il fornitore deve agire direttamente sulla struttura informatica del cliente. Infatti gli OLA sono degli accordi sui livelli di servizio che il cliente deve garantire al fornitore in merito alla propria struttura informatica ed ai servizi da esso stesso erogati, per permettere al fornitore di svolgere il proprio compito, fornire i servizi definiti nel contratto e garantire gli SLA. Ad esempio, se il fornitore utilizza le risorse informatiche del committente quali, ad esempio, linee di telecomunicazione ed elaboratori, il committente deve garantire al fornitore il funzionamento delle stesse, altrimenti impedisce al fornitore di rispettare gli SLA. In alcune grandi organizzazioni gli OLA siano adottati anche all'interno dell'organizzazione stessa: ad esempio un grande fornitore può avere settori della propria azienda che a loro volta hanno sottoscrittodegli SLA con clienti esterni.

A parte il diverso obiettivo degli OLA ed il fatto che in questo caso deve essere il fornitore a richiederli ed essere attento che gli garantiscano la possibilità di svolgere correttamente il proprio lavoro, la procedura di creazione e formalizzazione degli OLA è del tutto simile a quella degli SLA, pertanto non ne discuteremo in dettaglio nel resto di questa sezione.

Tornando agli SLA, consideriamo ora alcuni degli elementi che di norma li compongono:

1. le parti che si accordano sul servizio, chi lo fornirà e chi ne usufruirà;
2. il servizio richiesto;
3. la durata del servizio;
4. l'orario di svolgimento del servizio;
5. le condizioni tecniche, organizzative, ambientali eccetera, nelle quali viene erogato il servizio;
6. il livello di prestazioni attese;
7. il reporting da parte del fornitore sul servizio, le modalità delle misurazioni, periodicità, il formato dei report, ecc.;
8. la responsabilità delle parti;
9. il prezzo per il servizio;
10. le penali o le procedure di bonus/malus;
11. i servizi aggiuntivi a richiesta e/o le procedure di ampliamento del servizio;
12. le procedure di revisione dello SLA stesso;

13. le condizioni a cui il cliente deve sottostare per fruire del servizio (queste devono essere rispecchiate negli OLA;

14. gli standard, le norme o le specifiche che il servizio deve adottare.

Si può affrontare la stesura degli SLA o dal punto di vista puramente tecnico, ed in questo caso ad ogni caratteristica di un servizio corrisponde il relativo SLA, oppure dal punto di vista di business, ovvero di un servizio completo come visto da parte del cliente. Ovviamente questa seconda prospettiva è la più corretta, ma richiede una formulazione più articolata di uno SLA. In pratica uno SLA così formulato è composto generalmente da due sezioni, una prima che descrive le caratteristiche generali del servizio, ed una seconda ove sono descritti i dettagli tecnici dei singoli processi.

La prima sezione può essere formulata come nella seguente scheda:

Campo	***Descrizione***
codice	nome identificativo unico del servizio
parti	parti contraenti, il fornitore ed il fruitore del servizio
responsabili	responsabili e punti di contatto per il servizio sia per il cliente che per il fornitore
obiettivi	obiettivi del cliente che devono essere soddisfatti da questo servizio
descrizione	descrizione, anche dettagliata, dei processi che compongono il servizio, devono essere indicati i vari processi descritti poi nelle schede tecniche
attivazione	criteri di attivazione del servizio, incluse date, procedure tecniche e degli operatori
chiusura	criteri di chiusura del servizio anche a seguito di una disputa, incluse date, procedure tecniche e degli operatori
orari	date ed orari di fornitura del servizio
fornitura	modalità di fornitura del servizio, incluse condizioni tecniche, organizzative, ambientali, ecc.
addestramento	procedure di addestramento, iniziale e periodiche, del personale cliente all'uso dei servizi
accesso	modalità di accesso al servizio da parte del cliente, incluse limitazioni e responsabilità dello stesso
norme e certificazioni	standard, norme o specifiche che il servizio deve adottare, indicazione delle conseguenze se tali norme non sono rispettate; certificazioni richieste per il personale del fornitore e del cliente, e per il sw e l'hw utilizzati
responsabilità	responsabilità sia del fornitore sia del cliente nei relativi ruoli di fornitura e fruizione del servizio
legali	responsabilità legali quali rispetto alle norme sulla Privacy, sicurezza dei lavoratori, assicurazioni, ecc.

Campo	*Descrizione*
responsabilità di terze parti	responsabilità di terze parti sia come sub-fornitori sia come ulteriori fruitori del servizio
proprietà	proprietà degli strumenti hw, sw, dati ed informazioni, copyright, diritti intellettuali, brevetti, ecc.
reportistica	procedure generali di reportistica sia dei servizi che dell'assistenza, inclusi periodicità, formati dei report, responsabili dei report da parte del fornitore e del cliente (soddisfazione del servizio)
revisioni	procedure per la revisione, periodica od a richiesta, dello SLA ed approvazione delle modifiche
assistenza	procedure per la segnalazione dei problemi all'help-desk, l'approccio e soluzione dei problemi (apertura e chiusura ticket), tempi garantiti e possibili penali (questi ultimi possono essere specificati in una apposita scheda tecnica di processo)
prezzo	modalità di calcolo del costo del servizio, incluse eventualmente formule basate sulle schede tecniche
penali	regole sull'applicazione di penali o procedure di bonus/malus basate sulle schede tecniche
servizi aggiuntivi	regole per l'estensione od ampliamento dei servizi o modifica dei livelli di servizio, su richiesta del cliente
dispute	procedure per la gestione delle dispute o contestazioni sul servizio da parte di entrambi i contraenti
terze parti	procedure per il coinvolgimento di terze parti per la risoluzione delle dispute
modifiche	procedure per la realizzazione di modifiche all'infrastruttura tecnica od ad altri servizi che potrebbero riflettersi anche indirettamente sul servizio in oggetto, sia per il fornitore sia per il cliente; procedure di segnalazione e nel caso modalità di revisione del servizio
informativa	procedure obbligatorie di informazione completa al partner rispetto a problemi tecnici, di sicurezza, vulnerabilità, guasti, attacchi informatici, modifiche temporanee o definitive del servizio anche se compatibili con i livelli di servizio garantiti (esempio: cambio di fornitore di connettività internet)
incidenti	procedure per la dichiarazione di un incidente e l'attivazione del processo di soluzione dello stesso
soddisfazione	procedure periodiche per la valutazione della soddisfazione del cliente, tramite questionari al personale, interviste e valutazioni da parte di commissioni miste dei report sui servizi; valutazione su ROI, efficienza del servizio e dei suoi processi

Per ogni processo di cui è composto il servizio, vi è poi una scheda tecnica che riporta generalmente i seguenti dati:

Campo	*Descrizione*
definizione	definizione del processo
descrizione	descrizione tecnica del processo
responsabili	responsabili e punti di contatto per il processo sia per il cliente sia per il fornitore
tempi di misura	tempi e frequenza delle misure dei livelli di servizio
ruoli	ruoli e responsabilità nella misura dei livelli di servizio
metriche	descrizione delle metriche adottate per la misura dei livelli di servizio
misura	descrizione tecnica del processo di misura incluse le fonti dei dati misurati
formula	formula per la valutazione dei livelli di servizio
soglie	soglie o formula per valutare il rispetto dei livelli di servizio
penali	procedura per valutare le penali od il bonus/malus od in generale le conseguenze del rispetto o mancato rispetto delle soglie dei livelli di servizio
eccezioni	situazioni eccezionali nelle quali non si applicano le procedure precedenti o nelle quali le procedure devono essere modificate
penali eccezionali	procedura da adottare nei casi eccezionali indicati precedentemente
reportistica	responsabili della stesura dei report dei livelli di servizio e frequenza della loro distribuzione
modulo	formato del modulo di report dei livelli di servizio
contestazioni	procedura da seguire in caso di contestazione del valore misurato, coinvolgimento di una terza parte fidata o simili
terze parti	terze parti da coinvolgere eventualmente nel caso di contestazione delle misure

E' forse conveniente dare due esempi di questa seconda parte, ipotizzando un servizio che richiede la connessione tra il cliente ed il fornitore attraverso delle linee dedicate a lunga distanza fornite dal fornitore stesso. Non indichiamo quale sia il servizio che è sostenuto da questa connessione, ma ipotizziamo che vi sia comunque un'assistenza di tipo help-desk da parte del fornitore per eventuali disservizi. Quindi, all'interno dell'ipotizzato servizio descritto nella prima parte dello SLA, vi sono vari processi che lo compongono, due dei quali hanno i seguenti livelli di servizio:

Servizio Help-Desk:

Campo	*Descrizione*
definizione	assistenza help-desk

Campo	*Descrizione*
descrizione	gli operatori autorizzati del cliente possono rivolgersi all'help-desk per qualsiasi problematica relativa al servizio in oggetto, sia per informazioni, dubbi sia per segnalare problemi ed aprire ticket per guasti; la richiesta deve essere formulata via web sulla intranet tramite compilazione del modulo all'indirizzo http://helpdesk.internal/, all'invio del modulo viene rilasciato automaticamente il numero di ticket e la data di apertura; ogni ulteriore comunicazione dall'help-desk verrà effettuata via email; sul sito dell'help-desk è consultabile lo stato di ogni ticket e tutte le sue modifiche; in casi di guasto al servizio intranet, è possibile contattare l'help-desk al numero di telefono 1234
responsabili	responsabile del servizio help-desk è il signor Rossi, email, tel, fax
tempi di misura	tutti i lunedì, od il primo giorno lavorativo della settimana
ruoli	l'operatore responsabile della gestione del database dell'help-desk
metriche	tempo minimo, medio, massimo di chiusura dei ticket numero di ticket aperti dopo 24, 48, 72 e 120 ore numero di ticket aperti ma non in lavorazione dopo 24 ore
misura	vengono selezionati nel database dell'help-desk tutti i ticket che nella settimana precedente sono stati nello stato aperto, per tutti vengono valutate le metriche indicate nel punto precedente, non considerando nel computo le giornate (24 ore) o mezze-giornate (12 ore) non lavorative
formula	numero totale dei ticket nello stato aperto nel periodo per tutti i ticket aperti nel periodo: data di entrata in lavorazione – data di apertura – giornate non lavorative per i ticket chiusi entro la fine del periodo: data di chiusura - data di apertura – giornate non lavorative; valutazione del minimo, medio e massimo per i ticket ancora aperti alla fine del periodo: data della fine dell'ultima giornata lavorativa – data di apertura – giornate non lavorative
soglie	numero di ticket aperti ma non in lavorazione dopo 24 ore: 0 numero di ticket aperti dopo 120 ore: < 5% dei ticket aperti nel periodo numero di ticket aperti dopo 72 ore: < 10% dei ticket aperti nel periodo numero di ticket aperti dopo 48 ore: < 20% dei ticket aperti nel periodo numero di ticket aperti dopo 24 ore: < 50% dei ticket aperti nel periodo
penali	se per almeno due misure consecutive sono state superate almeno due soglie, per ogni settimana di violazione vi è una penale di X
eccezioni	nel caso vi siano stati fermi macchina per manutenzione notificati con 72 ore di anticipo, o guasti hardware notificati entro 1 ora dall'evento, deve essere considerata come giornata non lavorativa la giornata in cui si è effettuata la manutenzione o è accaduto il guasto hw; questa eccezione è

Campo	*Descrizione*
	applicabile solo una volta in quattro settimane consecutive
penali eccezionali	nessuna
reportistica	report settimanale (ogni lunedì o primo giorno lavorativo della settimana) sul sito web intranet dell'help-desk, responsabile del report il Signor Rossi
modulo	vedi allegato Y
contestazioni	contestazioni sulle misure devono essere inviate alla commissione C utilizzando il modulo K
terze parti	nessuna

Servizio di Connettività:

Campo	*Descrizione*
definizione	connettività a lunga distanza tra cliente e fornitore
descrizione	per la realizzazione del servizio le sedi del cliente e fornitore sono connesse con una linea dati a xx Mbps gestita dal fornitore
responsabili	divisione networking del fornitore, email, tel, fax
tempi di misura	misura continua della connettività il primo mercoledì di ogni mese alle 10 ed alle 15; la misura richiede una breve interruzione del servizio, per questo non deve essere ripetuta eccessivamente; può essere effettuata in altre giornate su richiesta del cliente
ruoli	tecnico networking, un incaricato del cliente può assistere alla misura
metriche	round-trip di pacchetti icmp senza payload tempo di round-trip di pacchetti icmp senza payload, con 500, 1000 e 1450 byte di payload tempo di trasferimento di un file di dati compressi in entrambe le direzioni
misura	le misure vengono effettuate a partire dalla sede cliente; in entrambe le sedi sono connesse direttamente ai router nell'area di confine due macchine adibite ai test, nessuna prioritizzazione di traffico per queste macchine deve essere configurata sui router il tempo di uptime è misurato inviando continuamente dalla sede cliente un pacchetto icmp alla sede fornitore ogni 60 secondi, nel caso non venga ricevuto il pacchetto di risposta entro 3 secondi vengono inviati sino a 4 altri pacchetti, se non vi è risposta a tutti e 5 i pacchetti viene dichiarata chiusa la connessione in quel minuto i tempi di round-trip vengono misurati inviando pacchetti di tipo icmp dalla macchina di test del cliente a quella del fornitore; vengono inviati almeno

Campo	*Descrizione*
	300 pacchetti di ogni tipo, uno al secondo, mentre vi è traffico normale la capacità della linea viene misurata, disconnettendo momentaneamente ogni altro traffico dai router eccetto le macchine di misura, e trasferendo contemporaneamente in entrambe le direzioni due file di xyMByte contenente dati compressi, il tempo di trasferimento viene misurato con l'utility (nome dell'utility) ed include sia il tempo di trasferimento sulla linea sia i tempi di lettura e scrittura sulle due macchine di test simulando l'utilizzo reale dell'utente; a richiesta del cliente la misura può essere ripetuta una volta
formula	ricezione pacchetti di risposta tempi di round-trip: valori minimo, medio, massimo e deviazione standard capacità: tempo di trasferimento in entrambe le direzioni, velocità di trasferimento in Mbps
soglie	downtime-1: 10 minuti al giorno (99,3% uptime) downtime-2: 28,8 minuti al giorno (98% uptime) round-trip medi < 100ms round-trip massimi < 500ms round-trip deviazioni standard < D velocità di trasferimento-1 < H velocità di trasferimento-2 < J
penali	se per due giornate consecutive è stata superata la soglia downtime-1, per ogni giorno di violazione vi è una penale di X1 per ogni giorno in cui è superata la soglia downtime-2 vi è una penale X2 (non si applica in questo caso la penale X1) se sono state superate almeno due soglie di round-trip (su 12) vi è una penale di X3 se viene superata la soglia velocità di trasferimento-1 vi è una penale di X4 se viene superata la soglia velocità di trasferimento-2, vi è una penale di X5
eccezioni	downtime del collegamento per manutenzione programmata di cui il cliente è informato con almeno 72 ore di anticipo e per un massimo di 60 minuti al mese, non sono computabili
penali eccezionali	nessuna
reportistica	i report di uptime sono online sul server web intranet; i report di round-trip e capacità vengono inviati entro il 10 di ogni mese dall'ufficio A del fornitore all'ufficio B del cliente
modulo	vedi allegato C
contestazioni	contestazioni sulle misure devono essere inviate alla commissione D utilizzando il modulo K

Campo	*Descrizione*
terze parti	nel caso in cui la commissione D non trovi un accordo, può essere incaricata l'azienda F di installare proprie macchine di test al posto di quelle del fornitore ed eseguire i test qui indicati per un periodo di 30 giorni per i test di uptime, e per 4 mercoledì consecutivi per gli altri

3. L'AUDITING NELL'OUTSOURCING IT

3.1. L'AUDIT COME PROGETTO

3.1.1. ANALISI PRELIMINARE DEI MACRO-RISCHI

Come introdotto nel paragrafo 1.2 (*Analisi – individuazione delle esigenze e definizione strategie*) il progetto di outsourcing informatico costituisce una scelta strategica decisa e supportata dal vertice aziendale, il quale delinea un quadro di riferimento entro il quale si colloca l'ipotesi di outsourcing. Ciò significa che, a fronte degli obiettivi generali identificati, l'esternalizzazione dei servizi informatici rientra negli ambiti delle strategie che l'impresa intende adottare.

Con il progetto di outsourcing ha inizio una fase del ciclo di vita dell'impresa in cui "l'ipotesi di outsourcing", una volta presa in considerazione, deve essere avvalorata da elementi oggettivi che supportino una eventuale scelta definitiva seguita dall'avvio di una fase esecutiva.

Il contributo che l'Internal Auditing può fornire nella fase preliminare di un progetto di outsourcing si qualifica per la presenza dei seguenti fattori:

- Indipendenza da qualsiasi unità operativa
- Capacità di analizzare le problematiche partendo da un punto di vista guidato dal concetto di rischio
- Cultura del controllo
- Conoscenze in ambito IT, se nella struttura di Internal Auditing sono presenti professionalità di IS Audit.

Non sempre, però, il contributo dell'Internal Auditing in questa fase del processo è ricercato, malgrado le professionalità presenti nella sua struttura possano costituire un valore aggiunto sia per l'indipendenza e le conoscenze dei processi aziendali sia per la capacità di individuare i rischi e i relativi controlli.

I rischi caratteristici di questa fase sono da collocare a livello strategico, e alcuni dei prerequisiti che è necessario verificare sono:

- Chiara comprensione delle necessità del business,
- Comprensione dei tempi necessari per raggiungere gli obiettivi dell'operazione,
- Ruoli e responsabilità compresi e condivisi,
- Esistenza di un sistema di valutazione (scorecard) del successo.

Il contributo dell'Internal Auditing può essere, quindi, l'analisi dei rischi dell'operazione e l'individuazione delle opportune metriche per mitigarne l'effetto.

In questa fase l'analisi dei rischi deve essere focalizzata su ciascun servizio candidato all'esternalizzazione, e può essere condotta secondo le seguenti categorie:

- Business Process Risk – come viene gestito il business?
- Technical Deployment Risk – sono utilizzate le giuste soluzioni tecniche?

- Financial Result Risk – quali sono gli obiettivi finanziari che si intende raggiungere?
- Economic Realization Risk – quali sono i benefici economici attesi dall'outsourcing che si vogliono realizzare?

Anche per i rischi di outsourcing, una volta classificati in base alla loro probabilità di accadimento e all'impatto atteso sul business aziendale, è necessario individuare un piano di mitigazione che dovrà essere condiviso con il fornitore una volta che il processo avrà superato la fase preliminare. Tale piano dovrà essere in grado di contenere l'impatto dei rischi riducendone la frequenza di accadimento e/o l'impatto sul business seguendo, per esempio, un modello quale quello indicato nello schema seguente proposto da Gartner.

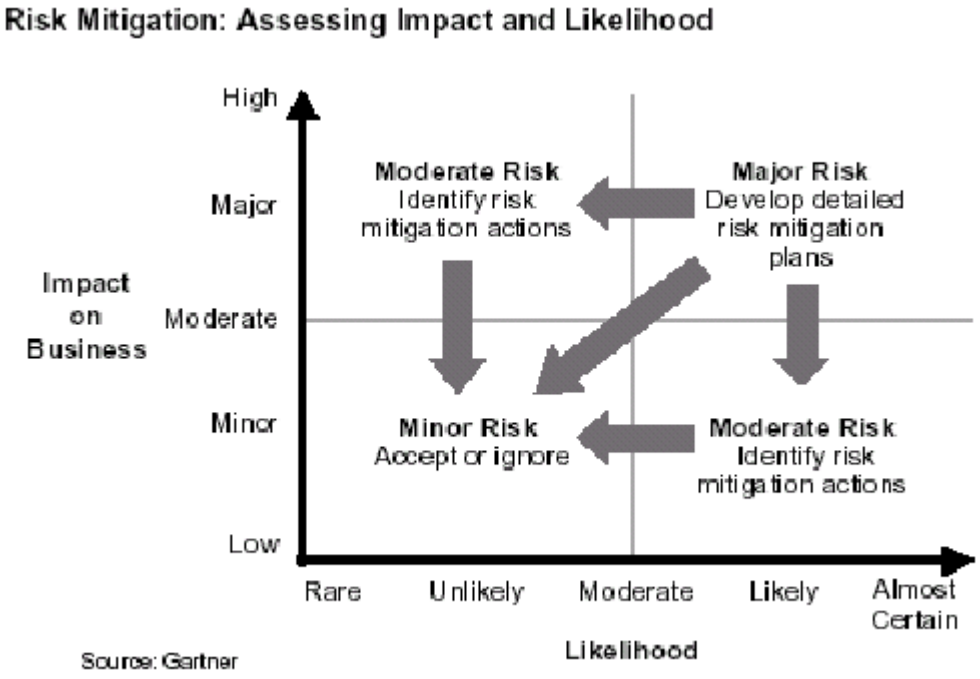

Figura 3. Modello Gartner sulla Risk Mitigation

3.1.2. IDENTIFICAZIONE E SVILUPPO DI UN SISTEMA DI CONTROLLO

L'ambito di controllo dell'audit può avere diversi obiettivi dipendenti dall'entità dei macro-rischi individuati in via preliminare; gli obiettivi possono quindi verificare uno o più tra i rischi identificati nei paragrafi precedenti, allo scopo di precisare – nella fase di esecuzione dell'audit – il perimetro esatto dell'intervento.

L'identificazione dell'ambito di controllo, quindi, è assoggettato alla collocazione dei rischi identificati secondo la classificazione qui proposta:

Tabella 3. Classificazione Rischi

RISCHI STRATEGICI	RISCHI TATTICI	RISCHI OPERATIVI
Chiara comprensione delle necessità del business	Dipendenza dal sistema informativo Competenze e skill Affidabilità del sistema informativo Cambiamenti Esternalizzazioni Importanza del Sistema Informativo per il management della società Protezione delle informazioni	Il contratto e la parte legale La sicurezza Gli SLA ed il loro monitoraggio La Governance
Comprensione dei tempi necessari per raggiungere gli obiettivi dell'operazione		
Ruoli e responsabilità compresi e condivisi		
Esistenza di un sistema di valutazione (scorecard) del successo		

I rischi evidenziati nelle colonne sono quelli che, in questa sede, sono stati identificati come i più significativi e applicabili alle varie realtà di mercato che conosciamo. I rischi identificati come "tattici", possono influire su più di un rischio identificato come "strategico"; la stessa cosa vale per i rischi identificati a livello "operativo" rispetto a quelli classificati a livello "tattico".

Il perimetro individuato per il progetto di audit sul tema dell'outsourcing, secondo i criteri appena esposti, permette di identificare:

a) Obiettivi,

b) Interlocutori,

c) Programmazione,

d) Risorse da impegnare,

e) Metodologia da applicare.

Per quanto riguarda la metodologia, lo sviluppo del sistema di controllo si baserà sull'applicazione delle opportune metodologie internazionali utilizzate nel campo dell'IS audit, della sicurezza IT, del risk management, oppure di metodologie emanate localmente[7].

Il risultato è un sistema di analisi in grado di rispondere efficacemente agli obiettivi di controllo previsti in fase di pianificazione.

Un fattore importante del quale è necessario tenere conto è, infine, quello relativo alle clausole contrattuali che sono state sottoscritte dalle parti relativamente alle verifiche ed ai controlli; la consistenza di tali clausole può influenzare notevolmente gli obiettivi del progetto di audit. Questo elemento assume minore rilevanza nel caso in cui il rapporto tra cliente e fornitore sia rafforzato da un

[7] Le principali sono COBIT, ISO 27001, ITIL, CMM.

vincolo di tipo societario (partecipazione azionaria, joint-venture, ecc.), elemento che facilita il rapporto di partership rispetto a quello contrattuale.

3.1.3. ESECUZIONE DEI CONTROLLI

La fase operativa è quella di maggior delicatezza, soprattutto nel caso in cui l'attività di audit sia svolta dal cliente nei confronti del fornitore. Il perimetro d'azione, determinato dall'interpretazione delle norme contrattuali in proposito, nonché nella necessità di rispettare formalmente le regole d'utilizzo degli strumenti di comunicazione nella pianificazione, nella tempistica, nell'allocazione delle risorse appropriate, per competenza e capacità relazionali, risulta determinante per raggiungere gli obiettivi del lavoro di audit. In questo specifico tipo di audit, per rafforzare i rilievi emersi e individuarne altri non facilmente identificabili e misurabili, assume valore l'utilizzo della tecnica del benchmarking che può essere utilizzata, sia per i rischi di tipo strategico sia per quelli tattico ed operativo, individuando in maniera opportuna gli indici di confronto adatti. Questa tecnica presuppone l'accesso ad informazioni organizzabili secondo varie aggregazioni, tipicamente destinate a chi opera nel settore delle analisi di mercato.

3.1.4. REPORTING

Nella fase del reporting si esprimono i risultati dell'audit svolto in funzione degli obiettivi, e le caratteristiche peculiari di ogni report di audit quali la terminologia, la struttura e la sintesi senza sminuire il contenuto, sono caratteristiche basilari di ogni audit report. Quando l'audit riguarda l'outsourcing, le caratteristiche del report sono influenzate dal livello del rischio analizzato (strategico, tattico, operativo), ed il livello dei suggerimenti e delle considerazioni dipende dell'unità di misura utilizzata per valutare l'attività (ad es. risorse umane risparmiate per il rischio strategico, n° di anomalie delle applicazioni registrate per il rischio operativo).

Nel report è importante riportare i parametri utilizzati per determinare i risultati dell'audit: trend di mercato, benchmarking, norme di legge, parametri tecnici. In alcuni casi particolarmente critici può essere opportuno completare i suggerimenti con vere e proprie proposte operative (ad es. proposte di ridefinizione di SLA risultati inadeguati, raccomandazioni di revisione di clausole per adeguare il contratto a norme di legge disattese, proposte organizzative per migliorare una IT Governance che sia risultata carente, ecc.).

3.1.5. FOLLOW-UP

Normalmente il follow-up ha una pianificazione separata da quella dell'audit in sé, anche se tale pianificazione ed il relativo ambito nascono proprio dai rilievi e dalle anomalie emerse durante l'attività di audit.

Tra i fattori che possono contribuire a determinare i tempi del follow-up ci sono:

- Entità dei rischi rilevati;
- Le scadenze contrattuali:
- La natura tecnica dei rilievi;
- L'acquisizione/sostituzione di strumenti di rilevazione degli SLA;
- Le modifiche organizzative nella IT governance;

- Le modifiche/adeguamenti a norme di legge o di settore;
- I rischi di sicurezza.

La modalità di esecuzione del follow-up dipende dalla situazione, e può variare dallo svolgimento di un ulteriore audit all'applicazione di tecniche di Control Self Assessment (CSA).

3.2. IL COINVOLGIMENTO DELL'AUDITING

3.2.1. AGGANCIO AL CICLO DI VITA E OPPORTUNO COINVOLGIMENTO DELL'AUDITOR

Con riferimento a quanto descritto nel primo capitolo, questa sezione intende approfondire quale dovrebbe essere il coinvolgimento e il ruolo dell'IT auditor nelle diverse fasi del ciclo di vita del contratto di outsourcing.

A tale scopo riportiamo la tabella, commentata nel paragrafo 1.2 nella quale abbiamo evidenziato le fasi in cui riteniamo opportuno il contributo dell'IS auditor.

Tabella 4. Posizionamento dell'IT Auditing nel ciclo di vita del contratto di outsourcing

a. PUNTO DI VISTA DEL CLIENTE	b. PUNTO DI VISTA DEL FORNITORE
a.1. ANALISI (*Plan*)	**b.1. ANALISI (*Plan*)**
a.1.1. Individuazione esigenze e definizione strategie	**b.1.1. Definizione del ruolo e delle strategie** Identificazione delle esigenze Identificazione degli obiettivi Assegnazione responsabilità commerciali
a.1.2. Identificazione team di analisi	
a.1.3. Analisi dei rischi e delle potenzialità Valutazione dei processi interni Identificazione dei criteri di scelta Scelta dei processi da esternalizzare e degli obiettivi	**b.1.2. Identificazione del cliente** Individuazione delle opportunità di mercato Identificazione team di analisi Analisi dei rischi e delle potenzialità Sviluppo dell'offerta commerciale
a.1.4. Identificazione del fornitore Ricerca di mercato Identificazione forma di outsourcing Identificazione outsourcer	b.1.3. Definizione dl progetto di attuazione e macro-plan
a.1.5. Definizione del progetto di attuazione e macro-plan	**b.1.4. Definizione del contratto**
a.1.6. Definizione del contratto	
a.2. IMPLEMENTAZIONE DEL CONTRATTO (*Do*)	**b.2. IMPLEMENTAZIONE DEL CONTRATTO (*Do*)**
a.2.1. Definizione del team misto cliente – outsourcer	b.2.1. Definizione del team misto cliente – outsourcer
a.2.2. Re-engineering del processo in outsourcing	b.2.2. Re-engineering del processo in outsourcing
a.2.3. Definizione strumenti di controllo ed indici	**b.2.3. Definizione strumenti di controllo ed indici**
a.2.4. Realizzazione del servizio Analisi organizzativa Adeguamento organizzativo Collaudo del servizio Accettazione del servizio	b.2.4. Realizzazione del servizio Progetto esecutivo Organizzazione del presidio al servizio Adeguamento organizzativo Collaudo del servizio
a.2.5. Formazione del personale	b.2.5. Formazione del personale
a.2.6. Migrazione al nuovo assetto	b.2.6. Migrazione al nuovo assetto
	b.2.7. Erogazione del servizio
	b.2.8. Supporto al cliente
a.3. GESTIONE E VERIFICA DEL CONTRATTO (*Check*)	**b.3. GESTIONE E VERIFICA DEL CONTRATTO (*Check)***
a.3.1. Gestione del contratto e del fornitore	**b.3.1. Gestione del contratto e del cliente**
a.3.2. Monitoraggio dei livelli di servizio	b.3.2. Monitoraggio dei livelli di servizio
a.3.3. Le attività di Auditing	**b.3.3. Le attività di Auditing**
a.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act)*	**b.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act*)**
a.4.1. Miglioramento continuo	b.4.1. Miglioramento continuo
a.4.2. Valutazione economica e strategica del servizio di outsourcing	**b.4.2. Valutazione del servizio di outsourcing**

a.4.3. Rinnovo del contratto/scelta diverso outsourcer	b.4.3. Rinnovo o termine del contratto

a. PUNTO DI VISTA DEL CLIENTE

a.1. ANALISI (*Plan*)

a.1.1. Individuazione esigenze e definizione strategie

A seconda delle dimensioni e della complessità dell'azienda, questa fase può includere o meno una identificazione e/o una valutazione preventiva, da parte della funzione interna di Auditing oppure di una società indipendente, dei maggiori rischi aziendali insiti nella scelta di outsourcing.

a.1.3. Analisi dei rischi e delle potenzialità

Nell'ambito della valutazione qualitativa, l'IS auditor dovrebbe essere coinvolto nelle seguenti attività:

- analisi dei rischi nei processi oggetto di outsourcing,
- valutazione dei rischi connessi all'IT Governance di tali processi,
- identificazione dei requisiti di controllo ritenuti minimali nello scenario futuro, con riferimento ai rischi rilevati nell'analisi svolta ai punti precedenti e agli obiettivi aziendali.

Nella valutazione quantitativa, l'IS auditor dovrebbe contribuire allo sviluppo dell'analisi dei costi e dei benefici utilizzando, informazioni di riferimento quali, ad esempio :

- i valori iscritti a bilancio (ad esempio le voci relative agli investimenti IT, i rispettivi ammortamenti, i costi del personale IT, ecc),
- gli obiettivi quantitativi espressi nel piano industriale,
- eventuali benchmarch di mercato.

Sulla base di questi valori, possono essere effettuate alcune proiezioni di costi e benefici sugli esercizi successivi anche al fine di stimare gli impatti sui principali indicatori di risultato aziendale e valutare un opportuno rapporto costi / benefici nella definizione dei requisiti minimali di controllo.

In questa fase l'IS auditor dovrebbe collaborare anche alla valutazione di eventuali impatti della scelta di outsourcing sulle normative interne, i processi interni, i rapporti contrattuali già in corso con altri fornitori.

a.1.4. Identificazione del fornitore

L'IS auditor dovrebbe collaborare alla stesura dell'RFP (*Request For Proposal*) e verificare che le clausole relative alle caratteristiche del servizio e agli aspetti economici siano coerenti con gli obiettivi indicati dalla Direzione e con i requisiti o vincoli quantitativi e qualitativi emersi dalla precedente analisi.

Ad esempio nella RFP dovrebbero essere incluse alcune specifiche relative all'istituzione o al mantenimento di un adeguato sistema di controllo, quali ad esempio la presenza di procedure

di back-up, disaster recovery, processi e procedure a presidio della disponibilità, integrità, riservatezza dei dati, del rispetto delle normative esterne, al diritto di effettuare o richiedere a società terze attività di audit presso il fornitore, ecc.

Inoltre l'IS auditor può contribuire alla fase di selezione verificando la coerenza del processo stesso ai requisiti di normativa interna (ad esempio rispetto del processo autorizzativo, redazione della documentazione, ecc).

Nelle aziende di maggiori dimensioni è possibile che, a conclusione della fase di valutazione delle proposte ricevute e a seguito della conseguente scelta del fornitore, il Vertice Aziendale decida di condurre un'attività di Due Diligence sulla società fornitrice identificata. In questo caso l'IS auditor può essere coinvolto, direttamente o a supporto di una società indipendente, nella valutazione qualitativa e quantitativa dell'azienda fornitrice con riferimento alle sue risorse tecnologiche, organizzative e di business che dovranno garantire l'erogazione del servizio.

a.1.5. Definizione del progetto di attuazione e macro-plan

L'IS auditor in questa fase dovrebbe contribuire a verificare la corrispondenza tra le clausole contrattuali ed i requisiti inclusi nella RFP. In particolare, l'IS Auditor potrà essere coinvolto nella verifica dell'adeguata formulazione delle condizioni relative a:

- gestione del periodo di transizione (da insourcing ad outsourcing, oppure passaggio di consegne da precedente a nuovo fornitore),
- gestione del servizio in riferimento ad esempio alle esigenze di continuità operativa, qualità percepita dall'utente, integrità del dato aziendale, rispetto della normativa esterna,
- capacità di adeguamento del servizio alle evoluzioni interne del cliente o indotte da mercato e legislazione,
- gestione del personale, ad esempio nel caso di cessione di ramo d'azienda o di assegnazione di dipendenti del fornitore presso strutture del cliente,
- definizione e valutazione dei livelli di servizio e dei relativi criteri per l'applicazione di bonus e penali,
- clausole di rinnovo e di chiusura del contratto.

a.2. IMPLEMENTAZIONE DEL CONTRATTO (*Do*)

Il progetto di realizzazione e migrazione al nuovo servizio dovrebbe essere sottoposto a specifico audit di progetto o a verifiche puntuali nelle fasi o nelle aree ritenute maggiormente significative per la conclusione positiva dell'implementazione. Tuttavia, non essendo le linee guida per l'Audit di Progetto incluse nell'ambito del presente studio, rinviamo a pubblicazioni specifiche per indicazioni di dettaglio su questa tipologia di auditing.

a.2.3. Definizione strumenti di controllo ed indici

In questa fase l'IS auditor può contribuire a che sia posta particolare attenzione agli obiettivi di controllo che discendono dalle fasi di analisi, quali ad esempio:

- adeguatezza e completezza degli indicatori rispetto alle clausole specificate nel contratto stipulato;

- adeguatezza degli strumenti di monitoraggio e rilevazione;
- adeguatezza degli strumenti di elaborazione delle rilevazioni rispetto alle regole di valutazione dei livelli di servizio definite nel contratto
- adeguatezza della reportistica di dettaglio e di sintesi alle esigenze di documentabilità di eventuali bonus o penali.

a.3. GESTIONE E VERIFICA DEL CONTRATTO (*Check*)

a.3.1. Gestione del contratto e del fornitore

Per garantire una maggiore efficacia delle attività di gestione, l'IS Auditor dovrebbe verificare che sia stata identificata un'unità organizzativa formalmente preposta al controllo del fornitore e del servizio erogato e per questo adeguatamente strutturata in termini di numero di risorse, ruoli/responsabilità e competenze.

Dovrebbe essere altresì verificata la definizione di processi atti a disciplinare il rapporto cliente – fornitore, che prevedano il monitoraggio periodico delle attività e che regolino la gestione operativa delle reciproche richieste di intervento o supporto.

Inoltre, l'auditor dovrebbe verificare che gli strumenti definiti per la misurazione dei livelli di servizio siano attivi, abbiano superato la necessaria fase di messa a punto e, soprattutto, che sia effettuata la rilevazione e la registrazione puntuale di tutte le informazioni necessarie a detti strumenti per il loro corretto funzionamento.

a.3.3. Le attività di Auditing

Questa fase è di totale competenza e responsabilità della funzione di auditing e quindi dovrebbe rientrare, con sistematicità, nella pianificazione annuale della funzione stessa.

Questa fase attiene all'oggetto principale del presente lavoro e quindi sarà sviluppata in dettaglio nei prossimi capitoli.

Essa consiste principalmente nella periodica verifica della conformità del servizio alle clausole contrattuali e della correttezza e completezza delle rilevazioni svolte per misurare il raggiungimento degli obiettivi posti al fornitore; essa include inoltre la valutazione dei rischi e dei controlli presenti nello scenario di outsourcing.

Da essa possono derivare suggerimenti per il rafforzamento del sistema di controllo esistente, espressi sotto forma di richieste di adeguamento del servizio o di segnalazioni della necessità di procedere alla revisione del merito delle clausole contrattuali.

a.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act*)

a.4.2. Valutazione economica e strategica del servizio di outsourcing

La funzione di Audit può essere coinvolta nella valutazione qualitativa ed economica dell'operato del fornitore. In questo caso, il ruolo dell'IS auditor dovrebbe consistere nell'analisi complessiva del servizio a partire dalle risultanze delle proprie attività di analisi ordinarie (descritte sopra nella fase "*Check*"), nonché dalle rilevazioni periodiche dei livelli di servizio, delle penali applicate e dei bonus riconosciuti.

a.4.3. Rinnovo del contratto/ scelta diverso outsourcer

All'interno di questa fase, l'IS auditor dovrebbe svolgere una funzione di controllo analoga a quella esercitata durante la prima stesura del contratto, ossia di verifica della correttezza complessiva del processo.

b. PUNTO DI VISTA DEL FORNITORE

b.1. ANALISI (*Plan*)

b.1.1 Definizione del ruolo e delle strategie

A seconda delle dimensioni e della complessità dell'azienda, questa fase può includere o meno una identificazione e/o una valutazione preventiva dei maggiori rischi aziendali, derivanti dalla scelta in oggetto da parte della funzione di Audit Interno, oppure da parte di una società indipendente.

b.1.2. Identificazione del cliente

La fase di analisi dei rischi e delle potenzialità ed il relativo coinvolgimento dell'Audit variano sensibilmente a seconda che il fornitore stia valutando la prima presa in carico di uno specifico servizio, oppure l'acquisizione di un nuovo cliente al quale si propone un servizio di outsourcing già attivo.

In ogni caso l'IS Auditor dovrebbe partecipare alle attività di analisi e valutazione qualitativa del rischio nei processi oggetto di outsourcing e di identificazione dei requisiti di controllo minimali. Inoltre, dovrebbe contribuire all'analisi dei costi e dei benefici sulla base, ad esempio, di un confronto tra:

- informazioni di riferimento quali, ad esempio, gli obiettivi quantitativi espressi nel piano industriale ed eventuali benchmarch di mercato,
- valori, stimati o simulati, degli investimenti necessari alla gestione dei processi da fornire in outsourcing, dei risparmi derivanti da possibili sinergie con pre-esistenti ed analoghe soluzioni di outsourcing in corso di erogazione per altri clienti, ecc.

Nel caso di una prima acquisizione è opportuno che l'analisi nella quale è coinvolto l'IS Auditor includa, tra gli altri, i seguenti aspetti:

- analisi quantitativa e qualitativa del potenziale cliente, sulla base dei documenti societari pubblici e delle informazioni di maggior dettaglio disponibili su basi dati specializzate,
- simulazione dei costi immediati e dell'entità di costi e benefici a regime,
- valutazione degli aspetti di IT Governance dei processi da erogare con riferimento alle strutture di governo e di controllo del fornitore stesso.

In questa fase l'IS auditor dovrebbe collaborare anche nella valutazione di eventuali impatti della scelta di acquisizione su normative interne, processi interni, rapporti contrattuali già in corso con altri clienti.

In casi particolarmente significativi, l'auditor potrebbe essere coinvolto anche nella fase di sviluppo dell'offerta commerciale.

In questi casi l'auditor dovrebbe verificare che l'offerta non esponga l'azienda a rischi di insuccesso o inadempienza - ad esempio per indisponibilità di adeguate risorse economiche,

tecniche o organizzative - che essa indichi in modo corretto e adeguatamente dettagliato l'ambito e le modalità di intervento, includa condizioni economiche coerenti agli impegni previsti, e sia coerente con eventuali vincoli imposti dalle normative interne.

b.1.4 Definizione del contratto

L'IS auditor dovrebbe essere coinvolto in questa fase per verificare la corrispondenza tra le clausole contrattuali e i requisiti inclusi nella RFP. Ad esempio, dovrebbe essere oggetto di verifica l'adeguata formulazione delle seguenti condizioni:

- definizione e valutazione dei livelli di servizio e dei relativi criteri per l'applicazione di bonus e penali,
- definizione dei pre-requisiti tecnologici, organizzativi e logistici che il cliente deve garantire per permettere la presa in carico del servizio e l'erogazione dello stesso secondo i livelli di qualità definiti nello SLA,
- definizione di modalità, tempi e responsabilità del passaggio di consegne al fornitore (da parte del cliente o di terza parte) o dell'implementazione del servizio ed eventuale messa a punto iniziale del processo di valutazione dei livelli di servizio,
- gestione del personale, sia nel caso di cessione di ramo d'azienda che di allocazione di dipendenti del fornitore presso strutture del cliente,
- clausole di rinnovo e di chiusura del contratto.

b.2. IMPLEMENTAZIONE E GESTIONE DEL CONTRATTO (*Do*)

Analogamente a quanto indicato a paragrafo *a.2* per il cliente, riteniamo che anche il fornitore dovrebbe sottoporre il progetto di implementazione del contratto a specifico audit di progetto o a verifiche puntuali nelle fasi o nelle aree ritenute maggiormente significative per la conclusione positiva dello stesso. Rinviamo a pubblicazioni specifiche per indicazioni di dettaglio su questa tipologia di auditing.

b.2.3. Definizione strumenti di controllo ed indici

In questa fase l'IS auditor può contribuire all'analisi degli obiettivi di controllo che discendono dalle fasi di analisi, quali ad esempio:

- adeguatezza e completezza degli indicatori rispetto alle clausole specificate nel contratto stipulato,
- adeguatezza degli strumenti di monitoraggio e rilevazione,
- adeguatezza degli strumenti di elaborazione delle rilevazioni rispetto alle regole di valutazione dei livelli di servizio definite nel contratto,
- adeguatezza della reportistica di dettaglio e di sintesi alle esigenze di documentabilità di eventuali bonus o penali.

Analogamente a quanto indicato a paragrafo a.2 per il cliente, riteniamo che anche il fornitore dovrebbe sottoporre il progetto di implementazione del contratto a specifico audit di progetto o a verifiche puntuali nelle fasi o nelle aree ritenute maggiormente significative per

la conclusione positiva dello stesso. Rinviamo a pubblicazioni specifiche per indicazioni di dettaglio su questa tipologia di auditing.

b.3. GESTIONE E VERIFICA DEL CONTRATTO (*Check*)

b.3.1. Gestione del contratto e del cliente

Per garantire una maggiore efficacia delle attività di gestione, l'IS auditor dovrebbe verificare che sia stata identificata un'unità organizzativa formalmente preposta al controllo del servizio erogato, allo svolgimento di eventuali verifiche sulla reportistica prodotta dal cliente, e per questo dotata di risorse adeguate in termini di dimensionamento, competenze e ruoli/responsabilità.

Dovrebbe essere altresì verificata la definizione dei processi atti a disciplinare il rapporto cliente – fornitore, che prevedano il monitoraggio periodico delle attività e che regolino la gestione operativa delle reciproche richieste di intervento o supporto.

Inoltre, l'auditor dovrebbe verificare che gli strumenti definiti per la misurazione dei livelli di servizio siano attivi, abbiano superato la necessaria fase di messa a punto e riflettano correttamente la qualità del servizio erogato.

b.3.3. Le attività di Auditing

Anche per il fornitore la pianificazione annuale della funzione di Audit dovrebbe prevedere verifiche sistematiche sui servizi erogati.

Questa fase attiene all'oggetto principale del presente lavoro e quindi sarà sviluppata in dettaglio nei prossimi capitoli.

Essa consiste principalmente nella periodica verifica della conformità del servizio alle clausole contrattuali e della correttezza e completezza delle rilevazioni svolte dal cliente per misurare il raggiungimento degli obiettivi posti al fornitore; inoltre include la valutazione di rischi e controlli presenti nel processo interno di erogazione del servizio.

Da essa possono derivare suggerimenti per il rafforzamento del sistema di controllo interno, indicazioni per l'adeguamento dei criteri di valutazione, il rafforzamento di alcuni pre-requisiti cliente, la revisione delle clausole contrattuali.

b.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act*)

b.4.2. Valutazione del servizio di outsourcing

In questa fase la funzione di Audit può essere coinvolta nella valutazione qualitativa ed economica del servizio erogato. Il ruolo dell'IT auditor dovrebbe dunque consistere nell'analisi complessiva del servizio a partire dalle risultanze delle proprie attività di verifica ordinarie (descritte sopra nella fase "*Check*") nonché dall'analisi dei costi sostenuti dall'azienda e dei ricavi, delle penali pagate e dei bonus ricevuti, con riferimento agli obiettivi aziendali di budget e di piano industriale.

b.4.3. Rinnovo o termine del contratto

All'interno di questa fase, l'IT auditor dovrebbe svolgere una funzione di controllo analoga a quella esercitata durante la prima stesura del contratto, ossia di verifica della correttezza complessiva del processo.

3.3. CLASSIFICAZIONE DEI RISCHI DELL'OUTSOURCING

Il ricorso all'outsourcing è a volte una scelta obbligata per alcune aziende, sia nazionali che internazionali. Come esaminato in un'altra sezione del presente documento, questa tendenza consolidata riguarda molteplici funzioni aziendali, dal Customer Service fino ai Sistema Informativi. Nonostante l'esternalizzazione sia generalmente considerata una scelta strategica vantaggiosa in termini di riduzione dei costi, ad essa è associata, tuttavia, anche una certa gamma di rischi.

Da un'indagine condotta negli Stati Uniti nel corso del 2000 è emerso che circa il 35%degli accordi di outsourcing fallisce.[8] Alla luce di queste considerazioni vanno, quindi, individuati i principali parametri da monitorare durante tutto il ciclo di vita di un contratto di outsourcing. Secondo quanto riportato nel settembre del 2004 dalla società di consulenza legale Baker & McKenzie "studi recenti rilevano come nell'ambito delle aziende maggiormente collegate a società di fornitura esterne ed organizzate per processi di business, mentre la rilevanza attribuita alla riduzione diretta dei costi – a fronte dell'esternalizzazione – diminuisce, l'importanza assegnata ad aspetti quali la sicurezza, la qualità e quali il livello di servizio incrementa sensibilmente".[9] Molteplici sono, infatti, i costi indiretti da considerare come associati al processo di gestione della relazione di outsourcing.

Sulla base di queste premesse si elencano di seguito i rischi potenziali, associati ai principali processi aziendali, che dovrebbero essere analizzati dal management aziendale nell'ambito delle valutazioni preliminari ad una scelta strategica per l'outsourcing.

Tabella 5. Rischi potenziali

Processo	Rischio	Descrizione
Gestione dei rapporti con i fornitori **Definizione del responsabile dei rapporti con i fornitori** **Qualificazione delle terze parti**	**Rischio di budgeting e pianificazione**	▪ Definizione degli obiettivi ▪ Definizione dell'orizzonte temporale
Gestione dei rapporti con i fornitori	**Rischio di frode e di atti illegali da parte di terzi**	▪ Frodi / malversazioni / attività non autorizzate di collaboratori ▪ Frode di terzi

8 Cfr. Gay, Charles E.; James Essinger; Inside Outsourcing: The Insider's Guide to Managing Strategic Sourcing, London, Nicholas Brealey Publishing, 2000. Oxford University's Institute of Information Management and the University of Missouri (USA), 2000 riportato in Catherine Wright "Top Three Potential Risks With Outsourcing Information Systems", Volume 5, 2004.

9 Cfr. Theodore Ling, "Global Outsourcing - Outsourcing to Canada: legal & tax considerations", Baker & McKenzie, September 2004.

Processo	Rischio	Descrizione
		▪ Furto di assets aziendali (beni fisici / proprietà intellettuali) ▪ Danni ai beni di proprietà
Gestione dei rapporti con i fornitori	**Rischio di reputazione**	▪ Frode/attività non autorizzate/atti illegali ▪ Interruzione dei processi / Produzione output errati
Definizione del responsabile dei rapporti con i fornitori **Stipula e gestione di contratti con terze parti** **Qualificazione delle terze parti**	**Rischio di performance**	▪ Identificazione degli indicatori di performance ▪ Completezza dell'informativa degli indicatori di performance ▪ Chiarezza/Efficacia informativa degli indicatori di performance ▪ Affidabilità informativa degli indicatori di performance
Definizione del responsabile dei rapporti con i fornitori **Qualificazione delle terze parti**	**Rischio di valutazione degli investimenti**	▪ Definizione e applicazione dei criteri di valutazione ▪ Monitoraggio della redditività
Definizione del responsabile dei rapporti con i fornitori **Gestione della sicurezza fisica e logica**	**Rischio di non conformità alla normativa esterna**	▪ Gestione e aggiornamento della contrattualistica ▪ Processo di sicurezza non garantito
Definizione del responsabile dei rapporti con i fornitori **Qualificazione delle terze parti**	**Rischio di outsourcing**	▪ Selezione e monitoraggio dell'outsourcer ▪ Divario di performance tra la società e l'outsourcer ▪ Formalizzazione costi, poteri, limiti e livelli di servizio ▪ Perdita di know-how della società/Gruppo ▪ Sottrazione di clienti da parte dell'outsourcer alla società
Gestione dei rapporti con i fornitori **Definizione del responsabile dei rapporti con i fornitori** **Stipula e gestione di contratti con terze parti** **Qualificazione delle terze parti** **Stipula e gestione di**	**Rischio di disponibilità**	▪ Procedure di archiviazione dei dati ▪ Gestione delle copie di sicurezza ▪ Gestione del dimensionamento del servizio IT

Processo	Rischio	Descrizione
contratti di outsourcing **Gestione della continuità del servizio** **Gestione della sicurezza fisica e logica** **Monitoraggio dell'esecuzione del contratto**		

Si esaminano nel seguito alcune aggregazioni di rischio ritenute particolarmente critiche in tema di outsourcing.

3.3.1. IL CONTRATTO E LA PARTE LEGALE

Gli elementi appartenenti a questo ambito che sono ritenuti particolarmente rilevanti, sono elencati di seguito:

a) Barriere all'uscita;

b) Rischi legali;

c) Aspetti legati alla gestione delle risorse umane.

Il primo aspetto è riferito sia al grado di affidabilità riposto dalla società cliente nell'outsourcer, sia alle problematiche potenziali presenti nel momento in cui la relazione contrattuale giunge al termine.

Il secondo elemento è collegato, in primo luogo, alla mancanza di un rapporto fiduciario tra outsourcer e cliente e, in secondo luogo, all'incremento di responsabilità nel corso del ciclo di vita della relazione contrattuale.

Il terzo punto è, infine, conseguente alla sostituzione parziale di personale interno – in termini di esperienza e skill professionali maturati – con personale esterno.

L'elenco dei rischi potenziali appena visto può essere riconducibile – in termini generali - alla perdita di controllo da parte del cliente delle capacità direzionali e strategiche nei confronti del proprio sistema informativo ossia, in sintesi, alla perdita di controllo sugli aspetti esecutivi, strategici e operativi, nonché su quelli correlati ai temi del Disaster Recovery.

Con riguardo alla potenziale perdita di capacità "direzionali e strategiche" dobbiamo segnalare che l'attivazione di una relazione contrattuale di outsourcing favorisce l'instaurarsi di barriere all'uscita senz'altro significative, soprattutto se l'oggetto del contratto riguarda lo sviluppo di sistemi ("system development") ed il supporto alla clientela ("end user support"), e non si limita al semplice "data processing". La perdita di capacità professionali interne, impiegabili nella gestione del proprio sistema informativo ("internal IS capabilities"), determina un forte incremento del grado di dipendenza del cliente. L'evidenza di ciò non è, tuttavia, immediatamente percepibile dal management aziendale. Alla scadenza del ciclo di vita del contratto di outsourcing, la scelta – economica, commerciale o strategica – di non rinnovare il contratto in essere può, infatti, riservare

ostacoli prevedibili ma non realmente previsti, collegati, ad esempio, alla difficoltà di scegliere un nuovo fornitore – magari più efficiente ed affidabile – o agli sforzi eccessivi necessari per ricondurre lo sviluppo, la produzione o la gestione del servizio che si era esternalizzato nell'ambito delle competenze interne.

Per quanto riguarda la qualità del servizio IT, vanno considerate le implicazioni legate al fatto che in genere i contratti di outsourcing prevedono la corresponsione di un prezzo fisso. Qualora la società esterna giungesse a valutarlo non adeguati i profitti conseguiti, si profilerebbe il rischio che per aumentare questi ultimi essa riduca il livello qualitativo del servizio erogato. In alcuni casi, ad esempio, la società esterna potrebbe esprimere l'intenzione di aumentare le capacità elaborative del Sistema Informativo affidatole, senza specificare, però, il periodo di tempo entro il quale la maggior capacità verrebbe ad essere resa disponibile.

Un ulteriore aspetto, infine, inerente al grado di affidabilità garantito dall'outsourcer, è collegato al tema del "disaster recovery": la società cliente corre il rischio che il fornitore esterno non sia in grado di rispondere adeguatamente ad eventi disastrosi e, soprattutto, di rispondere con modalità simili o paragonabili a quelle normalmente considerate in una gestione interna ("in-house").

3.3.1.1. Le esternalità del contratto di outsourcing[10]

Al fine di fornire una valutazione empirica delle indicazioni riportate sopra, di seguito indichiamo sinteticamente i risultati di un'indagine condotta negli Stati Uniti che ha coinvolto il vertice aziendale di tre grandi aziende statunitensi.[11] L'indagine era finalizzata ad evidenziare i principali rischi, percepiti come gravi minacce da un organizzazione che decide di coinvolgere nel proprio processo produttivo società esterne.

Le principali categorie di rischio evidenziate dal management intervistato sono state, in ordine decrescente di frequenza, le seguenti:

1. sicurezza logica;
2. dipendenza/barriere all'uscita;
3. rischi legali.

In prima posizione si colloca il rischio relativo alla sicurezza logica, che verrà commentato più avanti, mentre il rischio legale è stato percepito prevalentemente rilevante dalle aziende farmaceutiche e dalle istituzioni finanziarie, laddove quello di dipendenza è considerato invece rilevante soprattutto dalle aziende farmaceutiche e retail.

Di seguito facciamo alcune considerazioni sui rischi riferiti al secondo e terzo punto:

- **Dipendenze/Barriere all'uscita**

La produzione di servizi ed applicazioni ICT in regime di outsourcing costituisce per l'azienda cliente il rischio della perdita del controllo sul proprio sistema informativo. Questo potrebbe significare, in mancanza di una fattiva collaborazione da parte dell'outsourcer, la difficoltà nell'adeguare il proprio sistema informativo. Il cliente potrebbe inoltre incontrare difficoltà, con

[10] Influenza dell'attività economica dell'outsourcer sul cliente

[11] Anthem - health care insurer; Bank of America – financial/banking institution e Wal-Mart – retailer.

eventuali perdite di risorse economiche, nell'ottenere dalla società esterna gli adeguamenti alle nuove tecnologie messe a disposizione dall'industria ICT. In casi estremi, qualora la società esterna non fosse all'altezza di sviluppare adeguatamente le modifiche richieste, il cliente potrebbe ritrovarsi in ritardo rispetto alle tendenze del mercato di riferimento ed allontanarsi dal cosiddetto "cutting edge of technology" (margine tagliente della tecnologia).

Inoltre, qualora l'outsourcer non fosse in grado di adempiere alle proprie responsabilità contrattuali, l'operatività stessa dei servizi ed applicazioni ad esso conferiti in outsourcing potrebbe essere fortemente compromessa ed il cliente potrebbe non essere in grado, almeno nel breve periodo, di mettere in campo le adeguate risorse professionali capaci di sostituirsi alle competenze proprie della società esterna. Ne risulta ovvio, quindi, che il potere contrattuale conseguibile dall'outsourcer rappresenta uno dei principali elementi da qualificare in sede di analisi preliminare.

Come ulteriore elemento da valutare si segnalano le criticità insite al termine del ciclo di vita contrattuale. Possono sussistere molti e diversi motivi alla base della conclusione - forzosa - del ciclo di vita di una relazione di outsourcing. ed il cliente si troverebbe, in casi come questi, a dover trovare immediatamente un'organizzazione sostitutiva capace di replicare esattamente le attività svolte dalla precedente.

- **Rischi Legali**

Ricorre spesso il concetto che *l'outsourcing coinvolge due entità che interagiscono fra loro in una relazione commerciale molto stretta e che si traduce in una ricetta per complicazioni legali.* Il senso di questa espressione sta nella particolare relazione fiduciaria instaurata nell'ambito del ciclo di vita del contratto di outsourcing. Uno dei rischi è che l'outsourcer non si ritenga condizionato nei confronti del cliente da particolari obbligazioni, legalmente vincolanti, e ciò specialmente quando impieghi contratti standard che contemplano la descrizione dei servizi in modalità statica ("as-is,") e che non prevedono alcun impegno in termini di responsabilità di risultato. Va considerato, peraltro, che la relazione di outsourcing in nulla sposta (e per certi versi amplia) la responsabilità dell'organizzazione cliente nei confronti della propria clientela, nonché nei confronti di terze parti come, ad esempio, i software licensor. La condivisione del software con la società di outsourcing, infatti, potrebbe rendere più complessa la gestione degli accordi di licenza o costituire ipotesi di infrazione del copyright, aumentando i rischi legali per il cliente qualora l'outsourcer impiegasse il software condiviso per erogare servizi ICT ad altri clienti, senza contestualmente regolarizzare insieme al cliente gli aspetti legati, appunto, alla licenza d'uso.

3.3.1.2. Aspetti legati alla gestione delle risorse umane

Con riferimento alle problematiche collegate alle gestione delle risorse umane, interne ed esterne, occorre rilevare che spesso le risorse tecnologiche e quelle umane sono fornite direttamente dalla società esterna e collocate presso le strutture del cliente. L'assenza di risorse specializzate nei comparti di ICT delle aziende viene, in questi casi, compensata dall'intervento esterno e può generare due ordini di rischi. Il primo è un rischio di "frode e di atti illegali da parte di terzi" consistente, ad esempio, in possibili frodi, malversazioni od attività non autorizzate da parte di collaboratori esterni. Il secondo, invece è un rischio legato all'impatto organizzativo derivante dall'esternalizzazione che, almeno in generale, può indurre una modifica dell'organigramma della funzione ICT interna: dall'organico potrebbero, infatti, scomparire le unità organizzative che erano titolari delle attività conferite al fornitore, generando la necessità di elaborare strategie di riconversione o riallocazione delle risorse umane per mezzo di piani di formazione specifici,

oppure di trasferimento di figure professionali al fornitore, o, per mezzo di piani di incentivazione o pre-pensionamento, di risoluzione del rapporto di lavoro.

3.3.1.3. Il rischio legale correlato all'Audit

Il rischio che si associa alla scelta di conferire in outsourcing i Sistemi Informativi dell'azienda viene solitamente collocato nelle aree di carattere economico (affidabilità finanziaria dell'outsourcer), strategico (reale capacità dell'outsourcer di sfruttare l'evoluzione tecnologica), di mercato (dipendenza del cliente dall'outsourcer) o operativo (incapacità dell'outsourcer di erogare il servizio definito dal contratto).

Riguardo la natura di tali rischi va ricordato che quello operativo si rivela particolarmente elevato qualora il contratto non definisca, contestualmente al servizio, i livelli del servizio stesso ed il relativo sistema di gestione (metriche, reportistica, protocolli di comunicazione e penali).

E' interesse comune, del cliente e dell'outsourcer, che questa materia sia definita e formalizzata nella maniera più accurata: è, quindi, praticamente sempre presente nello scopo dell'Audit IS (interno o esterno, del cliente o dell'outsourcer) la revisione dei processi che sono correlati ai Livelli di Servizio concordati in sede contrattuale, al fine di verificarne l'esistenza effettiva e l'efficacia.

Oggi risulta comunque riduttivo limitarsi ai soli aspetti appena ricordati per valutare la natura del rischio insito nell'outsourcing: l'evoluzione delle normative correlate all'IT sta evidenziando, infatti, la necessità di coinvolgere l'outsourcer nella verifica e nella attestazione di aderenza alle leggi cui il cliente è soggetto, essendo consolidato il concetto che il conferimento in Outsourcing non solleva il cliente dagli obblighi che esse impongono, e semmai aggiunge ad essi quello della vigilanza attiva, e delle verifiche, sul fornitore del servizio.

Ciò ha effetti evidenti sull'attività di Audit, ed è quindi di particolare interesse in questa sede.

Esistono nella realtà circostanze che, in relazione al rischio correlato alla legislazione vigente, praticamente inducono una azienda a richiedere un Audit presso l'outsourcer, e di tali circostanze se ne possono citare qui due esempi relativi l'uno al contesto italiano e, l'altro, a quello statunitense: rispettivamente il D.L. sulla Protezione dei Dati Personali ed il Sarbanes-Oxley Act.

- D.L. 196/03 sulla Protezione dei Dati Personali

Il ruolo dell'outsourcer può configurarsi, in rapporto ad una azienda sua cliente che sia "Titolare del trattamento" dei Dati Personali, come quello di "Responsabile del trattamento" degli stessi Dati. In questo caso ogni dipendente dell'outsourcer che questi abbia individualmente autorizzato all'accesso ed all'elaborazione dei Dati Personali per conto del cliente "Titolare", assume per la legge il ruolo di "Incaricato del trattamento".

La circostanza che induce ad estendere un audit sull'eventuale outsourcer si presenta in questo caso perché la legge prevede che tali ruoli si esercitino attenendosi alle istruzioni impartite dal "Titolare", il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni.

Il rischio corso dall'azienda cliente, se omette di verificare (anche eventualmente tramite un Audit) l'operato del "Responsabile del trattamento" e dei suoi "Incaricati", è quindi particolarmente acuto, soprattutto se ad essa venissero contestate inadempienze nella protezione dei dati sensibili, fatto che il D.L. 196/03 assimila all'esercizio di attività pericolose (almeno ai fini del danno).

- SARBANES OXLEY ACT

Ai fini del Sarbanes-Oxley Act (SOXA, legge approvata in U.S.A. nell'estate del 2002) i controlli interni dell'outsourcer IT sono parte integrante di quelli dell'azienda cliente. Questa legge si applica a tutte le aziende quotate negli Stati Uniti, anche se straniere, e si estende a tutte le aree operative di ciascuna azienda, anche quelle collocate fuori degli Stati Uniti.

Con il SOXA il titolare dell'azienda rischia personalmente condanne penali estremamente pesanti da parte del giudice americano, e nella Sezione 404 esso obbliga il Vertice aziendale alla dichiarazione dell'esistenza di un attivo ed efficiente sistema di controlli interni su tutto quanto è correlato al trattamento di dati rilevanti per il bilancio, coinvolgendo quindi esplicitamente i sistemi informativi.

La legge impone inoltre che la dichiarazione sia sottoposta alla validazione di un auditor indipendente ed avente titolo (perché iscritto presso un'authority, il PCAOB – "Public Company Accounting Oversight Board") a rilasciare questo genere di attestato.

L'osservanza del SOXA implica quindi l'obbligo, per il vertice aziendale dell'azienda cliente, di attestare l'esistenza e l'efficacia anche dei sistemi di controlli interni implementati dall'outsourcer e quindi, in pratica, di sottoporre quest'ultimo ad audit allo scopo di acquisirne visibilità e verificarne l'efficacia.

Secondo il PCAOB l'acquisizione di un "Report Type II"[12] conseguente ad un esame SAS-70[13] eseguito da un "Service Auditor" può essere qualificante per l'outsourcer ai fini del suo ruolo in rapporto ad una azienda cliente soggetta al SOXA, ed è corretto aspettarsi che, in generale, l'azienda cliente ed il suo "User Auditor" facciano riferimento a tale Report nell'adempiere agli obblighi di legge relativi alle attestazioni sui controlli interni riferiti al reporting di tipo finanziario.

Di qui l'opportunità per l'outsourcer di conseguire di propria iniziativa, tramite un "Service Auditor", e mantenere nel tempo tale attestazione per poter proporre all'azienda cliente di acquisirla come evidenza di compliance senza tecnicamente incaricare lo "User Auditor" di sottoporre a revisione la sua organizzazione ad ogni ciclo di bilancio.

3.3.1.4. Audit dell'outsourcer da parte di uno "USER AUDITOR"

La circostanza nella quale una azienda che è ricorsa all'outsourcing dei propri sistemi informativi richiede un audit presso l'outsourcer può essere, come si è visto, determinata da fattori di varia natura, non ultimo dei quali un rischio legale, e l'auditor ("User Auditor") potrà essere l'auditor interno dell'azienda cliente stessa o un auditor indipendente.

In ogni caso il contratto di servizio e i relativi accordi sui livelli del servizio stesso, costituiscono la base normativa sulla quale costruire le modalità di svolgimento dell'Audit (in loco o da remoto).

L'outsourcer farà infatti riferimento al contratto con il cliente per verificare che l'ambito e le modalità di svolgimento della revisione gli assicurino comunque la possibilità di salvaguardare l'erogazione del servizio ai livelli previsti per tutti i clienti (incluso il committente dell'Audit), e

[12] Il Report Type II è un report di controllo interno (SAS 70) che può essere prodotto su richiesta dell'auditor che conduce l'audit annuale di una società di servizi.

[13] Lo Statement on Auditing Standards Number 70 (SAS 70) è uno standard per il controllo riconosciuto a livello internazionale dall'American Institute of Certified Public Accountants (AICPA). I SAS 70 sono riconosciuti come controlli di sicurezza approfonditi rivolti ad ambienti di fornitori di servizi, che prevedono controlli sulle reti e relativi processi.

curerà che gli sia garantita la facoltà di applicare tutte le necessarie procedure per la protezione delle proprie informazioni e di quelle degli altri clienti dall'incauta o indebita diffusione.

La salvaguardia dell'erogazione del servizio potrà essere conseguita mantenendo tutto lo svolgimento dell'Audit nell'ambito di ben determinate procedure condivise in via preliminare, e regolando in modo formale e rigido qualsiasi eventuale attività comporti interventi sui sistemi di produzione.

La protezione delle informazioni proprie e dei clienti (incluso il committente dell'Audit) sarà conseguita permettendo l'accesso dello "User Auditor" solo alle informazioni attinenti lo scopo dell'Audit stesso e dietro accordo scritto sulla non diffusione di qualsiasi informazione acceduta direttamente o indirettamente.

Tuttora non sempre il contratto di outsourcing contiene clausole atte a regolamentare esplicitamente lo svolgimento di un Audit richiesto dal cliente. Non ci si riferisce qui al solo sancire il diritto del cliente a richiederlo, ma alla descrizione dei processi da attivare e delle procedure da eseguire, da parte di tutte le parti interessate, nel caso in cui tale diritto sia esercitato. Queste clausole, spesso richiamate come "Audit provisions", servono a tutelare entrambe le parti in quanto garantiscono ad esse l'ottimizzazione delle onerose fasi preliminari di accordo sui tempi, sui ruoli, sulle responsabilità e sui protocolli secondo i quali l'Audit si svolgerà; inoltre, assicurando al cliente che lo "User Auditor" verrà supportato nel più efficiente dei modi nel sito dell'outsourcer, queste clausole garantiscono anche l'outsourcer che la delicata fase del lavoro si svolgerà secondo modalità concordate e soprattutto tali da minimizzare l'impatto sull'erogazione del servizio.

Si pone poi il problema del rapporto tra quanto riportato come risultato di Audit interni o esterni precedenti effettuati da altri "Service Auditor" e l'ambito di un Audit esterno eseguito su richiesta di un cliente da parte di uno "User Auditor".

Mentre in linea generale l'outsourcer può produrre qualsivoglia evidenza delle risultanze degli Audit passati e dei processi atti a garantire l'allineamento alle politiche di gestione del rischio adottate nell'erogazione del servizio, allo scopo di dimostrare l'esistenza e l'efficace applicazione dei controlli interni, lo "User Auditor" può evidentemente chiedere a sua volta di poter eseguire nuovi test sul campo per quei controlli interni o per altri, allo scopo di verificarne l'esistenza e l'efficacia nel periodo temporale di svolgimento dell'Audit, ed a conferma dell'affidabilità globale del sistema di controlli mantenuto attivo dall'outsourcer.

La disponibilità per l'outsourcer di un "Report type II" del SAS-70, che comporta successive osservazioni a regolari scadenze temporali, redatto e rilasciato da un "Service Auditor" indipendente, mette a disposizione dell'azienda cliente la possibilità di utilizzare le attestazioni relative al livello dei controlli interni dell'outsourcer a complemento di quelle relative ai propri, fornendo al proprio Auditor la documentazione di una revisione condotta secondo uno standard effettivamente orientato alla comunicazione tra diversi Auditor e specializzato alle aziende di erogazione di Servizi IT.

Per definizione lo "User Auditor" avrà il compito di svolgere le attività di analisi, verifica e valutazione dei rischi e dei controlli durante il ciclo di vita del contratto.

3.3.1.5. CASE STUDY - La Banca come cliente: il contesto di riferimento internazionale e nazionale

Alla luce delle recenti disposizioni del "**Basel Committee on Banking Supervision**", gli Organismi di Controllo delle banche dovrebbero monitorare costantemente i rischi di outsourcing – i cosiddetti *Key risks in Outsourcing*.[14] Come già evidenziato, il ricorso alle varie forme di outsourcing può esporre, di fatto, una banca all'aumento del rischio e, in particolare, alle varie tipologie di rischio considerate nei documenti ufficiali prodotti nel tempo dal Comitato di Basilea. Nella tabella che segue sono state elencate le principali categorie di rischio associate alle varie forme di outsourcing.

Tabella 6 - Key Risks in Outsourcing

Strategic Risk	The third party may conduct activities on its own behalf which are inconsistent with the overall strategic goals of the regulated entity. Failure to implement appropriate oversight of the outsource provider. Inadequate expertise to oversee the service provider.
Reputation Risk	Poor service from third party Customer interaction is not consistent with overall standards of the regulated entity. Third party practices not in line with stated practices (ethical or otherwise) of regulated entity.
Compliance Risk	Privacy laws are not complied with. Consumer and prudential laws not adequately complied with. Outsource provider has inadequate compliance systems and controls.
Operational Risk	Technology failure. Inadequate financial capacity to fulfil obligations and/or provide remedies. Fraud or error. Risk that firms find it difficult/costly to undertake inspections.
Exit Strategy Risk	The risk that appropriate exit strategies are not in place. This could arise from over-reliance on one firm, the loss of relevant skills in the institutions itself preventing it bringing the activity back in-house and contracts which make a speedy exit prohibitively expensive. Limited ability to return services to home country due to lack of staff or loss of intellectual history.
Counterparty Risk	Inappropriate underwriting or credit assessments. Quality of receivables may diminish.
Country Risk	Political, social and legal climate may create added risk. Business continuity planning is more complex.
Contractual Risk	Ability to enforce contract. For off-shoring, choice of law is important.
Access Risk	Outsourcing arrangement hinders ability of regulated entity to provide timely data and other information to regulators.

[14] Cfr. Basel Committee on Banking Supervision The Joint Forum "Outsourcing in Financial Services", Consultative document, August 2004.

	Additional layer of difficulty in regulator understanding activities of the outsource provider.
Concentration and Systemic Risk	Overall industry has significant exposure to outsource provider. This concentration risk has a number of facets including**:** ▪ Lack of control of individual firms over provider; and ▪ Systemic risk to industry as a whole

Fonte: Basel Committee on Banking Supervision The Joint Forum "Outsourcing in Financial Services", Consultative document, August 2004.

In Italia, nell'ambito dei gruppi di lavoro della Convenzione Interbancaria per i Problemi dell'Automazione – **CIPA** – e sulla scia delle iniziative internazionali, si è voluto intervenire per valutare gli effetti che l'adozione dell'outsourcing può avere sul rischio complessivo di una azienda bancaria. A tal proposito, è stato dichiarato che "il ricorso all'outsourcing, più che considerarsi come una fonte specifica di rischio per l'azienda bancaria, assume rilevanza per il fatto di aumentare l'esposizione dell'intermediario alle varie tipologie di rischio. In particolare, l'affidamento a terzi, in tutto o in parte, del proprio sistema informativo può essere causa di:

- un'incontrollata traslazione al fornitore del governo dei rischi tecnologici e una conseguente deresponsabilizzazione, con effetti pericolosi sulla stessa stabilità aziendale[15];
- un aumento dei rischi strategici, nel caso di mancato raggiungimento da parte del fornitore degli obiettivi concordati;
- l'emergere di rischi legali, connessi ad eventuali controversie relative all'interpretazione o all'inadempimento di clausole contrattuali e, nei confronti dei terzi, ad eventuali carenze nella gestione delle informazioni riservate;
- una particolare esposizione a rischi di reputazione, poiché i malfunzionamenti del servizio verrebbero dalla clientela senz'altro imputati all'intermediario."[16]

In analogia con (ed a conferma di) quanto indicato dalla CIPA, nell'ambito di un generico processo bancario di "erogazione e di supporto" è, ad esempio, possibile identificare le seguenti principali categorie di rischio di outsourcing:

- Rischio di "Selezione e monitoraggio dell'outsourcer";
- Rischio di "Divario di performance tra la società e l'outsourcer";
- Rischio di "Formalizzazione costi, poteri, limiti e livelli di servizio";
- Rischio di "Perdita di Know-how della società/gruppo";
- Rischio di "Sottrazione di clienti da parte dell'outsourcer alla società".

3.3.2. LA SICUREZZA

Tra i rischi operativi correlati con l'outsourcing, così come gia ricordato, devono essere considerati quelli concernenti la sicurezza.

[15] Il riferimento è rivolto a tutte le problematiche connesse alla continuità di servizio.

[16] Cfr. www.cipa.it

Lo scopo di questa parte del documento è descrivere alcune possibili linee guida utili ad individuare e classificare tale tipologia di rischi.

Giova, prima di procedere, richiamare la definizione di **sicurezza** come *l'insieme dei controlli e degli strumenti che permettono di rispondere ai requisiti di riservatezza, integrità e disponibilità delle informazioni e, quindi, anche dei sistemi informativi,* giacché la perdita di disponibilità di un sistema corrisponde anche alla perdita di disponibilità dei dati da esso trattati e, quindi, delle informazioni.

In base a tale definizione possiamo individuare i seguenti rischi operativi relativi ai processi IT, correlandoli al ciclo di vita dell'outsourcing che è stato descritto in questo documento:

ANALISI (*Plan*)

- errata o assente individuazione ed allocazione delle risorse da utilizzare per proteggere le informazioni, nell'ambito della complessiva definizione delle attività oggetto dell'outsourcing e dei rapporti tra le parti;
- insufficiente considerazione delle informazioni disponibili a supporto delle scelte in materia di sicurezza o non disponibilità delle stesse;
- insufficiente od errata definizione dei requisiti di sicurezza, dei livelli di servizio relativi alla sicurezza, delle reciproche responsabilità e delle modalità di controllo.

IMPLEMENTAZIONE E GESTIONE DEL CONTRATTO (*Do*)

- applicazioni in uso non in grado di supportare i requisiti di sicurezza;
- piattaforme tecnologiche in uso non in grado di supportare i requisiti di sicurezza;
- errato/non appropriato utilizzo delle funzionalità di sicurezza delle applicazioni e delle piattaforme tecnologiche in uso;
- insufficiente o assente verifica dei controlli di sicurezza implementati;
- frodi;
- errori di programmazione e/o di configurazione;
- non appropriata definizione del ruolo e delle responsabilità dei terzi a cui l'outsourcer demanda parte delle proprie attività;
- problemi di disponibilità dei sistemi derivanti da mancanza di risorse elaborative;
- insufficiente coinvolgimento del cliente nei processi di disaster recovery e business continuity;
- utilizzo non consentito delle informazioni;
- diffusione di informazioni riservate;
- alterazione dei dati;
- perdita di integrità dei dati;
- distruzione dei dati;
- mancata individuazione e/o risoluzione degli incidenti e delle relative vulnerabilità;
- misure di sicurezza fisica non adeguate a proteggere le infrastrutture tecnologiche;
- errori nell'attività di gestione operativa.

GESTIONE E VERIFICA DEL CONTRATTO (*Check*)

- non corretta misurazione dei livelli di sicurezza e/o comprensione degli stessi;
- inadeguata attività di verifica e di reporting sull'efficacia dei controlli di sicurezza;
- contestazioni sulla misurazione dei livelli di servizio.

EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act*)

- identificazione di nuovi/ulteriori indicatori di performance in base ai quali misurare i livelli di servizio al modificarsi dei requisiti di sicurezza individuati inizialmente;
- inadeguato miglioramento dei controlli in essere in seguito all'evolversi della best practice in materia di sicurezza.

Alcuni dei rischi elencati sono propri di tutte le situazioni in cui si ricorre all'outsourcing, mentre altri sono rischi di sicurezza in sé. Il nostro parere è che nell'analisi dei rischi di sicurezza relativi all'outsourcing debbano essere considerati anche i "normali" rischi di sicurezza, per valutarne la differente significatività (in termini di probabilità e impatto) che, proprio in relazione all'outsourcing, questi ultimi assumono.

Per ciascuna delle tipologie di rischio identificate, proviamo quindi ad analizzare sia il rischio intrinseco sia il rischio di controllo[17].

Una prima riflessione potrebbe riguardare quei rischi che in relazione all'outsourcing modificano la loro rilevanza intrinseca (diventano quindi più o meno probabili o aumentano/diminuiscono il loro impatto sul business) e di quelli che invece mantengono inalterata la loro rilevanza. A tal riguardo potremmo indicare le seguenti linee di analisi:

- i rischi correlati con gli aspetti di definizione a livello contrattuale o comunque formale, anche se extra-contrattuale, aumentano la loro rilevanza, in relazione alla presenza dell'outsourcing. Rientrano in questa prima tipologia i rischi della fase di analisi (o *Plan*) o della fase di evoluzione e revisione del contratto (o *Act*). Infatti il consolidamento formale dei rapporti tra cliente e fornitore, nonché gli interessi delle parti, talora anche contrapposti, introducono elementi di rigidità e di maggiore complessità organizzativa, rendendo conseguentemente maggiore l'impatto di una analisi errata o insufficiente;
- verosimilmente non dovrebbero invece modificarsi i rischi intriseci derivanti da azioni umane intenzionali, quali alcuni dei rischi relativi alla fase di implementazione (o *Do*), ad esempio frodi o diffusione di informazioni riservate, in quanto tale tipologia di rischio è correlata con le caratteristiche delle informazioni elaborate, più che con i processi di gestione delle stesse;
- dovrebbero invece ridursi i rischi intriseci correlati ad errori umani, in base alla considerazione che presso il fornitore dovrebbero mediamente essere presenti maggiori competenze tecniche e processi maggiormente standardizzati (quali altri rischi della fase di implementazione e gestione, ad

[17] Per **rischio intrinseco**, o rischio inerente, si intende il rischio che un determinato evento possa verificarsi a prescindere dagli eventuali controlli posti in essere per ridurne le conseguenze o la probabilità (ad esempio la possibilità che un virus venga inviato alla nostra casella di posta elettronica a prescindere dal fatto che sia stato installato un anti-virus in grado di individuarlo e fermarlo). Per **rischio di controllo**, o rischio residuo, si intende la possibilità che il verificarsi di un determinato evento possa non essere rilevato dai controlli posti in essere e che quindi le conseguenze dello stesso possano manifestarsi (ad esempio la possibilità che l'antivirus non riconosca il virus e quindi non lo neutralizzi).

esempio misure di sicurezza fisica non adeguate a proteggere le infrastrutture tecnologiche o errori nell'attività di gestione operativa);

- infine aumentano, per l'accrescimento della complessità organizzativa, i rischi intriseci relativi alla interrelazione tra cliente e fornitore (nella fase di implementazione e gestione – ad esempio, insufficiente coinvolgimento del cliente nei processi di disaster recovery e business continuity – e i rischi della fase di controllo e verifica).

Una seconda riflessione potrebbe invece riguardare l'aumento, o il ridursi, dei rischi di controllo. In generale, almeno per quanto riguarda il cliente, i rischi di controllo possono accrescersi in caso di outsourcing: le attività, di fatto, sono affidate all'esterno e con esse una parte considerevole dei relativi controlli rendendo più complessa la possibilità per il cliente di individuare e conseguentemente controllare il verificarsi di eventi avversi. Il complessivo rischio di controllo è però influenzato anche dalla capacità del fornitore di individuare e gestire tali eventi, capacità che potrebbe essere influenzata dai seguenti fattori:

- la già ricordata maggiore competenza tecnica e la presenza di processi maggiormente standardizzati del fornitore dovrebbero ridurre il rischio di controllo complessivo;
- la maggiore complessità organizzativa e, conseguentemente, la possibilità che non tutte le informazioni necessarie siano note a chi deve implementare o gestire i controlli, dovrebbero al contrario accrescere il rischio di controllo complessivo.

Giova infine osservare che la rilevanza di questo genere di rischi, espressa sia in termini di probabilità di accadimento sia di impatto atteso sul business aziendale, è correlata con la valutazione dei rischi di più alto livello, di natura strategica e tattica.

In merito alla correlazione con i rischi strategici, un livello significativo di tali rischi si ripercuote negativamente sui rischi di livello inferiore, ivi inclusi i rischi relativi alla sicurezza, soprattutto su quelli la cui rilevanza è aumentata dalla presenza dell'outsourcing (vedi quanto detto sopra).

Dello stesso segno è anche la correlazione con i rischi tattici: rischi tattici maggiori comportano rischi operativi maggiori. Ad esempio, come già detto, i rischi relativi al valore delle informazioni sono correlati con i rischi operativi derivanti da azioni umane volontarie (indipendentemente dalla presenza di outsourcing), mentre i rischi relativi alle conoscenze e alle competenze tecniche del personale impiegato sono correlati con i rischi derivanti da errori.

Come più volte già sottolineato le tipologie di outsourcing sono diverse tra loro e ancor più diverse sono le realtà di outsourcing: la valutazione dei rischi di sicurezza dovrà, di conseguenza, essere calata nella specifica realtà in esame, e sono possibili risultati anche diversi da quelli illustrati.

3.3.3. GLI SLA E IL LORO MONITORAGGIO

Come già indicao nei capitoli precedenti, è importante dedicare attenzione ai contenuti di uno SLA, perchè dalla completezza e precisione dello SLA dipendono in buona parte l'andamento positivo del rapporto e la soddisfazione delle parti.

L'asse portante di uno SLA è comunque la definizione dei criteri concordati che permettano una valutazione oggettiva, basata su dati quantitativi, del servizio erogato.

3.3.3.1. I Principali rischi sottostanti gli SLA

- **Servizi ottenuti difformi da quelli richiesti**

  Tra i principali rischi sottostanti ad uno SLA non ben gestito e/o organizzato, vi è quello di ottenere dei servizi difformi da quanto previsto.

  Per mitigare tale rischio è necessario, innanzitutto, che siano definiti puntualmente tutti i servizi oggetto del contratto con i relativi obiettivi ed il riferimento alla correlazione di questi agli obiettivi aziendali.

  Si può affermare che la conoscenza approfondita dei servizi che si gestiscono internamente è un prerequisito fondamentale alla buona riuscita della loro esternalizzazione.

- **Livello del servizio diverso da quanto previsto**

  Per livello di servizio si intende un aspetto misurabile che sia significativo ai fini della valutazione del grado di soddisfacimento, traducibile nel raggiungimento di specifici valori di soglia, dei requisiti relativi all'erogazione di quel servizio.

  La scelta di quali fenomeni misurare per valutare l'andamento di un servizio, e perciò di quali livelli di servizio concordare con il fornitore, è quindi fondamentale ai fini della significatività della valutazione stessa.

  La scelta, invece, di quali misure sia più opportuno attivare in un dato contesto può dipendere anche dalla facilità di effettuarle, dal costo, dalla capacità di gestire ed elaborare il volume di informazioni raccolte.

  Inoltre, la natura dinamica e continuativa dei servizi consiglia di non basare le valutazioni su singole misure isolate, ma su misure rilevate con continuità durante l'erogazione del servizio, eventualmente nell'ambito di determinati intervalli di tempo.

  In sintesi le misure sull'andamento del servizio possono essere rilevate:

  - con continuità durante l'erogazione;
  - in intervalli di tempo prefissati;
  - in occasione del verificarsi di determinati eventi ritenuti significativi.

  La tipologia delle misure da utilizzare per calcolare i livelli di servizio varia in genere da servizio a servizio: in certi casi saranno più importanti le prestazioni rispetto al tempo (es. tempi di risposta ecc.), in altri andranno contate le occorrenze di eventi, oppure dovranno essere considerati alcuni parametri dimensionali (per esempio: il volume di utenti serviti contemporaneamente da un Help Desk).

- **Difficoltà nel riscontro dei servizi forniti**

Altro componente chiave della gestione di un servizio in outsourcing è la modalità di rendicontazione circa l'andamento del servizio.

E' fondamentale che siano definite le principali informazioni che l'*outsourcer* fornirà al cliente, la periodicità della rendicontazione ed il periodo di copertura cui ogni resoconto si deve riferire.

Per facilitare il riscontro dei servizi erogati il sistema di gestione dei livelli di servizio dovrà preferibilmente essere un sistema automatizzato in grado di assicurare la gestione dei dati di dettaglio inerenti ai servizi e la gestione delle soglie, secondo viste differenti in funzione degli utenti del sistema.

Al sistema di gestione dovrà essere affiancato un sistema di pubblicazione in grado, per esempio, di assicurare la presentazione dei dati su pagine web, l'integrità dei dati ed il controllo degli accessi. Il fornitore dovrà quindi implementare gli opportuni controlli per assicurare accuratezza, completezza e coerenza dei dati forniti.

Se considerata in tempo nella fase di trattativa, la definizione di un'adeguata rendicontazione può essere sicuramente considerata una buona misura atta a mitigare il rischio di un difficile controllo sui servizi e sui livelli di servizi forniti dal fornitore.

- **Controversie inerenti l'accordo di servizio**

  Nella redazione di un accordo di servizio, uno degli elementi da prendere in considerazione sono le penali.

  Le penali devono essere viste all'interno di un accordo di servizio non già come un espediente per far risparmiare il cliente in funzione di un minor livello di servizio ricevuto, ma come uno strumento di governo del contratto, a disposizione del cliente, attraverso il quale segnalare al fornitore la necessità di adottare adeguate azioni correttive.

  La gestione delle penali è, di solito, caratterizzata da una logica di flessibilità legata al fatto che, in qualunque contesto, i livelli di servizio teoricamente raggiungibili nell'erogare un determinato servizio e quelli effettivamente conseguibili non possono sempre coincidere, e chiedere al fornitore di concordare il rispetto al 100% dei livelli di servizio teoricamente raggiungibili comporterebbe costi inaccettabili per il fornitore stesso e, di conseguenza, un prezzo inaccettabile per il cliente.

  Un ulteriore obiettivo delle penali in un contratto è anche quello di scoraggiare il fornitore dall'attuare strategie di ottimizzazione dei propri margini basate sulla riduzione dei livelli di servizio.

3.3.4. LA GOVERNANCE

La IT Governance è parte integrante della Corporate Governance e si riferisce agli strumenti ed all'efficacia con cui un'organizzazione governa e controlla le attività che richiedono l'impiego di sistemi informativi, anche in caso di outsourcing.

E' necessario che il vertice aziendale, nell'ambito della scelta strategica di optare per l'outsourcing, tenga in considerazione che aspetti esterni alla relazione tra le due parti, come le normative nazionali (Privacy, ecc..) o quelle emesse da specifici organismi (Banca d'Italia, Consob) possono avere un impatto rilevante imponendo vincoli e determinando i contorni delle scelte.

- **I Rischi nella Governance**

In questa elencazione dei rischi specifici della governance dell'outsourcing, la prospettiva è quella del cliente, per il quale sono più rilevanti le variazioni rispetto ad una situazione di insourcing, mentre per l'outsourcer (il cui core business è solitamente proprio la prestazione di servizi ICT) i rischi ricalcano prevalentemente quelli relativi ad una gestione interna/insourcing e di "cliente interno".

I rischi indicati valgono, in generale, qualunque siano i servizi /attività /risorse IT esternalizzati, e naturalmente i rischi saranno tanto maggiori quanto maggiori saranno il numero e l'importanza dei servizi /attività /risorse IT esternalizzati.

Nel caso di più contratti di outsourcing con più fornitori diretti, separati, e ciascuno relativo ad un sottoinsieme dei Servizi IT, a quelli citati di seguito si aggiungerebbero i rischi di coordinamento ed integrazione.

Tabella 7. Rischi di Governance

Rischi	Fase ciclo PDCA
Inadeguata selezione dell'outsourcer, con scelta di una azienda che non offra sufficienti garanzie di affidabilità, qualità, ecc.	P
Inadeguata definizione degli accordi contrattuali (vaga o incompleta definizione delle varie componenti oggetto dell'outsourcing, inadeguata definizione dei livelli di servizio previsti e della necessaria scalabilità, inadeguate procedure di revisione, gestione controversie, definizione responsabilità, ecc.)	P
Inadeguata valutazione di costi/benefici e relativi aspetti economico/finanziari contrattuali (canoni, penali, premi, ecc.)	PC
Inadeguata predisposizione di idonee strutture organizzative responsabili della gestione del rapporto cliente-fornitore (demand management, problem management, reporting, evoluzioni, ecc.)	D
Inadeguato controllo su servizio ricevuto e compliance; inadeguate verifiche (dirette e/o tramite terze parti indipendenti) del sistema di controllo interno dell'outsourcer, fondamento per il rispetto degli obiettivi nel tempo.	C
Progressiva perdita di valide competenze interne del cliente sull'ICT, conseguenza della cessione, o destinazione ad altri incarichi, del personale interno ICT, con impatti sulle capacità di vision strategica dell'ICT del cliente stesso.	PD
Dipendenza del cliente dal fornitore, tanto maggiore quanto maggiore risulta la criticità dei servizi esternalizzati e quanto più lunga risulta la durata contrattuale e più gravose le clausole rescissorie.	PDCA

3.4. L'ESECUZIONE DELL'AUDIT

Questa parte sviluppa i temi relativi alle particolari condizioni e modalità di esecuzione di un Audit che comprenda nel proprio scopo la valutazione del livello di controlli interni sui Sistemi Informatici quando questi siano dati in Outsourcing.

Tuttavia, prima di entrare nel merito della trattazione nell'ottica del cliente, vogliamo soffermarci brevemente sull'audit dal punto di vista del fornitore di servizi IT, elemento al quale non sempre viene data la giusta visibilità. Una strutturazione interna all'outsourcer in questo senso è sintomo di qualità del servizio nei confronti del cliente e di corretto indirizzamento rispetto al proprio business.

3.4.1. L'AUDIT NELL'OTTICA DELL'OUTSOURCER

In questa sezione si intende mettere a fuoco il ruolo delle componenti organizzative dell'outsourcer ed i processi interni che questo mette in atto allo scopo di applicare le politiche necessarie a rendere i propri livelli di controllo interno rispondenti alle aspettative, proprie e dei propri clienti, di continuità, affidabilità e integrità dei servizi che esso eroga.

Nel seguito vengono definiti e descritti i seguenti aspetti basilari:

- Audit Interno dell'outsourcer,
- Audit dell'outsourcer da parte di un "Service Auditor",
- La struttura di "gestione della compliance" dell'outsourcer.

Gli aspetti legati al rischio correlato all'outsourcing dei sistemi informativi e l'audit dell'outsourcer da parte di uno "User Auditor" sono già stati affrontati in altre parti dello studio (cap. 3.3.1.4) .

3.4.1.1. Audit interno dell'outsourcer

L'azienda che sul mercato opera come o*utsourcer* di servizi informatici non differisce dalle aziende clienti per quanto riguarda la predisposizione e l'esercizio di processi interni di governo mirati a gestire i rischi, né riguardo agli obblighi cui tutte le aziende sono soggette in virtù delle leggi vigenti nei paesi in cui operano.

In particolare l'*outsourcer* si trova nella condizione di dover anche mettere a confronto le proprie politiche di gestione del rischio con quelle dei singoli clienti ai quali eroga il servizio, e questo è di particolare complessità nel caso più classico, cioè quello nel quale tale servizio è erogato da una struttura organizzativa disegnata per specializzazioni (Servizi di Hosting, Servizi Distribuiti, Servizi di Memorizzazione, Servizi di Rete,…), che gestisce un'infrastruttura tecnologica non dedicata al singolo cliente ma condivisa (sito fisico, elaboratori, periferiche, connessioni…), sulla base di processi coerenti e comuni (Gestione delle modifiche, dei problemi, delle emergenze, della continuità dell'erogazione del servizio, ecc.).

La funzione di Audit Interno dell'outsourcer sottopone quindi a verifica l'efficace applicazione delle politiche interne di gestione del rischio da parte dell'organizzazione che eroga i servizi, e nel farlo deve tener conto di quelle esigenze peculiari dei clienti (derivanti direttamente a loro volta dalle loro politiche di gestione del rischio) che sono tali da introdurre deviazioni dalle politiche stesse dell'outsourcer.

Una contrapposizione di questo tipo va risolta introducendo un processo che isoli e descriva la deviazione, attribuendo esplicitamente le responsabilità di controllo e monitoraggio dei rischi ad essa correlati

La funzione di Audit interno di un'azienda outsourcer dovrebbe promuovere costanti attività di controllo dell'aderenza dei sistemi e dei processi di erogazione alle politiche di gestione del rischio e far evolvere gli interventi di audit da eventi di rilevazione isolati (anche se ripetuti periodicamente) a passi integrati in un ciclo di test /verifica /correzione effettuati nell'ambito dell'erogazione stessa, in un'ottica di produzione industriale.

Diventa quindi compito dell'Audit Interno dell'outsourcer sollecitare la definizione di politiche e l'attivazione e la verifica di processi che assicurano il presidio dei rischi legati alle attività di implementazione e supporto (impostazione dei sistemi, disegno di nuovi processi, disegno delle applicazioni, disegno dell'organizzazione, progettazione, documentazione).

Nell'azienda di Servizi Informatici focalizzata sul mercato dell'outsourcing è quindi opportuna la presenza di componenti organizzative dedicate a favorire l'aderenza dell'erogazione del servizio alle politiche di gestione del rischio, e che a questo scopo definiscono metodi e procedure che dovranno poi essere applicati mediante l'attivazione di processi, ruoli e responsabilità all'interno delle strutture che gestiscono l'erogazione dei servizi.

Il ruolo dell'Audit Interno in un'azienda di Servizi di IT, si esprime attraverso un piano ciclico di verifiche esercitate nei siti di erogazione del servizio, aventi punti di controllo collocati in settori ben definiti, che solitamente sono:

- Sicurezza fisica del sito di erogazione,
- Sicurezza logica delle singole piattaforme informatiche,
- Efficace implementazione dei processi gestione della compliance,
- Processi di gestione delle modifiche e dei problemi,
- Piani di continuità,
- Gestione dell'attribuzione dei costi,
- Gestione di beni fisici,
- Gestione dell'inventario del software e dell'hardware.

Ad ogni ciclo di verifica, che si concretizza quindi in una visita di audit, la funzione di Audit Interno produce una valutazione del livello di controllo esercitato sui processi e sulle componenti aziendali che concorrono all'erogazione dei servizi (operazioni tecniche e di supporto tipicamente informatiche, ma anche attività amministrative di contabilità e gestione del personale, finanziarie, immobiliari).

Le criticità individuate durante ogni verifica vengono formalizzate, una volta condivise con il management del sito sottoposto a revisione, associando ogni singola criticità al rischio ad essa correlato ed al piano d'azione da implementare; il Management del sito dovrà indicare modalità di soluzione, obiettivi, scadenze intermedie, responsabili operativi e figure manageriali coinvolte in una risoluzione efficace della criticità o alla predisposizione di quanto necessario a che la stessa criticità non si ripresenti in futuro.

Particolare attenzione deve essere posta dall'Audit Interno dell'outsourcer alla verifica della effettiva implementazione dei piani d'azione definiti per risolvere le criticità segnalate in sede di revisione. Questo si attua mediante sessioni di revisione di ritorno, dette anche di follow-up, da effettuare dopo un periodo di tempo conveniente (solitamente non superiore a 12 mesi), in quei siti dove il livello di controllo sia stato valutato insoddisfacente.

Nella valutazione del livello di controllo esercitato presso i siti di erogazione, l'Audit Interno di un outsourcer può applicare pesi differenti nella valutazione delle criticità riscontrate a seconda che esse siano o no criticità già segnalate in passato ma non ancora presidiate da adeguati controlli; questo si traduce in valutazioni critiche sulla affidabilità del management stesso quando tali criticità ripetute siano presenti.

Nel caso di aziende di Servizi IT di grandi dimensioni ed a struttura globale, nelle quali l'Audit Interno si trovi a sottoporre a valutazione più Siti in localizzazioni diverse, può essere applicato il principio secondo il quale ogni segnalazione di criticità indipendentemente dal sito in esame ha valore globale per l'azienda e quindi nel caso la stessa criticità sia successivamente riscontrata presso un qualsiasi altro sito, è considerata "criticità ripetuta" e valutata quindi con peso diverso.

Questo metodo richiede un efficiente e costante processo di comunicazione e di revisione delle criticità a livello globale, il che configura un processo di Audit continuo cui l'intera struttura di erogazione del servizio dell'outsourcer si trova soggetta.

3.4.1.2. Audit dell'outsourcer da parte di un "SERVICE AUDITOR"

E' generalmente definito "Service Auditor" l'organizzazione indipendente di revisione cui un'azienda di Servizi IT conferisce l'incarico di sottoporre ad Audit una componente della propria organizzazione.

La scelta di un outsourcer di conferire un tale incarico di revisione risponde normalmente anche ad una logica di attestazione del positivo superamento di una revisione basata su criteri standard, effettuato da una terza parte indipendente e codificato secondo modalità formali accettate dalla comunità delle società di Auditing.

Tale genere di attestazione è perseguita in funzione della necessità di rappresentare in modo oggettivo al proprio cliente il livello di controllo interno che l'outsourcer esercita nell'erogare il servizio, e la standardizzazione sia delle modalità dell'esame che della relazione finale dell'esito possono rendere tale esito riconosciuto anche dall'Auditor del cliente, sia interno che esterno ("User Auditor"), permettendo a questo di acquisire tale attestazione in modo formale nell'ambito della propria valutazione.

Lo standard SAS-70, adottato per l'esame dei controlli interni di una società di servizi di IT, prevede due livelli possibili di esame, ed il più impegnativo – che produce il cosiddetto "Report Type II" (o "Report on controls placed in operations and test of operating effectiveness") – è generalmente conforme alle norme di attuazione della legislazione degli Stati Uniti nell'ambito della legge entrata in vigore nell'Aprile 2002, e nota come Sarbanes-Oxley (sezione 404), cui tutte le aziende iscritte al S.E.C. sono soggette.

Un "Service Auditor" verrà quindi utilizzato, per esempio, da una azienda di servizi IT che voglia sottoporsi ad un esame SAS-70 ed acquisire, per poi mantenere, un "Report type II" col quale presentarsi sul mercato dell'outsorcing ed in particolare ai propri clienti soggetti alla Sarbanes-Oxley, conseguendo un vantaggio competitivo, disponendo di un'opportunità commerciale

aggiuntiva (perché può mettere a disposizione del cliente il proprio report SAS-70) e ponendo le condizioni migliori a minimizzare l'impatto operativo e finanziario che il supporto agli Audit dei propri siti, richiesto da tutti i clienti soggetti alla Sarbanes-Oxley, comporta sull'erogazione del servizio.

3.4.1.3. La struttura di "GESTIONE DELLA COMPLIANCE" dell'outsourcer

Il primo ruolo di una struttura di "Compliance" in una azienda di servizi IT è quello di mantenere tutte le componenti aziendali che contribuiscono all'erogazione del servizio all'azienda cliente sul binario dell'efficace applicazione delle politiche di gestione del rischio e di accertare costantemente la dimostrabilità sostanziale e formale di tale applicazione secondo modalità accettabili da qualsiasi auditor.

Nell'esercizio di questo ruolo, che nel ciclo di ognuno dei contratti di outsourcing sottoscritti con i clienti si colloca nella fase di implementazione, la struttura di "Compliance" agisce come riferimento responsabile funzionalmente per tutti i processi di controllo interno di tipo tecnico e di tipo generale nei sistemi IT, assegnando direttamente ai team di supporto il compito di eseguire specifiche azioni di test ed allineamento dell'ambiente, e verificando i risultati di tali azioni con l'obiettivo di realizzare l'ottica industriale del controllo insito nel ciclo stesso della produzione.

Rientrano nella tipologia dei controlli di tipo tecnico quelli sull'impostazione delle piattaforme tecnologiche (mainframe, midrange) sulle quali si eroga il servizio quali, per esempio, la tracciabilità e attribuibilità delle operazioni di modifica delle librerie critiche del software di base e dei parametri dello stesso, la corretta impostazione dei privilegi degli utenti, il corretto mantenimento delle tabelle dei programmi che operano in stato privilegiato, la corretta gestione dei ruoli operativi e dei conflitti d'interesse tra di essi.

Rientrano invece nella tipologia dei controlli di tipo generale quelli sui processi e l'organizzazione del sito di erogazione quali, per esempio, l'efficacia dei piani di continuità del servizio (Backup, Business Continuity, Disaster Recovery), la sicurezza fisica del sito, la sicurezza logica dei dati, le modalità operative.

Il secondo ruolo di questa struttura è assumere la leadership durante lo svolgimento dell'Audit (interno o esterno), costituendo il punto unico di riferimento per l'Auditor, per il Vertice aziendale e per la Dirigenza del sito obiettivo della revisione.

Espletando questo ruolo, che nel ciclo di ognuno dei contratti di outsourcing sottoscritti con i clienti si può collocare sia nella fase di implementazione (Audit Interno) che in quella di controllo (Audit Esterno), la struttura di "Compliance" è quella che sviluppa i piani di preparazione e di supporto all'Audit, coordinandone poi la conseguente esecuzione.

Durante lo svolgimento dell'Audit la funzione di "Compliance" presiederà tutte le riunioni formali e presenzierà alle interviste più rilevanti, curerà che lo svolgimento dell'attività si mantenga nell'ambito del piano concordato e segnalerà ogni criticità sia al vertice aziendale sia al team di Audit.

In realtà di considerevoli dimensioni non è trascurabile l'importanza della tempestività nella attivazione della struttura di "Compliance" a fronte di una notifica di Audit esterno richiesto da un cliente e, a questo proposito, si riscontra la necessità di formalizzare un "protocollo" interno che, soprattutto in assenza di clausole contrattuali specifiche, stabilisca regole a salvaguardia

dell'erogazione del servizio sulle modalità ed i tempi di tale attivazione da parte delle funzioni aziendali dell'outsourcer che curano il rapporto col cliente che richiede l'Audit.

I contenuti del "protocollo" interno tra "erogatori del servizio" e "gestori del cliente" dovranno coprire i seguenti aspetti:

- il tempo minimo di preavviso dell'inizio dell'Audit,
- l'elenco delle informazioni necessarie da ottenere dall'Auditor al momento del preavviso, e cioè :
    - calendario, luogo e scopo delle visite e delle interviste,
    - aree di revisione previste,
    - identità dei componenti del team,
    - tempi minimi delle richieste di istallazione di strumenti software per la produzione di report,
    - calendario delle riunioni sullo stato di fatto,
    - calendario delle riunioni formali di inizio e fine del lavoro sul campo;
- la necessità della pianificazione congiunta dell'attività e della comunicazione formale dei risultati,
- i criteri che rendono necessaria la sottoscrizione di impegni di non divulgazione delle informazione da parte dei membri del team di Audit.

A fronte del rispetto di questo "protocollo", la funzione di "Compliance" si attiverà per predisporre il più efficiente supporto all'Audit e soprattutto la più adeguata preparazione ad esso curando insieme al vertice aziendale sia la predisposizione del piano di verifiche preliminari nelle aree di prevista revisione sia la più adeguata composizione del team di coloro che, responsabili per le singole aree, saranno impegnati nelle interviste, nell'esecuzione dei test e nella predisposizione e fornitura della documentazione richiesta.

Il "protocollo interno" si pone a complemento del contratto col cliente e si colloca quindi, dal punto di vista dell'outsourcer, nella fase di analisi del ciclo di vita del contratto stesso laddove, per quanto riguarda l'attuazione della prassi che esso definisce, regolamenta la modalità di svolgimento della fase di controllo per quanto riguarda le attività di auditing.

Il terzo ruolo della funzione di "Compliance" dell'outsourcer è quello del continuo sviluppo della cultura dei controlli in tutti i livelli del management della struttura di erogazione del servizio IT, ed in questo si colloca sia nella fase di implementazione del ciclo di vita del contratto (formazione), che in quella di evoluzione (miglioramento continuo). L'esercizio di tale ruolo si realizza tramite la periodica relazione sullo stato dei controlli interni nelle sedi istituzionali e la promozione del coinvolgimento diretto del management nel conseguimento degli obiettivi di compliance tramite le sessioni di training sui processi di controllo interno e attraverso la conduzione di workshop sulla applicabilità globale delle risultanze degli Audit condotti di volta in volta nei singoli siti di erogazione.

3.4.2. GLI STRUMENTI: LE CHECKLIST DI CONTROLLO

Dopo esserci focalizzati su alcune particolarità legate all'ottica dell'outsourcer, abbiamo ritenuto opportuno approntare alcuni strumenti di indagine utilizzabili dall'auditor per effettuare verifiche a fronte delle principali categorie di rischi prese in considerazione nel presente elaborato.

Tali strumenti (checklist di controllo) sono stati presi come riferimento, nel loro formato sostanziale, da quelli già proposti nel Gruppo di Ricerca AIEA "L'Auditing ISO17799/BS7799": tali checklist sono risultate efficaci e danno la possibilità di effettuare analisi più approfondite nei casi in cui venivano registrati punti di discontinuità rispetto ai risultati attesi.

Le domande riferite agli requisiti di controllo risultano variamente dettagliate in base al rischio da analizzare; inoltre alcuni argomenti oggetto delle domande sono ripetuti in uno o più obiettivi di controllo, anche se con sfaccettature differenti.

GUIDA PER LA COMPILAZIONE DELLE CHECKLIST

Ci sono due domande base che potrebbero riguardare ciascun requisito di controllo. Le domande sono:

Q1 – È stato implementato il requisito adeguato?
Sono possibili tre risposte:

- **SI** – significa che gli elementi sono applicati con buona soddisfazione dei requisiti;
  Possono essere fornite alcune spiegazioni per giustificare questa risposta – vedi "COMMENTI" sotto;
- **PARZIALMENTE** – alcune elementi sono applicati secondo i requisiti indicati ma non sono sufficienti per rispondere "SI";
- **NO** – nessun elemento è stato considerato rispetto ai requisiti indicati. Questa è anche la risposta appropriata dove il controllo non è adeguato al sistema sotto revisione. Una risposta "NO" potrebbe anche essere data se un requisito di controllo è rilevante ma è implementato attraverso un altro tipo di controllo.

Q2 – Se un requisito non è pienamente implementato, perché non lo è stato?
È importante capire i motivi della parziale o mancata implementazione. Questi sono classificati secondo le seguenti categorie, con la possibilità di più risposte contemporanee:

- **RISCHIO** - non giustificato dall'esposizione al rischio;
- **BUDGET** - ci sono spesso limitazioni finanziarie riguardanti gli elementi che devono essere implementati;
- **AMBIENTE** - fattori ambientali, come la dislocazione logistica dell'outsourcer, potrebbero influenzare la scelta degli elementi considerati;
- **TECNOLOGIA** - alcune misure sono tecnicamente irrealizzabili a causa dell'incompatibilità dell'hardware e del software;
- **CULTURA** - le limitazioni sociologiche sull'implementazione dei requisiti potrebbero riguardare una nazione, un settore o una organizzazione. Le misure potrebbero essere inefficaci se non sono accettate dal personale e/o dai clienti;
- **TEMPO** - non tutti i requisiti possono essere considerati immediatamente. Alcuni potrebbero aver bisogno di più tempo a causa delle caratteristiche tecnologiche, altri di un'opportunità adatta per essere inseriti in un più vasto piano di miglioramento;
- **Non Applicabile -** per esempio, quando le caratteristiche del rapporto societario tra cliente e fornitore superano gli elementi considerati;
- **ALTRO -** ci potrebbero essere ulteriori motivi per la mancata implementazione oltre quelli sopra elencati;

COMMENTI - in tutti i casi di mancata implementazione dovrebbero essere forniti ulteriori commenti per chiarirne i motivi. Questi potrebbero comprendere:

- Dove i requisiti di controllo sono stati implementati può essere utile, ma non essenziale, descrivere il modo in cui sono stati attivati. Questo in sé potrebbe portare al riconoscimento che devono essere eseguiti ancora ulteriori interventi in quell'area.

In alternativa, la precisazione delle misure implementate può indicare che è stato fatto più di quanto necessario e che può essere operato un risparmio riducendo talune misure;

- Dove non è specificato il motivo per una mancata o parziale implementazione (per esempio quando ricade nella categoria ALTRO), dovrebbe essere fornita una spiegazione di dettaglio;
- Dove il motivo per una mancata o parziale implementazione è tra quelli identificati nelle categorie sopra elencate, dovrebbero essere fornite le opportune spiegazioni;
- In ogni caso dovrebbe essere fornita un'indicazione su quali azioni dovranno essere intraprese e con quali tempi si potrà andare a coprire l'assenza dei requisiti richiesti;
- Dove i requisiti sono stati coperti solo parzialmente, deve essere indicato chiaramente cosa deve essere ancora fatto;
- In alcuni casi potrebbe essere stata presa una decisione per non implementare ulteriori misure in una determinata area: effettivamente è stata assunta la decisione di accettare il livello di rischio. In questi casi dovrebbe essere ampiamente spiegato il motivo di tale decisione.

3.4.2.1. Obiettivo di controllo: Il contratto e la parte legale

IL CONTRATTO E LA PARTE LEGALE

Indice degli argomenti trattati

IL CONTRATTO E LA PARTE LEGALE	
argomento	**Prestazioni rese dal fornitore del servizio**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Nel contratto sono state inserite le clausole di più ampia portata, contenenti le categorie generali delle obbligazioni dell'outsourcer in termini, ad esempio, di gestione tecnico-operativa, di attività di manutenzione correttiva e adattativi, ecc.?					
Sono state previste delle disposizioni relative alla decorrenza e alla durata del contratto?					
Sono state disciplinate le modalità con le quali i servizi devono essere forniti?					
Le parti hanno la possibilità di identificare dei servizi addizionali non previsti in origine (prestazioni dei servizi in luoghi diversi, variazioni alla tempistica, approvvigionamento accelerato di hardware, ecc.)?					
Negli allegati è stata inserita la descrizione tecnica delle varie attività previste dal contratto?					
La struttura degli allegati consente adeguamenti e modifiche in corso d'opera senza necessità di revisionare completamente il contratto nelle sue clausole di carattere generale e speciale?					

Note:_____

IL CONTRATTO E LA PARTE LEGALE	
argomento	**Corrispettivi previsti**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono state identificate le modalità di determinazione del corrispettivo e del relativo pagamento?					
L'ammontare del canone da corrispondere è stato commisurato al livello di utilizzo dei servizi, oltre che al livello di qualità richiesti?					
È stato previsto un allegato che riporta il canone annuo, le tariffe e i prezzi unitari per singole attività compiute?					
È previsto il pagamento delle spese vive sostenute dall'outsourcer nella prestazione dei servizi, ivi inclusi eventuali canoni relativi a linee di trasferimento dati o voce?					

Note:_____

IL CONTRATTO E LA PARTE LEGALE	
argomento	**Definizione dei Service Level Agreement**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Il contratto prevede la possibilità di modificare i livelli di servizio nel tempo in base alle esigenze dell'azienda?					
Sono state definite le soglie minime che costituiscono il corretto adempimento prevedendo delle conseguenze per il mancato raggiugimento delle stesse?					
Sono stati previsti i seguenti requisiti di qualità? • Durata delle operazioni batch, • Puntualità dell'apertura dei servizi on-line, • Integrità e correttezza formale dei supporti contenenti gli output prodotti, • Tempo di risposta ai malfunzionamenti, • Tempo di intervento e di ripristino, • Tempestività di risposta on-line, • Disponibilità.					
Sono state create delle procedure di monitoraggio e di reporting periodico mirate alla verifica del raggiungimento e mantenimento degli standard indicati?					
Sono state previste clausole che stabiliscono gli incentivi e le penali?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
È stata prevista, a scadenze prefissate (p.es. annuali), una verifica della qualità e delle modalità di erogazione dei servizi?					

Note:_____

IL CONTRATTO E LA PARTE LEGALE	
argomento	**Clausole contrattuali inerenti alla collaborazione fra le parti**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Tra gli ulteriori obblighi gravanti sul committente, è stato previsto l'obbligo di collaborazione con l'outsourcer al fine di consentirgli il corretto adempimento delle obbligazioni contrattuali?					
È previsto l'obbligo di fornire tempestivamente dati ed informazioni veritiere e corrette?					
È previsto l'obbligo di garantire all'outsourcer libero accesso ai propri locali, riservandogli degli spazi all'interno degli stessi debitamente attrezzati?					
È garantito all'outsourcer l'accesso al proprio sistema informatico anche tramite le eventuali autorizzazioni di proprietari terzi?					
È prevista la garanzia di disponibilità/proprietà di quanto coperto da diritti di privativa, con corrispondente impegno a tenere indenne l'outsourcer da ogni pretesa relativa?					
È previsto il coordinamento di eventuali servizi erogati da terzi con quelli forniti dall'outsourcer?					

Note:_____

IL CONTRATTO E LA PARTE LEGALE	
argomento	**Rapporti con il Personale**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono stati disciplinati i rapporti con il personale esterno?					
Nel contratto è specificato che il committente non deve interferire nel rapporto di lavoro tra l'outsourcer ed il proprio personale?					
È stata stabilita la possibilità per il committente di comunicare all'outsourcer il mancato gradimento di specifiche risorse, con corrispondente obbligo da parte dell'outsourcer di sostituire l'interessato qualora riscontri un fondamento nelle lamentele?					

Note:_____

IL CONTRATTO E LA PARTE LEGALE	
argomento	**Riservatezza delle informazioni**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono stati definiti obblighi di confidenzialità e riservatezza dell'accordo?					
Le parti hanno assunto l'obbligo di non divulgare le informazioni riservate ricevute?					
È stato precisato che tutte le informazioni comunicate da una parte all'altra sia prima che dopo la data di inizio dell'accordo dovranno essere ritenute ed utilizzate per i soli scopi prescritti dall'accordo che si andrà a sottoscrivere?					
La durata degli obblighi, così come per l'accordo di riservatezza, è stata estesa anche al periodo successivo alla cessazione del contratto. È stato previsto un termine di durata degli obblighi di riservatezza, di qualche anno successivo alla sottoscrizione dell'accordo?					
La clausola contiene l'informativa ed il consenso al trattamento dei dati personali ed include la nomina del fornitore a Responsabile del trattamento?					
Sono state individuate le modalità di scambio delle informazioni, che dovrà avvenire per iscritto al fine di potere identificare come "riservate" le informazioni fornite?					
È stato convenuto che le parti siano esse stesse responsabili per l'osservanza delle clausole da parte di soggetti terzi, estranei al contratto?					

Note:

IL CONTRATTO E LA PARTE LEGALE	
argomento	**Clausole contrattuali ulteriori**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono state previste ulteriori clausole contrattuali per limitare i rischi del contratto?					
Sono state inserite clausole relative all'individuazione dei referenti delle parti ed alla istituzione di un'eventuale struttura di controllo (Comitato di Controllo congiunto cliente/fornitore)?					
È previsto il ricorso a riunioni tra i referenti per le problematiche meno gravi o relative a questioni attinenti i pagamenti, o mancanti pagamenti, delle fatture, stabilendo modalità di contestazione e destinazione delle somme contestate con l'obiettivo di giungere ad una composizione bonaria della questione?					
Le parti si sono impegnate a non sospendere servizi e/o pagamenti in caso di pendenza di contenzioso, vista l'importanza che i servizi resi possono rivestire per il cliente?					

Note:_____

IL CONTRATTO E LA PARTE LEGALE	
argomento	**Clausole di uscita**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Sono state previste clausole che disciplinano la risoluzione ed il recesso, le limitazioni di responsabilità e la fase di conclusione del rapporto contrattuale?					
Sono stati previsti anticipatamente, e quindi in sede contrattuale, l'ammontare dei corrispettivi dovuti per il recesso, con somme a scalare?					
Il corpo contrattuale prevede delle limitate ipotesi di risoluzione immediata, collegate a ripetuti inadempimenti o continuativa violazione dei livelli di erogazione dei servizi, a tutela della continuità del servizio gestito?					
Sono state stilate delle graduatorie di gravità degli inadempimenti dell'outsourcer, associando a ciascuna un punteggio e stabilendo penali e/o possibilità di risoluzione al superamento di determinate soglie nell'arco di un lasso temporale predefinito?					
È stata disciplinata la "restituzione" della struttura necessaria all'erogazione dei servizi al committente ovvero della sostituzione dell'outsourcer con altro operatore?					
È stato predisposto un piano di transizione, identificante gli obblighi di tutte le parti coinvolte, i costi da sostenere e la competenza di tali costi, e la valorizzazione della struttura da restituire o trasferire all'operatore subentrante?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Sono state previste delle garanzie sulla solidità finanziaria dell'outsourcer?					

Note:_____

3.4.2.2. Obiettivo di controllo: La sicurezza

LA SICUREZZA

Indice degli argomenti trattati

LA SICUREZZA	
argomento	**Identificazione dei rischi sulla sicurezza correlati con il ricorso all'outsourcing**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
È stata effettuata una analisi dei rischi sulla sicurezza?					
L'analisi dei rischi ha identificato le minacce derivanti da: - fattori tecnologici? *(considerare ad esempio fattori derivanti da migrazione a nuove piattaforme o modifiche alla rete)* - processi di gestione? *(considerare ad esempio fattori derivanti dai processi di gestione operativa e/o di sviluppo applicativo impattati dall'outsourcing)* - utilizzo di risorse esterne? *(considerare ad esempio fattori derivanti dalla gestione all'esterno di informazioni critiche)* - altri fattori?					
L'analisi dei rischi ha identificato l'impatto di tali minacce sulle applicazioni, l'infrastruttura IT e le informazioni gestite?					
L'analisi dei rischi ha identificato l'impatto di tali minacce su: - gli obiettivi aziendali? - i processi aziendali coinvolti nell'outsoricing? - i beni aziendali?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Per i rischi identificati è stato definito il livello che la società ritiene accettabile?					
Il livello di rischio accettabile è stato definito da un adeguato livello di management aziendale?					

Note:_____

LA SICUREZZA	
argomento	**Valutazione del fornitore e della soluzione offerta**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
I rischi identificati e i livelli ritenuti accettabili dall'azienda sono stati comparati con i rischi derivanti dalla scelta dello specifico fornitore?					
Sono state valutate le misure di gestione del rischio implementate o implementabili dal fornitore e/o dalla società nel rapporto con il fornitore?					
Nel caso in cui l'analisi abbia mostrato la necessità di implementare ulteriori misure di gestione dei rischi: - è stato definito un piano per l'implementazione di tali misure? - è stato definito il costo relativo all'implementazione di tali misure?					
Gli elementi emersi da tale analisi sono stati considerati nella scelta del fornitore?					

Note:_____

LA SICUREZZA	
argomento	**Definizione dei requisiti di sicurezza a livello contrattuale**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Il contratto identifica il cliente come proprietario dei dati e fissa conseguentemente limiti all'utilizzo che il fornitore può fare dei dati?					
Il contratto identifica i requisiti di business relativi alla sicurezza delle informazioni gestite dal fornitore? *(Considerare se i requisiti vengono definiti in modo generico oppure in modo specifico, eventualmente differenziandoli in base alla tipologia di informazione)*					
Il contratto identifica e definisce diverse classi di informazioni e associa a ciascun classe determinati requisiti in termini di riservatezza, integrità e disponibilità?					
Il contratto definisce i processi necessari per classificare le informazioni?					
Se la tipologia di contratto lo richiede, vengono definite le caratteristiche architetturali che i sistemi devono avere rispetto ai requisiti e alle classi di informazioni definite? *(Considerare se vengono definiti determinati requisiti architetturali sulla base dell'analisi dei rischi effettuata e sulla base dei requisiti identificati, anche per tipologia di informazione)*					

Note:_____

LA SICUREZZA	
argomento	**Definizione delle responsabilità e dei Processi per la Gestione della Sicurezza in fase di Contratto**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Il contratto (e/o gli allegati) definisce il processo di identity management e i relativi ruoli sia presso il cliente sia presso l'outsourcer? *(Considerare se il processo definito considera sia i rischi emersi dall'analisi iniziale sia i requisiti di sicurezza identificati)*					
Il contratto (e/o gli allegati) definisce il processo di gestione degli incidenti e i relativi ruoli? *(Considerare se il processo definito considera sia i rischi emersi dall'analisi iniziale sia i requisiti di sicurezza identificati)*					
Il contratto (e/o gli allegati) definisce i ruoli del cliente dell'outsourcer, i processi e le responsabilità in caso di disastro? *(Considerare se il processo definito considera sia i rischi emersi dall'analisi iniziale sia i requisiti di sicurezza identificati)*					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Il contratto (e/o gli allegati)definisce il processo di audit e i relativi ruoli? *(Considerare anche se vengono definite le modalità di gestione delle problematiche che potrebbero emergere dagli audit)*					

Note:_____

LA SICUREZZA	
argomento	**Definizione dei Livelli di Servizio sulla Sicurezza**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Il contratto definisce livelli di servizio per la sicurezza? *(Considerare se i livelli definiti sono di carattere tecnico e/o se derivano dai requisiti di sicurezza identificati)*					
Il contratto definisce indicatori specifici e il processo per la loro misurazione?					
Il contratto definisce un processo di audit sulle modalità di misurazione degli indicatori?					
Il contratto definisce come gestire i casi in cui i livelli di servizio indicati non vengano rispettati? *(Considerare:* - *penali* - *escalation, ecc.)*					

Note:_____

LA SICUREZZA	
argomento	**Sicurezza nell'Implementazione e Manutenzione dei Sistemi**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
E' stato definito un processo (interno al cliente) per la gestione dei progetti di implementazione /manutenzione affidati all'outsourcer? *(Considerare se al processo del cliente corrisponde il processo definito presso l'outsourcer)*					
E' stato definito un processo (interno al cliente) per la gestione di modifiche infrastrutturali affidate all'outsourcer? *(Considerare se al processo del cliente corrisponde il processo definito presso l'outsourcer)*					
Vengono comunicati all'outsourcer i requisiti dell'applicazione in termini di sicurezza? *(Considerare, a secondo della tipologia di outsourcing, se sono stati comunicati* - *i requisiti di business* - *i requisiti funzionali* - *le specifiche tecniche)*					
Vengono comunicati all'outsourcer i requisiti del software infrastrutturale (O.S., DBMS, ecc.) e dell'hardware in termini di sicurezza? *(Considerare, ad esempio, hardening dei sistemi operativi, server e relative applicazioni, configurazioni delle apparecchiature di sicurezza, firewall ecc.)*					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Vengono definiti piani di quality assurance che considerano anche il rispetto dei requisiti di sicurezza delle applicazioni e dell'infrastruttura IT? *(Considerare se tali piani indirizzano anche i rischi correlati a possibili modifiche non autorizzate)*					

Note:_____

LA SICUREZZA	
argomento	**Sicurezza nella Gestione Operativa**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono stati definiti i requisiti in termini di salvataggio e retention dei dati?					
Sono stati definiti i requisiti in termini di sicurezza fisica?					
Esiste un controllo da parte del cliente sulla schedulazione e sulle modifiche alla stessa?					

Note:_____

LA SICUREZZA	
argomento	**Gestione della Sicurezza**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Gli utenti che accedono ai sistemi sono autorizzati dal cliente secondo procedure standard?					
Vengono effettuate delle review periodiche degli utenti che hanno accesso al sistema? *(Considerare le modalità e la periodicità con cui il cliente viene informato o ha la possibilità di conoscere le autorizzazioni di accesso alla sistema)*					
Il cliente viene informato di eventuali incidenti e delle azioni di gestione e risoluzione poste in essere dall'outsourcer? *(Considerare le modalità e la periodicità con cui il cliente viene informato o ha la possibilità di conoscere gli incidenti e/o le anomalie relative alla sicurezza del sistema)*					
La sicurezza della rete del cliente viene monitorata? *(Considerare modalità e periodicità)*					
Vengono effettuati dei vulnerability assessment periodici e il risultato viene comunicato al cliente? *(Considerare modalità e periodicità)*					

Note:_____

LA SICUREZZA	
argomento	**Disaster Recovery**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
L'outsourcing prevede anche un servizio di disaster recovery? *(Considerare, nel caso in cui il servizio di disaster recovery sia fornito da un terzo (diverso dall'outsourcer), se le attività a carico dell'outsourcer sono chiaramente definite)*					
Nel caso in cui sia previsto anche il servzio di disaster recovery, sono definiti i relativi livelli di servizio? *(Considerare, ad esempio, garanzie sui tempi di recovery in caso di incidente, per la ricostruzione di apparecchiature di riserva e recovery dei dati)*					
Vengono effettuati test periodici del disaster recovery plan?					
Ai test partecipa il cliente? *(Considerare, nel caso in cui il servizio di disaster recovery sia fornito da un terzo, diverso dall'outsourcer, se ai test partecipa anche l'outsourcer)*					

Note:_____

LA SICUREZZA	
argomento	**Gestione dei Livelli di Servizio sulla Sicurezza**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Gli indicatori sui livelli di servizio relativi alla sicurezza vengono effettivamente misurati?					
Nell'ultimo periodo (ad es. anno) i livelli di servizio previsti sono stati rispettati?					
Se non sono stati rispettati, sono state poste in essere le opportune azioni correttive? *(Considerare se è stato definito un piano di miglioramento)*					
Sono state effettuati degli audit sulle modalità di misurazione degli indicatori?					
Si sono verificati cambiamenti o sono emersi elementi nuovi che possono richiedere modifiche agli SLA in materia di sicurezza?					

Note:_____

LA SICUREZZA	
argomento	**Audit della Sicurezza**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Vengono effettuati degli audit sugli aspetti relativi alla sicurezza?					
A seguito degli audit vengono definiti dei piani di miglioramento?					

Note:_____

LA SICUREZZA	
argomento	**Monitoraggio dei Processi di gestione della Sicurezza**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
E' stato definito un processo in base al quale l'outsourcer valuta la sicurezza dell'infrastruttura e presenta al cliente la necessità di modifiche infrastrutturali?					
Se si sono verificati incidenti, le azioni correttive appropriate sono state poste in essere?					
Se dal monitoraggio dei livelli di servizio sono emersi problemi, le azioni correttive sono state poste in essere?					
Se dagli audit sono emersi problemi, le azioni correttive sono state poste in essere?					

Note:_____

LA SICUREZZA	
argomento	**Monitoraggio del Contratto**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Viene effettuata una revisione periodica del contratto?					
Tale revisione tiene conto delle modifiche e dei nuovi elementi intercorsi? *(Considerare:* - *nuovi rischi* - *nuovi livelli di servizio* - *punti di attenzione emersi dagli audit, ecc.)*					

Note:_____

3.4.2.3 Obiettivo di controllo: Gli SLA ed il loro monitoraggio

GLI SLA E IL LORO MONITORAGGIO

Indice degli argomenti trattati

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli generali**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
È stata definita la tipologia della gestione oggetto del contratto di outsourcing (facility management, application management, Tlc, ecc).?					
È presente una descrizione di massima sulle aspettative inerenti alla gestione, con evidenza delle principali caratteristiche richieste al servizio (possibili criticità, disponibilità, massima sicurezza ecc..), sulla base delle esigenze del cliente (business driver)?					
È stata definita la periodicità di aggiornamento degli SLA?					
Sono indicate le condizioni di massima nelle quali ha la validità l'accordo (ambientali, societarie, organizzative, tecniche ecc)?					
Sono presenti clausole che considerano eventuali variazioni all'oggetto, quali: eseguire prestazioni non previste (qualora siano indispensabili per l'esecuzione del servizio), tollerare le variazioni (non significative) nelle modalità di esecuzione dei servizi ecc.?					
È presente una scheda relativa alle definizioni che esplicita il significato dei termini tecnici riportati nello SLA?					
Sono stati definiti gli obblighi, da parte del fornitore e del committente, necessari affinché il servizio possa essere espletato (es. disponibilità di personale, strutture, accessi particolari ecc..)?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
È presente uno schema (es. flow chart) che rappresenti graficamente l'oggetto della gestione, i servizi, gli attori (fornitore e cliente) coinvolti, il processo di erogazione ed il controllo dei servizi?					
In base all'oggetto della gestione, sono elencate tutte le tipologie di servizi inclusi (es. gestione dei sistemi, assistenza e risoluzione problemi, servizi specifici, ecc)?					
È stata considerata l'attività di presa in carico del servizio, con evidenza degli obblighi tra le parti (es. formazione, manualistica ecc)?					
Nel caso in cui sia necessaria un'attività di migrazione dei sistemi informatici (ante-gestione), sono state definite le responsabilità tra le parti e le risorse necessarie allo svolgimento di tale attività?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di identificazione dei servizi oggetto di outsourcing**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
È presente l'elenco dei servizi oggetto della prestazione contrattuale?					
Per ciascuno dei servizi oggetto della prestazione è presente una descrizione degli obiettivi posti al servizio (per quelli consolidati è sufficiente l'indicazione del servizio richiesto, per altri più innovativi è necessario dare una descrizione più dettagliata)?					
Per ciascuno dei servizi oggetto della prestazione è presente una descrizione dei principali processi che costituiscono il servizio?					
Se necessario, per ciascun servizio sono definiti i criteri di attivazione e di chiusura del servizio (pianificati, a richiesta ecc..)?					
Sono stati individuati ruoli e responsabilità in essere inerenti la gestione del servizio (sia lato outsourcer sia cliente)?					
Se il servizio è composto da numerosi task, per ciascuno di essi sono attribuite le responsabilità di gestione?					
Sono state definite le finestre temporali di erogazione del singolo servizio (che può rappresentare l'intervallo di tempo nel quale vengono calcolati i livelli di servizio)?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Per determinati servizi sono previsti diversi livelli di priorità di gestione con l'indicazione dei tempi di "reazione"?					
È stata definita una procedura di "escalation" in caso di malfunzionamenti e/o problemi sui servizi ritenuti critici?					
Nel caso di esternalizzazione dell'intera gestione del sistema informatico aziendale, è stata considerata anche l'erogazione del servizio di Disaster Recovery?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sui servizi di Application Management**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono elencate le procedure informatiche in gestione?					
È regolamentata la proprietà dei dati?					
Sono state individuate le tipologie di attività da svolgere (manutenzione evolutiva, manutenzione correttiva, help desk ecc..) e le relative tempistiche di evasione?					
È stato individuato il livello di qualità richiesto?					
È definito il processo di richiesta di cambiamento/evoluzione del software applicativo con l'identificazione dei momenti di controllo/ autorizzazione e dei rispettivi responsabili per entrambi cliente e fornitore?					
È definito il processo di gestione del ciclo di vita del software, in particolare il passaggio dall'ambiente di test/collaudo a quello di produzione con l'identificazione dei principali punti di controllo e dei referenti, cliente/fornitore, responsabili della loro attuazione?					
Sono definite le procedure informatiche ed organizzative per le modifiche in emergenza degli applicativi, i controlli da adottare e i sistemi per la loro completa tracciatura?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
È previsto uno strumento per la tracciatura di tutti gli eventi legati ai processi di change request e change management, adeguata reportistica periodica di sintesi e un processo di comunicazione cliente/ fornitore per la condivisione dell'avanzamento delle attività?					
Sono identificate le procedure e le responsabilità per il governo dei differenti ambienti tecnologici necessari al ciclo di vita del software?					
Sono definite le policy di sicurezza per l'accesso del personale del fornitore a dati e software in produzione, sono attivi opportuni meccanismi di gestione e controllo periodico di utenze e accessi, sono previste penali in caso di accessi non autorizzati all'ambiente di produzione da parte del personale esterno?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sui servizi di Facility Management**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
È stato individuato un adeguato livello di sicurezza relativo a: accesso ambientale sale macchine, controllo accessi dispositivi LAN/WAN e controllo accessi alle applicazioni, in grado di garantire la riservatezza e l'integrità dei dati dell'outsourcer?					
È stato individuato un adeguato sistema di Change Management relativo alle infrastrutture tecnologiche (ampliamenti, upgrade, manutenzioni) che preveda, almeno per i maggiori cambiamenti: un'informativa preventiva, adeguate sessioni di test, un piano di contingency, ecc.?					
Nel caso sia stata compresa nel contratto anche l'erogazione del servizio di Disaster Recovery, è prevista la pianificazione almeno annuale di test (e ricevimento dei risultati)?					
Nel caso in cui il contratto stipulato abbia una durata di alcuni anni, sono definiti anche meccanismi di controllo sulle performance dei sistemi (capacity planning)?					
E' stato verificato che sia stata definita una procedura di "Incident Management" che sia in grado di gestire gli eventuali incidenti, tracciandone gli aspetti salienti e analizzandone le cause?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di scelta dei livelli di servizio: definizione KPI**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Per ciascun servizio o tipologia di servizio oggetto di outsourcing, sono individuate le caratteristiche elementari misurabili?					
Per ciascun servizio o tipologia di servizio oggetto di outsourcing, sono individuati gli indicatori di prestazione quantitativi, derivabili dalle caratteristiche misurabili dei servizi, che esprimono la qualità del servizio erogato (Key Performance Indicator)?					
Per ciascun KPI sono definite le elaborazioni sui dati elementari (espresse ad es. per mezzo di formule) che permettono la loro valorizzazione?					
I dati elementari utilizzati per il calcolo dei KPI sono disponibili con regolarità?					
I dati elementari utilizzati per il calcolo dei KPI sono accessibili con regolarità?					
Sono definiti gli strumenti e i metodi per la misurazione dei KPI?					
I KPI definiti includono i requisiti di disponibilità del servizio?					
I KPI definiti includono i requisiti di efficacia del servizio?					
I KPI definiti includono i requisiti di efficenza (buone prestazioni) del servizio?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
I KPI definiti includono la valutazione del livello di fruibilità del servizio da parte dell'utente finale?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di scelta dei livelli di servizio: misurazione dei KPI**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Sono formalmente assegnati i ruoli dei responsabili della rilevazione e validazione delle misurazioni raccolte sui dati elementari e delle valutazioni dei KPI?					
Per ciascun KPI sono definiti i criteri di rilevazione delle seguenti misurazioni? *(periodo di osservazione oppure condizioni/eventi che determinano l'attivazione e la conclusione della misurazione (data/ orario/ scadenza/ particolari condizioni dell'hardware/software, periodi di picco delle richieste utente, etc.),* *periodicità,* *eventuale numero minimo di misurazioni,* *eventuali periodi di avviamento o di sospensione delle misurazioni (ad es., per la messa a regime dell'accordo di servizio, o in caso di installazione di nuovo sw/hw, etc.))*					
Sono definiti gli strumenti per l'elaborazione e l'aggregazione dei dati elementari e la conseguente misurazione dei KPI?					
Le procedure, gli strumenti e i supporti per la raccolta sistematica ed automatizzata dei dati elementari che definiscono i KPI sono esistenti e funzionanti a regime?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Le procedure, gli strumenti e i supporti per la misurazione dei KPI sono esistenti e funzionanti a regime, dopo adeguato test condotto congiuntamente con il fornitore?					
Sono disponibili a regime le procedure e gli strumenti per la conservazione e l'archiviazione delle misurazioni effettuate e della rendicontazione periodica del fornitore e del cliente?					
L'accesso agli strumenti per l'acquisizione dei dati elementari, la loro aggregazione ed elaborazione è limitato al personale competente?					
L'accesso agli strumenti per la gestione dei diversi valori di riferimento è limitato al personale competente?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di scelta dei livelli di servizio: valori di riferimento**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Per ciascun KPI sono definite una scala di valori e, in questa, delle soglie di riferimento che esprimono il diverso grado di soddisfazione del cliente?					
Per ciascun KPI sono stati stabiliti i valori obiettivo che il fornitore deve raggiungere per non incorrere nel pagamento delle penali e le relazioni numeriche che collegano i valori obiettivo alla definizione numerica dei KPI?					
Sono stati stabiliti valori ottimali di servizio che, se raggiunti, permettono al fornitore di ottenere il pagamento di bonus e le relazioni numeriche che collegano tali valori alla definizione numerica dei KPI?					
Per i KPI che richiedono la comparazione del livello di servizio con la qualità raggiunta nel periodo precedente (ad esempio "Il numero delle eccezioni del mese N+1 deve essere non superiore a quello del mese N) sono stati definiti i valori soglia che costituiscono il livello iniziale di riferimento (nell'esempio citato dovrà essere stabilito il numero iniziale delle eccezioni, ossia il numero delle eccezioni da attribuire al "mese 0")?					
Sono stati definiti dei valori di riferimento dei KPI che guidano l'eventuale attivazione di processi di segnalazione e sollecito al fornitore o l'adozione di misure correttive e/o preventive?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
La definizione dei vari valori di riferimento corrisponde ad una valutazione della criticità del servizio, degli impatti diretti e indiretti di eventuali disservizi e dei costi necessari al loro raggiungimento?					
La definizione dei vari valori di riferimento è stata raggiunta dopo un'adeguato periodo di analisi del servizio e di raccolta preliminare di misurazioni e valutazioni interenti la qualità dello stesso?					
È previsto un processo di revisione periodico dei valori di soglia e dei valori obiettivo?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di scelta dei livelli di servizio: rendicontazione**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni
-

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Sono stati definiti i documenti di rendicontazione che il fornitore deve consegnare al cliente con l'indicazione dettagliata dei contenuti minimi e le scadenze di consegna?					
Sono stati definiti i documenti di rendicontazione che il cliente intende redigere autonomamente ai fini del monitoraggio e controllo dei livelli di servizio con l'indicazione dei contenuti minimi e le scadenze per la loro produzione?					
Sono definite le modalità di rappresentazione e i criteri di interpretazione delle misurazioni rendicontate da cliente e fornitore?					
Sono definite le procedure e gli strumenti per la condivisione e validazione dei documenti di rendicontazione periodica, nonché strumenti per l'estrazione di statistiche sull'andamento dei livelli di servizio? Documenti e informazioni sono disponibili e accessibili con regolarità, gli strumenti sono esistenti e funzionanti a regime?					
L'accesso agli strumenti di gestione dei report è limitato al personale formalmente autorizzato?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono definiti i processi di controllo periodici dell'andamento dei KPI, quali ad esempio incontri cliente-fornitore per l'analisi delle misurazioni effettuate nel periodo?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di scelta dei livelli di servizio: Penali / Bonus**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono definiti e documentati i criteri per il calcolo delle penali a fronte del non raggiungimento dei valori obiettivo?					
Sono definiti e documentati i criteri per il calcolo dei bonus a fronte del raggiungimento dei valori ottimali?					
Le procedure e gli strumenti per il calcolo automatizzato di penali e bonus sono disponibili, attivi e funzionanti a regime?					
Sono definite e documentate le eventuali franchigie per penali e bonus?					
Sono definiti specifici report per documentare le cause e gli importi di penali e bonus, sono specificati i responsabili della loro elaborazione, le scadenze di consegna e i destinatari?					
Esiste uno specifico processo di analisi e verifica delle misurazioni che generano addebito di penali o riconoscimento di bonus che precede l'adozione delle rispettive misure nei confronti del fornitore, al termine del quale sono tempestivamente informate le strutture competenti per il controllo del budget?					
Il processo di addebito delle penali o di riconoscimento dei bonus prevede autorizzazioni formali da parte delle strutture competenti?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono stati censiti e documentati i casi di non applicabilità delle penali o le situazioni che esonerano il fornitore dal raggiungimento dei valori obiettivo?					
L'accesso agli strumenti per il calcolo di penali e bonus è limitato al personale formalmente autorizzato?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di gestione operativa dell'Outsourcing: rendicontazione**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Per la fase iniziale di erogazione del servizio è stato previsto un periodo di osservazione relativamente all'andamento del servizio, a seguito del quale perfezionare quanto stabilito?					
È stata definita la periodicità di rendicontazione più opportuna (mensile, trimestrale ecc..)?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di gestione operativa dell'Outsourcing: gestione**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
È stato adottato un sistema automatizzato di gestione dei livelli di servizio?					
Se adottato, il sistema consente di gestire: l'acquisizione dei dati, la normalizzazione/ elaborazione degli stessi e la gestione delle soglie?					
Il sistema automatizzato garantisce adeguati controlli sulla qualità (accuratezza, completezza) dei dati in input?					
È stata utilizzato un sistema di pubblicazione automatizzato dei livelli di servizio, il quale consente di gestire diverse tipologie di viste (in base alle necessita)?					
Il sistema produce delle statistiche relative ai periodi di erogazione del servizio?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di gestione operativa dell'Outsourcing: Problem Management**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
È stata concordata una prassi operativa da seguire in caso di problemi rilevanti nella gestione del servizio?					
La prassi operativa concordata prevede la registrazione automatizzata dei problemi riscontrati, con almeno le informazioni relative a: l'identificativo del problema, data di apertura e chiusura, il richiedente, l'azione attivata, l'applicazione o il servizio in errore, ecc.?					
La prassi operativa concordata prevede la rendicontazione statistica dei problemi riscontrati (il numero, la distribuzione per argomento, i tempi di risoluzione, ecc..)?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di gestione operativa dell'Outsourcing: aspetti organizzativi / continuità operativa**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono previste indagini periodiche relative alla soddisfazione del cliente in merito ai servizi erogati?					
Sono previsti incontri periodici tra le parti al fine di analizzare la rendicontazione prodotta ed approfondire eventuali problematiche emerse?					
È stato formalmente attribuita la responsabilità di gestione e monitoraggio dei livelli di servizio (da ambo le parti)?					
Nel caso in cui la tematica sia compresa nel contratto, è prevista la verifica che i livelli di servizio definiti siano coerenti con la classificazione delle risorse ICT e le esigenze di business (priorità applicazioni, RTO ecc..) del cliente?					
Il committente ha ricevuto adeguata documentazione e formazione sulle procedure del piano di continuità operativa?					

Note:_____

GLI SLA E IL LORO MONITORAGGIO	
Argomento	**Controlli sul processo di gestione operativa dell'Outsourcing: Pricing & Help Desk**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
È stato concordato un sistema di pricing adeguato alla tipologia di contratto stipultato (fisso, variabile in base al livello di servizi erogato, ecc..)?					
Il supporto agli utenti avviene tramite una struttura di Help Desk (lato fornitore)?					
Le richieste degli utenti sono registrate e conservate mediante procedure e strumenti adeguati?					
È regolarmente prodotto ed analizzato un reporting periodico su tutte le richieste ricevute dall'Help Desk e comparato con le rilevazioni dei LdS effettuate (analisi da portare agli incontri tra le parti)?					

Note:_____

3.4.2.4 Obiettivo di controllo: La Governance

LA GOVERNANCE

Indice degli argomenti trattati

LA GOVERNANCE	
argomento	**Controlli sui punti qualificanti generativi dell'outsourcing e sul governo del contratto**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
E' stata creata una struttura/comitato, di livello aziendale adeguato, per le scelte relative all'outsourcing?					
E' stata effettuata un'adeguata selezione/valutazione dei servizi/componenti che si intendono esternalizzare?					
E' stata effettuata un'adeguata valutazione della forma di outsourcing da adottare?					
E' stata effettuata un'adeguata valutazione/stima di costi e benefici, con il coinvolgimento dei responsabili delle varie componenti (economiche, operative, organizzative, tecnologiche, ecc.)?					
E' stata effettuata un'adeguata valutazione dei rischi legati all'esternalizzazione di tali servizi/componenti?					
E' stato esplorato adeguatamente il mercato alla ricerca dei fornitori migliori?					
E' stato effettuato un'adeguato processo di selezione dell'outsourcer?					
Sono state verificate solidità, affidabilità, prestazioni, qualità dell'outsourcer, e possibili vincoli o conflitti?					

Note:_____

LA GOVERNANCE	
argomento	**Controlli sui punti qualificanti generativi dell'outsourcing e sul governo del contratto**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
E' stata verificata presso terzi della capacità dell'outsourcer di rispettare le prestazioni ed i livelli di servizio concordati?					
Sono state mantenute all'interno risorse umane con profili tali da poter gestire con competenza adeguata il rapporto con l'outsourcer?					
E' stato steso ed approvato dal legale e dal management, un contratto di outsourcing, che copra adeguatamente i vari aspetti, da quelli prettamente legali a quelli operativi, organizzativi, economici, di servizio, ecc.? *(per dettagli vedere parte su Contratto)*					
E' stata prevista una exit-strategy?					
E' stato previsto un "diritto di audit" da parte dell'outsourcee sull'outsourcer?					
Sono stati definiti, all'interno del contratto e relativi allegati, adeguati livelli di servizio? (per dettagli, vedere parte su SLA)					
Sono state predisposte idonee strutture organizzative responsabili della gestione del rapporto cliente/fornitore (dal demand management, al problem management, al reporting, ecc.)?					

Note:_____

LA GOVERNANCE	
argomento	**Controlli sui punti qualificanti generativi dell'outsourcing e sul governo del contratto**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO……	
Sono state previste adeguate forme di reporting del servizio erogato?					
Sono previste penali? Ricorrendone le condizioni, ci si attiva per incassarle?					
Sono state identificate ed esplicitamente specificate le clausole contrattuali relative a sicurezza e controllo degli accessi, nonché alla proprietà dei dati? Tali clausole sono conformi ai requisiti legali e a quelli previsti dai regolamenti vigenti (es. Codice sulla privacy)?					
Sono state previste clausole contrattuali con riferimento alle responsabilità relative alla proprietà dei dati (ad esempio, è stato stabilito il confine tra la responsabilità dell'outsourcer e del cliente in merito alla correttezza dei dati)?					
Sono state previste misure per il back-up e il disaster recovery? Sono state considerate le problematiche legali connesse alle responsabilità per garantire la continuità aziendale?					
Sono state incluse le modalità di collaudo e documentazione dei risultati del collaudo (anche mediante attestazione del management dell'outsourcer)?					

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono state specificate le misure di sicurezza relativamente ai dati ed alle modalità di accesso ai dati (incluse le modalità di accesso da remoto)?					

Note:_____

LA GOVERNANCE	
argomento	**Controlli sui punti qualificanti generativi dell'outsourcing e sul governo del contratto**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Sono state specificate le misure di sicurezza delle reti di comunicazione, delle connessioni ad Internet (ISPs) e dei siti web aziendali?					
E' stata verificata l'adeguatezza della banda di rete o comunque della capacità di trasmissione delle informazioni rispetto alle esigenze aziendali presenti e pianificate?					
Sono indicate le modalità di gestione dei dati (conservazione, utilizzo, monitoraggio dello stato dei dati)?					
E' stata valutata la dipendenza dall'outsourcer per lo sviluppo e la manutenzione di nuovi sistemi?					
E' stato indicato un ordine di priorità nella gestione del portafoglio progetti?					
Sono state stabilite le modalità di gestione dei progetti per nuovi sistemi in funzione delle prestazioni realizzabili?					
Viene costantemente monitorata la conformità ai termini contrattuali (es. servizio erogato vs. pagamenti effettuati)?					
Viene costantemente valutata la profittabilità del servizio anche in relazione al costo dei livelli di servizio effettivamente erogati?					

Note:_____

LA GOVERNANCE	
argomento	**Controlli sui punti qualificanti generativi dell'outsourcing e sul governo del contratto**

NOTA BENE:

- Considerare gli aspetti relativi agli obiettivi di controllo e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggerimenti	
	SI	PARZ.	NO	RISCHIO, BUDGET,AMBIENTE, TECNOLOGIA,CULTURA,TEMPO,N/A,ALTRO.....	
Viene verificata la conformità ed adeguatezza delle misure di sicurezza effettivamente in essere?					
Viene valutata la qualità delle informazioni prodotte e l'adeguatezza del patrimonio informativo disponibile rispetto alle esigenze dell'organizzazione utente?					
Viene valutata la capacità di informare e supportare il cliente in caso di criticità relative all'integrità delle informazioni?					
Vengono costantemente monitorate le prestazioni e la conformità ai livelli di servizio concordati contrattualmente? La reportistica prodotta è adeguata?					
Viene svolto un adeguato controllo sui servizi erogati e sul rispetto degli SLA?					
Viene effettuato un piano strategico pluriennale dell'IT?					
Viene utilizzata qualche metodologia di governance dell'Information Technology che coinvolga i vertici aziendali?					
Vengono svolte verifiche sul sistema di controllo interno dell'outsourcer?					

Note:_____

APPENDICE

A.1. Definizioni

- **INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)**

  L'insieme dei settori riguardanti l'informatica (IT) e le telecomunicazioni (TLC) accomunati dall'utilizzo della tecnologia digitale.

  L'Information and Communication Technology è un insieme integrato di tecnologie informatiche e di comunicazione attraverso le quali, oltre alla codifica dei dati e loro elaborazione, è possibile gestire informazioni e processi, consentire una circolazione delle informazioni e delle conoscenze che permetta di raggiungere, attraverso una gestione ottimale delle risorse, risultati maggiormente efficaci ed efficienti.

- **ESTERNALIZZAZIONE**

  Realizzazione o utilizzazione del patrimonio informatico di un'impresa da parte di una società terza. Vedi Outsourcing.

- **OUTSOURCING**

  Espressione tratta dal linguaggio delle scienze economiche e sociali, indicativa delle tecniche con cui un'impresa scompone i propri processi di business e ne dismette la gestione diretta di alcuni segmenti per affidarli ad un soggetto esterno.

  L'outsourcing consiste nell'assegnazione ad organizzazioni esterne specializzate di attività o di processi tradizionalmente interni all'azienda, che in questo modo può valorizzare le proprie competenze distintive concentrandosi sulle attività a maggior valore aggiunto.

- **OUTSOURCING ICT**

  Attività di gestione di servizi ICT svolte, per un periodo di tempo prolungato (diversi anni) e definito a livello contrattuale, da un operatore esterno all'azienda cliente, permettendo a quest'ultima di concentrarsi sul proprio core business.

  Tali servizi continuativi vengono erogati in base a diverse tipologie di contratto che ne caratterizzano le modalità di esecuzione e ne identificano il grado di esternalizzazione.

  Outsourcing: modalità contrattuale per i servizi di gestione dell'infrastruttura e dell'ambiente applicativo da parte di un operatore esterno cui il cliente trasferisce gli asset coinvolti nella gestione e, in alcuni casi, anche parte del personale interno.

  Facility management: modalità di contratto per i servizi di gestione di una intera infrastruttura o di una parte consistente di essa che rimane comunque di proprietà del cliente.

  Maintenance & support: modalità di contratto per i soli servizi di assistenza tecnica (manutentiva e di supporto) dell'infrastruttura relativa al Sistema Informativo (o parte di esso): in questo caso la responsabilità della gestione rimane a carico del cliente.

- **INSOURCING**

  Oggi l'insourcing viene definito soprattutto per opposizione all'outsourcing, poiché non vi sono riprese né di attivi né di personale. Il prestatore d'opera assicura il controllo del mantenimento e del miglioramento di un sito e la gestione delle sue infrastrutture con un impegno forte sui risultati, negoziati di concerto. La definizione resta tuttavia a geometria variabile; alcune società di servizi informatici vi inglobano lo sviluppo di applicazioni.

- **INTEGRAZIONE VERTICALE**

  Processo di concentrazione tra imprese che svolgono fasi successive di intervento nella creazione di uno stesso prodotto/servizio o nella realizzazione di un determinato processo.

- **SLA - SERVICE LEVEL AGREEMENT**

  Termine anglosassone che indica principalmente un contratto tra un ISP (Internet Service Provider) e il suo cliente nel quale vengono specificati, in termini misurabili, i livelli di servizio sulla rete garantiti dal fornitore. Molti ISP ormai adottano questo genere di rapporto contrattuale, così che il loro livello qualitativo di servizio può essere misurato, giustificandone talvolta prezzi apparentemente elevati e consentendone un confronto con la concorrenza. Di solito gli SLA prevedono, in caso di disservizio, un risarcimento monetario o uno sconto sulle fatture seguenti.

  Alcune misurazioni adottate negli SLA sono:

  - La percentuale di up-time del servizio (ovvero, quanto, in percentuale il servizio sarà disponibile; ad es. 99,8%)
  - Il numero massimo di utenti che possono essere serviti contemporaneamente (in caso di Hosting o di applicazioni in affitto)
  - La schedulazione anticipata di eventuali disservizi previsti sulla rete che potrebbero avere effetto sui clienti (per esempio in caso upgrade della rete)
  - Il tempio medio di intervento dalla segnalazione di disservizi
  - Il tempo medio di attesa da parte dell'Help Desk.

- **BPO - Business Process Outsourcing**

  L'espressione indica l'esternalizzazione (outsourcing) di un processo aziendale affidandolo ad un fornitore che diviene responsabile della sua gestione, ovviamente sulla base di regole e criteri di misurazione dei risultati predefiniti. Il fornitore di un simile servizio diviene quindi responsabile del funzionamento di tutte le componenti del processo (dalle tecnologie utilizzate alle risorse umane impiegate) così come dei risultati ottenuti e di tutte le attività collaterali implicate (invio fatture, selezione del personale, scelte tecnologiche, ecc.).

- **JOINT VENTURE**

  Associazione di due o più aziende per la realizzazione di un progetto di natura industriale o commerciale e che vede l'utilizzo sinergico delle risorse portate dalle singole imprese partecipanti.

- **ASP - APPLICATION SERVICE PROVIDER**

  Il termine ASP, acronimo di "Application Service Provider", rappresenta il complesso di strutture e risorse che erogano un servizio informatico, tipicamente tramite l'utilizzo della rete Internet a banda larga o su reti private VPN. Applicazioni coinvolte: tutte, in teoria, dalla e-mail agli Erp (programmi di gestione integrati) passando per l'office automation.

  La fornitura di servizi in modalità ASP avviene generalmente dietro il pagamento di un canone fisso o commisurato all'utilizzo delle applicazioni (tipicamente per numero di utenti o, come nel caso dell'outsourcing degli stipendi, per numero di cedolini elaborati).

- **INTERNET SERVICE PROVIDER (ISP)**

  Letteralmente "fornitori di servizi Internet". Operatori che dispongono di proprie reti di telecomunicazione e forniscono l'accesso ai servizi Internet ad individui e organizzazioni. Gli ISP possono anche rivendere la facoltà di utilizzo della rete e dei servizi ad altri operatori, che possono operare a loro volta come fornitori di servizi utilizzando un proprio marchio e/o il marchio del Service Provider.

- **MANAGEMENT SERVICE PROVIDER (MSP)**

  Azienda che offre come propri servizi la possibilità di gestire per conto del proprio cliente le tecnologie informatiche. Un esempio chiarificatore è il caso in cui si chieda l'intervento in maniera continuativa di un MSP, nell'ottica di amministrare i propri computer e i propri server in alternativa a farlo con proprie risorse umane interne. Quindi, accedere ai servizi di un MSP, significa dare in outsourcing (si veda) una parte dei propri processi aziendali.

- **STORAGE SERVICE PROVIDER (SSP)**

  Azienda che offre "spazio disco" e la relativa gestione alle altre aziende che ne fanno richiesta. Ciò indica la possibilità per un'azienda cliente di usufruire di soluzioni di back-up, duplicazione dati, al fine di tutelarsi da eventuali perdite di dati o per rendere questi ultimi disponibili su più locazioni geografiche. Il servizio di un SSP può essere pagato mensilmente, come un affitto, oppure in funzione dei dati depositati o ancora per traffico generato presso l'SSP.

A.2. Classificazioni

Classificazione delle forme di outsourcing

Il fenomeno outsourcing può manifestarsi in una molteplicità di varianti.

La prima è il **"full outsourcing"**, che vede l'evoluzione dalla gestione in proprio all'esternalizzazione secondo criteri e finalità comuni tra cliente e provider; si fonda, quindi, sull'instaurarsi di una partnership tra le due parti, che assicura un elevato livello operativo e strategico, nonché la massima condivisione degli obiettivi.

Altra tipologia consiste nell'"**outsourcing di base"**, dove si ottiene di nuovo una gestione di terzi, al minimo costo, ma con uno stretto controllo sulle operazioni delegate, attraverso la gestione totale o parziale all'esterno dell'area interessata ed il mantenimento al proprio interno delle funzioni di controllo delle operazioni.

Una tipologia particolare di full outsourcing, detto **"transformational outsourcing"** si verifica quando, oltre all'affidamento esterno di una particolare area, si modifica la tradizionale struttura aziendale per le aree correlate. Questo fenomeno nasce e trova applicazione soprattutto in ambito informatico, che attualmente si configura come il più dinamico per quanto riguarda il ricorso all'outsourcing.

Infine, **l'"outsourcing funzionale"** si concretizza nella terziarizzazione di singole funzioni aziendali o parti di esse, a conferma della sempre maggiore pulsione all'esternalizzazione di funzione piuttosto che di processo.

Classificazione in funzione dell'oggetto di outsourcing

L'evoluzione del mercato dei servizi di outsourcing (da una parte l'affermarsi di contratti di outsourcing maggiormente flessibili, e dall'altra la tendenza da parte di alcuni fornitori a integrare in "pacchetti" servizi prima venduti singolarmente da più vendor) ha visto l'affermarsi di approcci più focalizzati su singoli aspetti del sistema informativo aziendale. Tale evoluzione ha portato alla presenza di un'ampia gamma di tipologie di outsourcing classificabili nel seguente modo:

- IS Outsourcing (cioè dei sistemi informativi);
- Processing Services, che include ad esempio servizi di elaborazione dati come la gestione paghe;
- Business Process Outsourcing (BPO), un mercato emergente dove vengono prese in gestione oltre alle risorse del sistema informativo anche parte di alcuni processi aziendali, come le attività di marketing. A questi servizi si aggiungono, come si è visto prima, i Managed Services.
- i cosiddetti servizi xSP.

I servizi di outsourcing, si distinguono per diversi elementi: trasferimento o meno di personale e della proprietà di asset aziendali dall'azienda cliente al fornitore; lunghezza e valore del contratto; ampiezza del servizio.

Inoltre i servizi di outsourcing possono essere suddivisi in tre sottocomponenti. Il primo, il desktop management, vede una relazione contrattuale che prevede l'esternalizzazione delle attività di gestione e manutenzione dei pc aziendali e del loro ambiente. A questo si affianca poi il network management, dove il rapporto tra azienda utente e fornitore riguarda le attività di gestione e manutenzione della rete aziendale ed eventualmente i servizi di sicurezza gestita. Tra i servizi di outsourcing si inserisce infine l'application management, in cui il cliente affida a terzi

le attività di sviluppo, gestione e manutenzione delle applicazioni aziendali. Queste possono essere proprietarie o pacchettizzate, e residenti fisicamente presso un data center o presso la sede del cliente.

Classificazione in relazione alle attività/funzioni aziendali gestite in outsourcing

L'outsourcing di una o di un insieme di attività/funzioni aziendali può configurasi in diverse tipologie:

- SPIN OFF - L'azienda cliente crea una business-unit/nuova azienda, specializzata nel servizio preso in considerazione, che si configura attorno alla precedente funzione aziendale di cui rileva le risorse. La funzione dell'azienda madre diventa una nuova società di servizi e può ampliare la sua offerta anche al mercato esterno.

Tuttavia esistono anche altre soluzioni d'outsourcing applicabili, tra cui:

- CONTRATTO DI FORNITURA - L'azienda cliente individua il fornitore di servizi logistici con riconosciuta qualifica e adeguata massa critica e mediante un contratto di fornitura gli affida la gestione delle attività oggetto d'outsourcing;
- SOURCING ESTERNO - L'azienda cliente delega le parti meramente esecutive delle attività oggetto d'outsourcing, ma ne mantiene il controllo, e ricerca la disponibilità di uno o più fornitori specializzati per i singoli servizi;
- JOINT-VENTURE E PARTNERSHIP - L'azienda cliente e il fornitore di servizi sviluppano un'attività imprenditoriale congiunta, che assicuri la reale possibilità di sinergie con flussi aggiuntivi e contributi di esperienza e di personale paritetici;
- CESSIONE DI RAMO D'AZIENDA - L'azienda cliente cede ad una terza parte un proprio ramo d'azienda. Tale accordo può avvenire con la sola cessione di personale (outplacement) all'operatore, che provvede alla gestione in-house delle attività o, in alternativa, anche di aree, apparecchiature ed impianti dell'azienda cliente.

BIBLIOGRAFIA

Cesara Pasini, “I servizi di outsourcing informatico”, Ed. Franco Angeli, 2001

MIP-EDS, “ICT strategic sourcing: un'ottica diversa nelle scelte di outsourcing”, novembre 2005

AA.VV., “Speciale outsourcing”, Bancaforte – AbiLab, Novembre/Dicembre 2002

ABI, “Linee Guida dell’Associazione Bancaria Italiana per l’adozione di modelli organizzativi sulla responsabilità amministrativa delle banche”, febbraio 2004

Azzaro A. M., “Contratto e mercato”, Giappichelli, Torino, 2004

Basel Committee on Banking Supervision - The Joint Forum, “Outsourcing in Financial Services”, Consultative document, August 2004

Bragg, Steven M., “Outsourcing: A Guide to ... Selecting the Correct Business Unit ... Negotiating the Contract... Maintaining Control of the Process, New York, USA, John Wiley & Sons Inc. ”, 1998

Champlain, Jack J., “Auditing Information Systems”, 2nd Edition, New Jersey, USA, John Wiley & Sons Inc., 2003

Deloitte, “The Titans take hold: How offshoring has changed the competitive dynamic for global financial services institutions”, 2004

Deloitte, "Making the off-shore call:The Road Map for Communication Operators", 2004,
URL: http://www.deloitte.com/dtt/cda/doc/content/ca_tmt_offshoreoutlook.pdf

Friedberg A.H., W.A.Yarberry Jr., “Audit rights in an outsource environment. Internal Auditor”, pag. 53-59, August 1991

Gay, Charles E.; James Essinger; “Inside Outsourcing: The Insider's Guide to Managing Strategic Sourcing”, Nicholas Brealey Publishing, London, 2000

Gates J., “Successful outsourcing depends on a successful contract. Corporate Controller”, pag. 17-19, May-June 1992

Guerrieri C., “I Contratti di Impresa”, Il Sole 24 Ore libri, 1995

ISACA, Top Three Potential Risks With Outsourcing Information Systems, 2005,
URL: http://www.isaca.org

Kearney A.T., "Making Offshor Decisions: 2004 Offshore Location Attractiveness Index", 2004,
URL: http://www.atkearney.com/shared_res/pdf/Making_Offshore_S.pdf

McKinsey Global Institute, "Offshoring: Is it a Win-Win Game?", August 2003.
URL: http://www.mckinsey.com/knowledge/mgi/rp/offshoring/perspective/

Mylott, Thomas R., III., “Computer Outsourcing: Managing the Transfer of Information Systems”, Prentice Hall, New Jersey, USA, 1995

MF Focus, “Capire l’outsourcing tecnologico”, 2004

Outsourcing Information Systems, 2004,
URL: http://www.aicpa.org/cefm/outsourcing.asp

PWC, "A Fine Balance: The Impact of Offshore IT Services on Canada's IT Landscape", 2004.
URL: http://www.pwc.com/ca/afinebalance/

Wright Catherine, “Top Three Potential Risks With Outsourcing Information Systems”, Volume 5, Oxford University's Institute of Information Management and the University of Missouri, (USA) , 2004

Alessandro Allaria, "Il contratto i outsourcing quale scelta strategica per le imprese",
URL: http://www.iusreporter.it/

Giorgio Cian, Alberto Trabucchi, "Commentario breve al Codice Civile" - CEDAM, 2004

Marco Camuffo, "IT outsourcing" - ITER n. 1, 2004

Anna Dessi, "Il contratto di outsourcing" – IPSOA, 2004

Nirvana Martina de Angeli, "Il contratto di outsourcing: consigli e indicazioni tecnico giuridiche per evitare brutte sorprese",
URL: http://www.filodiritto.com/diritto/privato/informaticagiuridica/contrattooutsourcing.htm

Ugo Draetta, Nicoletta Parisi, "Contrattualistica telematica: norme e casi", Franco Angeli Editore, 2003

Valentina Freudiani, "Cosa è il contratto di outsourcing e come va disciplinato",
URL: http://www.consulentelegaleinformatico.it

Michele Iaselli, "Il contratto di outsourcing", URL: http://www.abconsul.it

Luigi Neirotti, "I contratti di outsourcing: modelli contrattuali ed aspetti rilevanti",
URL: http://www.informatica-juridica.com

F. Tosi, "Il contratto di outsourcing di sistema informatico", Giuffrè Editore, 2001

Ministero per i beni e le attività culturali, GdL outsourcing, "Il contratto di outsourcing archivistico: caratteristiche e requisiti",
URL: http://archivi.beniculturali.it/divisione_III/outsourcing/outsourcing_contratto.pdf

AAVV, "Clausole EU per il trasferimento di dati personali verso Paesi Terzi",
URL: http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

Julia Allen, Derek Gabbard, Christopher May, "Outsourcing Managed Security Services", Carnegie Mellon University, January 2003, CMU/SEI-SIM-012,
URL: http://www.sei.cmu.edu/publications/documents/sims/sim012.html

AAVV, "SLA for Applications Management Outsourcing Deals", Gartner Tutorial TU-14-2818, 25-10-2001

Ian S. Hayes, "Metrics for IT Outsourcing Service Level Agreements", Clarity Consulting 2004, URL: http://www.clarity-consulting.com/metrics_article.htm http://www.clarity-consulting.com/MetricsforITоutsourcing.pdf

Kathleen Goolsby, "A Guide for Establishing Service Level Specifications for Outsourcing Relationship", Everest Group, December 2001,
URL: http://www.themorleygroup.com/outsourcing%20service.pdf

Lukman Susanto, "SERVICE LEVEL AGREEMENT (SLA) in OUTSOURCING", and refs. cited, 2003, URL: http://www.susanto.id.au/papers/SLA.asp

Pascal De Zitter, "Service Level Management. (SLM). What does it represent? How do we do it? Introduction to Service Level Management", TALLIC, 04 April 2003, URL: http://www.itsmf.be/itsmfnewsite/events/2003/RTM11092003/documenten/TALLIC%20internal%20-%20Intro%202%20SLM%20presentation.pdf

AAVV, "ISO 9000 Introduction and Support Package: Guidance on 'Outsourced Processes'", ISO/TC 176/SC 2/N 630R2

AAVV, "Service Level Agreements (SLAs) and Operating Level Agreements (OLAs)" - Duke University Office Information Technology,
URL: http://www.oit.duke.edu/oit/sla/ and documents therein

Rudy Bakalov, "Risk Management Strategies for Offshore Application and Systems Development", Information Systems Control Journal Vol. 5, 2004

Rudy Bakalov and Feisal Nanji, "Offshore Application Development Done Right", Information Systems Control Journal Vol. 5, 2005

Nicholas A. Benevenuto and David Brand, "Outsourcing - A Risk Management Perspective", Information Systems Control Journal Vol. 5, 2005

Orang Twofigh and Tom Wong, "Views of Outsourcing - a Canadian Perspective", Information Systems Control Journal Vol. 5, 2005

AIPA, "Manuale sui livelli di servizio nel settore ICT", Quaderni dell'Autorità per l'Informatica nella Pubblica Amministrazione, volume 7, gennaio 2002

Ongetta, Molteni e altri - Club sul Computer Crime, "Outsourcing: organizzazione e sicurezza", IPACRI, 1993

Ongetta, Molteni e altri - Club sul Computer Crime, "Oursourcing: livelli di servizio e sicurezza", IPACRI, 1994

Via Valla, 16 20141 MILANO
Tel +39 02 8474.2365 Fax +39 02 700.507.644
aiea@aiea.it www.aiea.it

Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO
Tel +39 347 231.9285 Fax +39 02 700.440.496
info@clusit.it www.clusit.it