Il controllo sugli outsourcer dei sistemi informativi

Stefano Tezzon
Responsabile servizio organizzazione e sistemi informativi

stefano.tezzon@creditosportivo.it

ICS ISTITUTO PER IL CREDITO SPORTIVO

1) Framework regolamentare in tema di outsourcing

Cosa è veramente cambiato rispetto a prima....è solo una questione di principi?

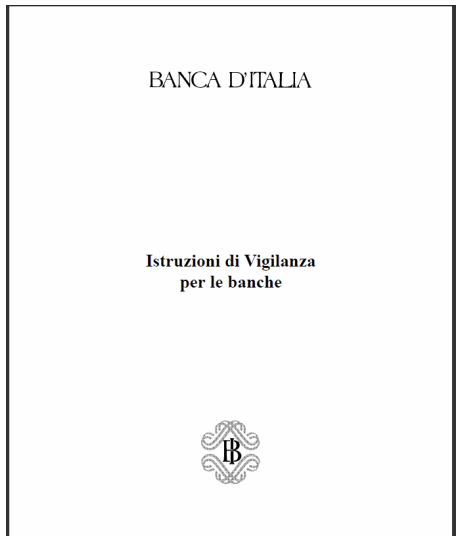
2) l'Intermediario e l'outsourcer

Come vivere il rapporto tra le due entità, tra business partnership e modelli di controllo

3) Conclusioni

L'outsourcing, tra sfide e opportunità… c'è la faremo?

1) Framework regolamentare in tema di outsourcing



titolo IV – vigilanza regolamentare

Capitolo 11 – sistema dei controlli interni, compiti del collegio sindacale

Sezione 2 – sistema dei controlli interni

Par. 4 – sistemi informativi

Già nel 1999 (circ.229) Bankit stabiliva un importante principio in tema di outsourcing

L'attribuzione a soggetti terzi di attività connesse con il funzionamento dei sistemi informativi non esonera le banche dalla responsabilità di controllo

Nel 2013, con il 15° aggiornamento della circolare 263/06

L'esternalizzazione di funzioni aziendali (*titolo V, Capitolo 7, Sezione IV)*

L'esternalizzazione del sistema informativo (*titolo V, Capitolo 8, Sezione VI)*

1) Framework regolamentare in tema di outsourcing

Il quadro normativo si complica ma, quel principio, rimane sempre valido

Le banche che ricorrono all'esternalizzazione di funzioni aziendali **presidiano i rischi** derivanti dalle scelte effettuate e mantengono la **capacità di controllo** e la **responsabilità** sulle attività esternalizzate nonché le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento

Evviva il principio di proporzionalità

A quel principio si aggiungono tante componenti che, nel loro insieme, ne dovrebbero garantire l'ottemperanza...*se ben strutturate*

1 - la valutazione dei rischi

Vado in outosurcing perché? Ho considerato i rischi operativi, di compliance, stategici, reputazionali, criticità dell'operatività esternalizzata, perdita di controllo su componenti del sistema informativo? Ho seguito un processo decisionale adeguato? Ho valutato i fornitori? È una scelta coerente con il RAF?

2 - il contratto

Livelli di servizio attesi, policy di sicurezza adeguate e allineate, proprietà dei dati, BC e DR, accountability, way out.

3 - la business partnership e le modalità di controllo

Gestione dell'audit, assurance esterne e certificazioni, modalità rilascio release, comitati tecnici e master plan, gestione anomalie

4 - la continuità operativa e le *exit strategies*

2) l'intermediario e l'outsourcer

Il contratto - Cosa non deve mancare

- Livelli di servizio attesi (oggettività e misurabilità)
- Modalità di controllo sul loro rispetto
- Durata del contratto
- Penali
- Modalità di revisione contrattuale prima della scadenza
- Recesso e modalità di uscita
- Livelli di servizio in emergenza e continuità operativa (procedure e flussi info)
- Partecipazione consortile (comitati tecnici, master plan, svolgimento audit)
- proprietà dei dati e loro disponibilità
- Sub esternalizzazioni
- Policy di sicurezza e tutela dei dati

2) l'intermediario e l'outsourcer

Fissiamo i punti oggetto di attenzione

- condizioni finanziarie outosurcer
- posizionamento sul mercato
- qualità e turnover del personale
- capacità di gestione della continuità operativa
- report direzionali sull'attività svolta
- competenza ed esperienza
- qualità e sicurezza
- economicità
- qualità sub fornitori
- affidabilità e scalabilità delle tecnologie
- qualità del reporting e dei flussi informativi
- ridondanze comunicative
- accountability

E creiamo una modello di controllo diviso per macroaree

Business partnership	- condizioni economiche - posizionamento sul mercato - capacità di investimento - qualità e turnover del personale - capacità di implementazione - flessibilità dell'outsourcer
SCI outosurcer	- certificazioni - modalità di conduzione di audit - accountability - segregation of duty - sistama monitoraggio SLA - sistema monitoraggio implementazioni - controlli di linea, II° e III° liv. - test rilascio release

2) l'intermediario e l'outsourcer

Fissiamo i punti oggetto di attenzione

- condizioni finanziarie outosurcer
- posizionamento sul mercato
- qualità e turnover del personale
- capacità di gestione della continuità operativa
- report direzionali sull'attività svolta
- competenza ed esperienza
- qualità e sicurezza
- economicità
- qualità sub fornitori
- affidabilità e scalabilità delle tecnologie
- qualità del reporting e dei flussi informativi
- ridondanze comunicative
- accountability

E creiamo una modello di controllo diviso per macroaree

Flussi informativi	- report delle strutture di controllo dell'outsourcer e dell'external auditor - master plan / portafoglio progetti - comitati tecnici - comitato information system audit - modalità di rilascio e contenuto delle release - richieste e rilascio di implementazioni
Sicurezza	- business continuity - disaster recovery - SLA (tempistiche manutenzione correttiva, tempistiche di ripresa servizio ecc.) - policy - data quality/data governance

2) l'intermediario e l'outsourcer

monitoraggio

Controller outsourcer

Risk appetite framework

Risk IT response

Exit strategies

Business partnership

Flussi informativi

Modello di controllo

SCI outsourcer

Sicurezza

Leve contrattuali

Vendor manager

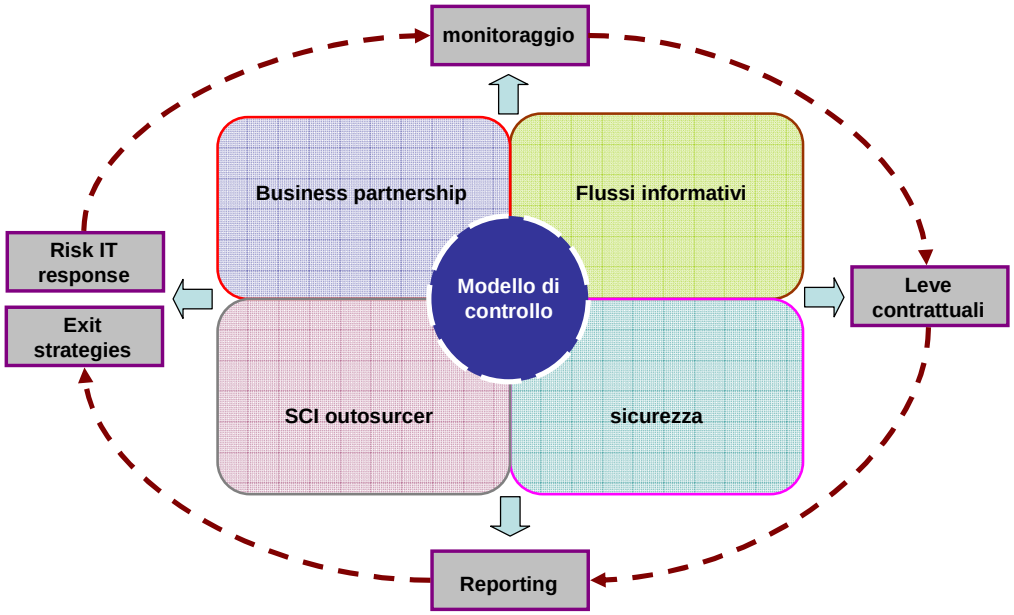
Reporting

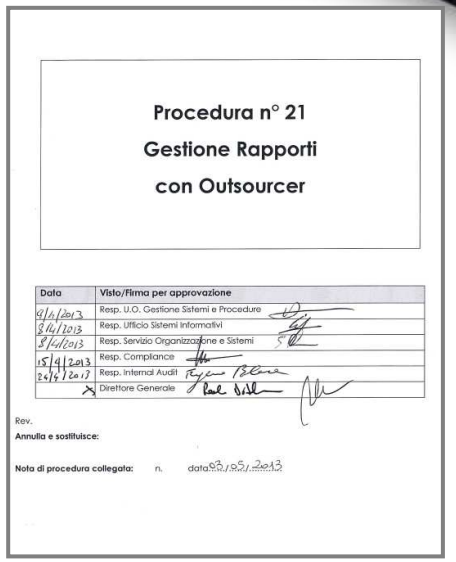
Organi di governo societario

Funzioni aziendali di controllo

Strutture aziendali e owner di processo

2) l'intermediario e l'outsourcer

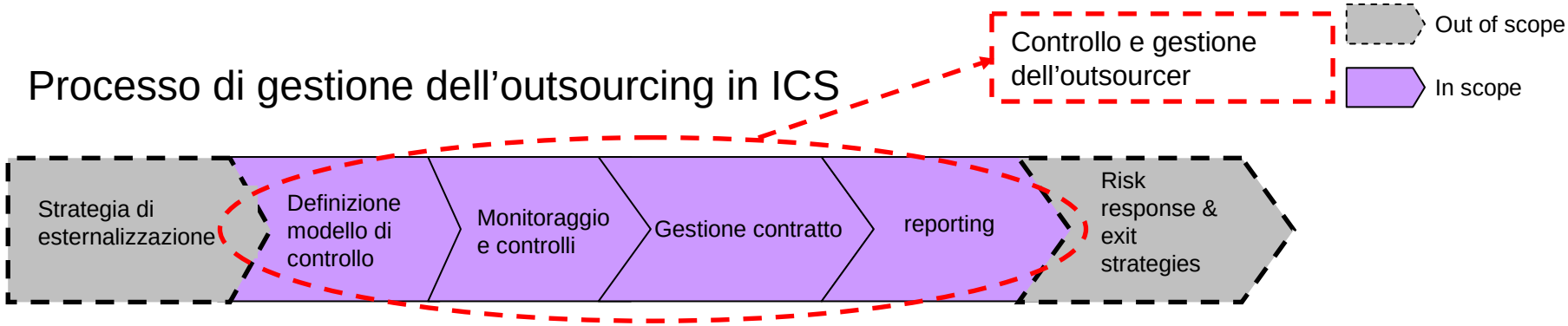



Procedura n° 21
Gestione Rapporti
con Outsourcer

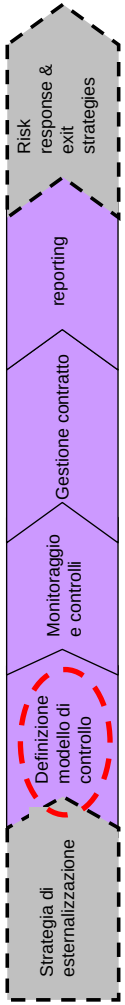
Data	Visto/Firma per approvazione
9/1/2013	Resp. U.O. Gestione Sistemi e Procedure
8/1/2013	Resp. Ufficio Sistemi Informativi
8/1/2013	Resp. Servizio Organizzazione e Sistemi
15/1/2013	Resp. Compliance
24/1/2013	Resp. Internal Audit
	Direttore Generale

Rev.
Annulla e sostituisce:
Nota di procedura collegata: n. data 02/05/2013

Processo di gestione dell'outsourcing in ICS



2) l'intermediario e l'outsourcer

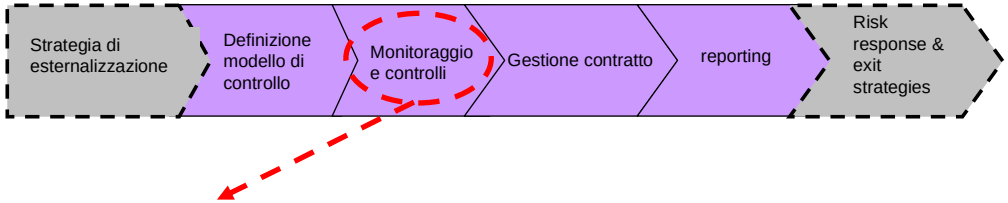


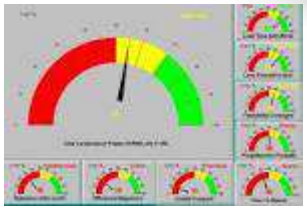
Struttura della procedura di gestione dell'outsourcer

Macro Area	Area	Oggetto del controllo
Business partnership	A1	Condizioni patrimoniali, economiche e finanziarie
	A2	Governance aziendale o di gruppo
	A3	Portafoglio progetti e piano degli investimenti
	A4	Portafoglio prodotti e servizi
	A5	Parco clienti
	A6	Modello organizzativo
	A7	Modello infrastrutturale
	A8	Project management e flessibilità
	A9	Modalità di interazione (numero e qualità dei comitati tecnici, workshop ecc.)
	A10	Economicità di servizio
SCI outsourcer	B1	Il controllo sull'outsourcer per mezzo dell'auditor indipendente
	B2	Report di audit interni
	B3	Audit condotti da ICS
	B4	Gestione rapporti mensili (SLA su performance di sistema, assistenza ed help desk, rilascio implementazioni)

Macro Area	Area	Oggetto del controllo
Flussi informativi	C1	Gestione richieste di nuove applicazioni
	C2	Gestione richieste di ampliamento delle funzionalità
	C3	Gestione richieste da parte strutture owner di processo
	C4	Gestione rilascio release
Sicurezza	D1	Business continuity
	D2	Disaster recovery
	D3	SLA su tempi di manutenzione correttiva, ripresa di servizio ecc:
	D4	Policy
	D5	Data quality e data governance

2) l'intermediario e l'outsourcer





Cruscotti e KPI monitoring

Performance di sistema

- ❑ disponibilità del servizio on line
- ❑ tempo di risposta delle principali transazioni
- ❑ timing batch (mensili, giornalieri ecc.)

→ **11 KPI**

Assistenza ed help desk

- ❑ tempistiche di presa in carico delle richieste
- ❑ tempistiche di risoluzione delle problematiche

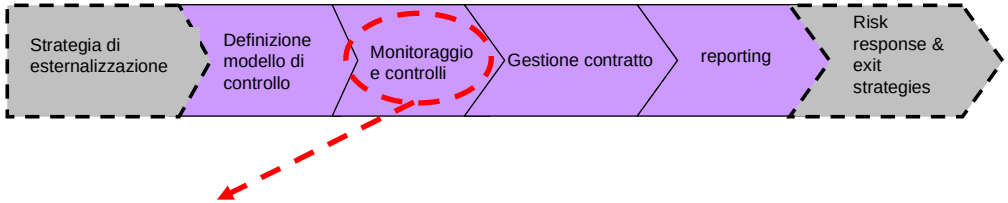
→ **3 KPI**

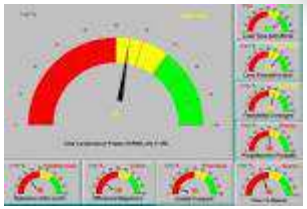
Personalizzazioni applicative e funzionali

- ❑ tempistiche per analisi funzionali e quotazione economica
- ❑ tempistiche di rilascio implementazioni

→ **6 KPI**

2) l'intermediario e l'outsourcer

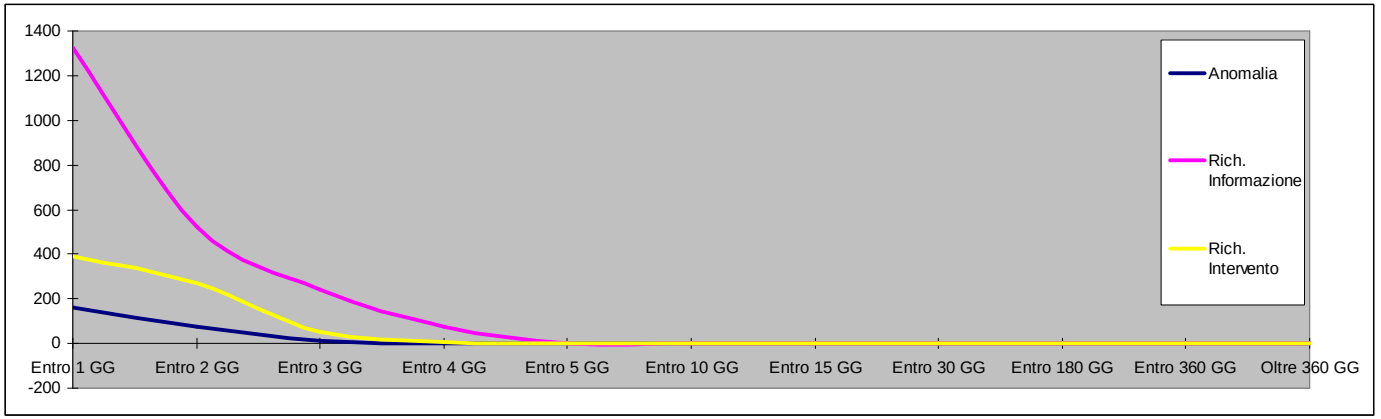




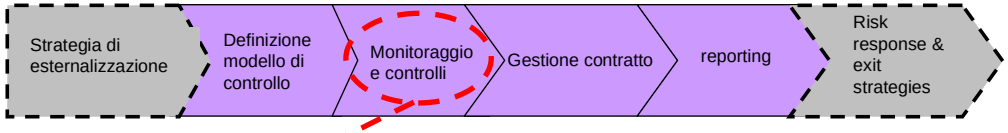
Cruscotti e KPI monitoring

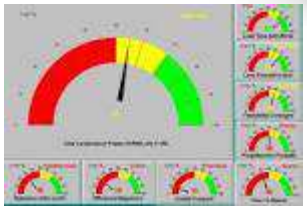
Dal: 01-01-20xx	Al: 31-12-20xx												
Tipo		**Entro 1 GG**	**Entro 2 GG**	**Entro 3 GG**	**Entro 4 GG**	**Entro 5 GG**	**Entro 10 GG**	**Entro 15 GG**	**Entro 30 GG**	**Entro 180 GG**	**Entro 365 GG**	**Oltre 365 GG**	**Totale**
Anomalia	num	161	78	13	1	0	0	0	0	0	0	0	**253**
	%	63,64%	30,83%	5,14%	0,40%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**100,00%**
Rich. Informazione	num	993	1106	243	76	3	0	0	0	0	0	0	**2421**
	%	41,02%	45,68%	10,04%	3,14%	0,12%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**100,00%**
Rich. Intervento	num	389	270	188	146	121	98	125	32	0	0	0	**1369**
	%	28,41%	19,72%	13,73%	10,66%	8,84%	7,16%	9,13%	2,34%	0,00%	0,00%	0,00%	**100,00%**

Assistenza ed help desk



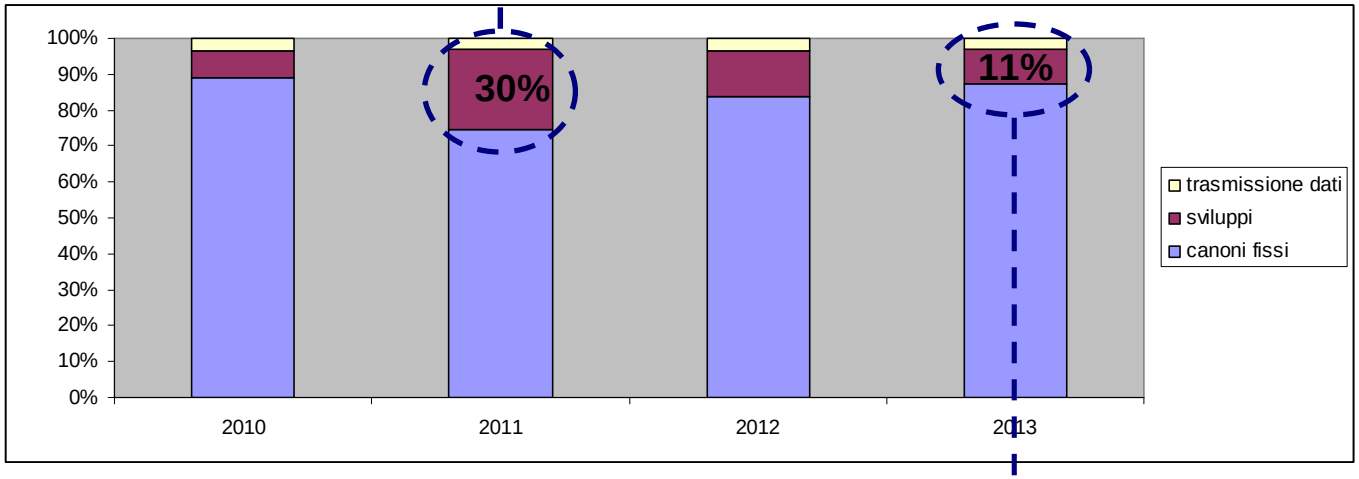
2) l'intermediario e l'outsourcer

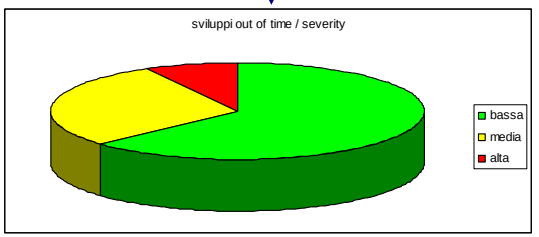


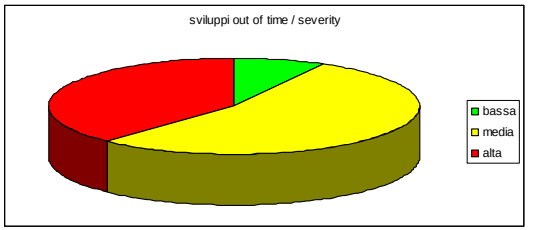


Personalizzazioni applicative e funzionali

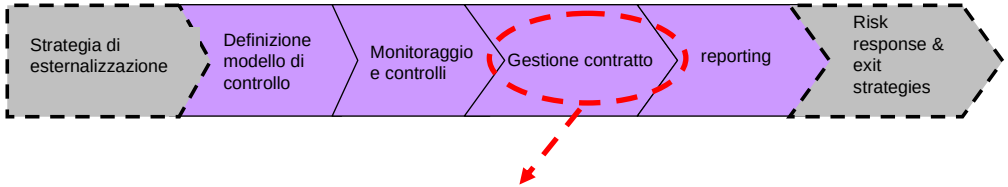
cruscotto costi e sviluppi											
anno	num.	sviluppi	importo medio	tempi medi di quotazione	tempi medi di realizzo	sviluppi in time	sviluppi out of time / severity			canoni fissi	trasmissione dati
							bassa	*media*	*alta*		
T0											
T1											
T2											
Tn											







2) l'intermediario e l'outsourcer



LIVELLO ANOMALIA / DISFUNZIONE	LINEA D'AZIONE	SOGGETTO / ORGANO DELEGATO
Livello 1	Percorsi di rimedio ad hoc (ad esclusione di quelli gestibili mediante gli strumenti ordinari)	- Controller outsourcer - Vendor Manager (se incidono sul budget)
Livello 2	Lettera di diffida (non comportante effetti economici)	Vendor manager
Livello 3	Lettera di diffida (comportante effetti economici)	Direzione generale
Livello 4	Applicazione di penali	Direzione generale

2) l'intermediario e l'outsourcer

STRUTTURA DELLA PROCEDURA DI GESTIONE DELL'OUTSOURCER					
Macro Area	**Area**	**Oggetto del controllo**	**Valutazione area - *Vi* (o)**	**Peso area - *Pi***	**Score area – *Vi (o)*Pi***
Business partnership	A1				
	A2				
	…				
	…				

$$S(o) = \frac{\sum_{i=1}^{n} p_i v_i(o)}{\sum_{i=1}^{n} p_i}$$

dove:
Vi (o) = valore area i-esima
n = numero aree
Pi = peso area i-esima
S(o) = punteggio finale

Valutazione area - *Vi* (o)	Inadeguato			
	Parzialmente adeguato			
	Adeguato			
	Più che adeguato			
Peso area – *Pi*	Da 1 a 3			
S(o)	Da 1,00 a 4,00			
	1,00-1,75	1,76-2,50	2,51-3,26	3,27-4,00
	inadeguato	**Parzialmente adeguato**	**adeguato**	**Più che adeguato**

3) conclusioni

- il fenomeno vendor lock-in

- il rapporto di outsourcing quale business partnership e l'importanza del ruolo degli IT Manager