

Le strategie preventive

■ RISK ASSESSMENT

Risk Identification. Si cerca di individuare tutti i potenziali rischi insiti in un servizio di SAP application management in offshore per tutta la durata del contratto attraverso discussioni di gruppo, questionari, check-list, esame di esperienze passate simili, formalizzazione dei vincoli/opportunità del servizio.

Risk Analysis. Per ogni rischio identificato, vanno analizzate le probabilità di accadimento e gli effetti dello stesso in termini di gravità corrispondenti al mancato o mutato conseguimento delle prestazioni del servizio di SAP application management come definito nel contratto di outsourcing. Si cercherà il più possibile di tradurre il rischio in termini di costi che, moltiplicati per la probabilità, esprimono una valutazione quantitativa e relativa del rischio.

Risk Quotation. Sulla base dell'analisi precedente viene redatta una scala delle priorità di rischio e quindi di intervento; viene anche definito un limite massimo accettabile, che obbliga a ricondurre tutti i rischi con valore superiore entro tale limite con appropriate azioni. È importante che il processo di ordinamento dei rischi sia esplicito e condiviso, anche con una visualizzazione tipo "diagramma radar" (sui raggi i singoli rischi e i livelli di rischio come cerchi concentrici).

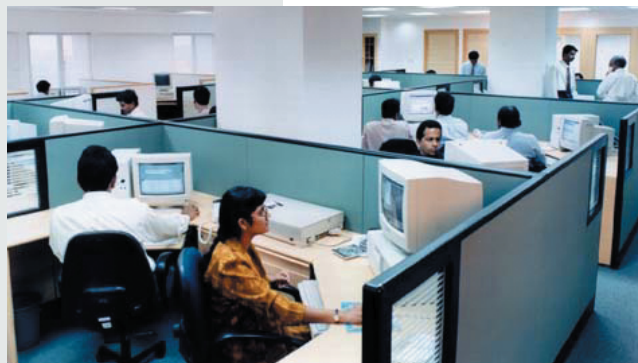
■ PIANI RMMM

Risk Mitigation (Riduzione dei rischi). Azioni che aiutano a ridurre la probabilità che i rischi presi in considerazione si verifichino. Gli interventi possono anche avere effetti sinergici tra di loro, e dopo la loro applicazione, ogni rischio deve essere ricalcolato (rischio residuo).

Risk Monitoring (Sorveglianza dei rischi). Questi piani aiutano a riconoscere tempestivamente i primi effetti sulla continuità del servizio di rischi che si stanno per verificare. Spesso, il solo fatto di

dedicare una costante attenzione al manifestarsi dei rischi consente di contenere eventuali rischi. È anche importante tenere sotto controllo l'efficacia delle misure prese.

Risk Management (o contingency plan). I piani di gestione dei rischi aiutano a ridurre la gravità degli effetti se i rischi si sono purtroppo concretizzati. Lo stesso piano RMMM dovrà essere ricontrattato mano a mano che il servizio viene erogato per assicurarsi che i rischi siano sempre sotto controllo e lo stesso piano sia realistico.



I rischi dell'offshore della gestione di SAP

E tutte le strategie per evitarli o mitigarne i danni, prima di decidere di sostituire il fornitore locale

prosegue da pagina 1

Quando i fornitori dei servizi di business process outsourcing, di application management o di sviluppo software hanno parte dell'organizzazione collocata in qualche 'low cost country' (India, Ucraina, Bielorussia, ecc), a prescindere dal modello organizzativo adottato (global delivery, hybrid delivery, global shared

service, build-operate-transfer, hub-and-spoke), è strategico entrare nel merito dei rischi possibili, pena l'insuccesso dell'iniziativa nel medio periodo, se non, a volte, nel breve. Anche attraverso un'analisi delle best practice che hanno permesso una continuità e qualità degli stessi in archi temporali molto lunghi. Infatti i progetti con un forte accento sulla gestione del rischio relativo presentano risultati migliori nel lungo periodo, anche se a budget si dovranno considerare nel breve i costi di implementazione di un sistema organizzativo ad-hoc per realizzare le attese dei piani RMMM (Risk Mitigation, Monitoring and Management).

APPLICATION MANAGEMENT

Si può riassumere la nozione di 'rischio' in 'problema potenziale': può verificarsi, ma anche non verificarsi. Indipendentemente dal risultato, è opportuno identificarlo, stabilire la probabilità che si verifichi, stimare il suo impatto

e stabilire un piano di contingenza nel caso il problema si dovesse verificarsi. Occorre quindi innanzitutto definire che cosa può andare storto durante un lungo periodo di erogazione di servizi.

Individuati i rischi, ognuno va analizzato per determinare la probabilità che si verifichi e i danni che eventualmente provocherà. Ottenute queste informazioni, i rischi possono quindi essere valutati in base alla probabilità e all'impatto sull'erogazione dei servizi di application manage-

Tutti i potenziali problemi in dettaglio

1 RISCHIO GEOPOLITICO

È l'insieme dei rischi relativi al ricevere servizi di SAP application management da aziende in Paesi instabili. Per esempio: agitazione ai confini del Paese, rivolte religiose, processi politici, burocrazia, politiche governative (tasse, dazi, leggi di regolazione commerci), relazioni tra i Paesi, guerre, terrorismo. Esempio: le tensioni tra India/Pakistan, e quelle medio-orientali.

2 RISCHIO PAESE

È il rischio associati al singolo Paese - supporto governativo ai servizi in offshore, stabilità politica, caratteristiche del bacino occupazionale, infrastrutture, sistema educativo, qualità dei processi, compatibilità culturale, sistema legale in essere, atteggiamento verso la globalizzazione. Per esempio alcuni rischi Paese della Russia sono la lingua, il supporto governativo, le infrastrutture, la fuga dei cervelli, la corruzione nella burocrazia, la credibilità.

3 RISCHIO SOCIO-ECONOMICO

È quello associato alla situazione socio-economica del Paese dove devono essere erogati

i servizi per il cliente e di quello in cui è localizzato il fornitore offshore. La significativa perdita di posti di lavoro tra i 'colletti bianchi' delle attività di back office, contact center, programmatori, personale amministrativo può causare conseguenze politiche sociali e societarie. Per esempio: la riduzione o il rallentamento dei tempi per l'emissione dei visti di ingresso di personale extracomunitario, le cause legali (Microsoft,...).

4 RISCHIO CULTURALE

È l'insieme dei rischi collegati alle caratteristiche nazionali legate alla diversa espressività, abitudini, reazioni fisiche come al diverso comportamento aziendale. Persone di diverse culture spesso non pensano alla stessa maniera o si capiscono tra di loro. Esempio: le differenze tra indiani e americani riguardo le apparenze esterne, la credibilità, il rispetto delle gerarchie, la propensione al rischio, il processo di delega, la comunicazione delle cattive notizie e la propensione verso la comunicazione diretta o indiretta; la diversità sui concetti di tempo speso, della puntualità, dell'amicizia, dell'individualismo, della propensione alla crescita professionale di

breve e lunga durata; e poi dei concetti di spazio, di possesso di beni materiali, di processo personale per il raggiungimento di un accordo, di atteggiamento nei confronti di critiche, di solidarietà.

5 RISCHIO LINGUISTICO

Deriva dal diverso livello nell'inglese scritto/parlato e dal diverso livello di comprensione tra persone di lingua madre inglese e altre lingue. Incomprensioni linguistiche giornaliere dovute ai diversi fusi orari, e incomprensioni per l'appartenenza a diverse culture. Perdita di completezza dell'informazione per utilizzo di vari strumenti di comunicazione. Per esempio, abbiamo bisogno di fissare un appuntamento martedì, e la conversazione potrebbe diventare la seguente. Martedì? Sì, martedì, puoi partecipare? Sai che è il compleanno di mio figlio? Ah Bene! Grazie della comprensione.

6 RISCHIO CAPITALE UMANO

Riguarda il capitale umano presente sia presso il cliente sia presso il fornitore che nei rispettivi mercati del lavoro nazionali: sono stati trovati i professionisti desiderati? Il fornitore ha un elevato turnover di personale? Si perde know-how quando le risorse sono spostate da onshore a

offshore? C'è "fuga di cervelli" ("brain drain") nel Paese? Per esempio: come confrontare un curriculum di un laureato in informatica di Torino e quello di un laureato del Birla Institute of Technology di Hyderabad (India)?

7 RISCHIO INFRASTRUTTURE

Si tratta di rischi relativi sia alle infrastrutture dei Paesi dove devono essere erogati i servizi per il cliente sia a quelle del Paese dove il fornitore offshore è presente. Pochi Paesi dove sono localizzati fornitori che forniscono servizi in offshore o dove saranno presenti i siti del cliente hanno infrastrutture equivalenti a quelle americane o europee (rete elettrica, acqua, rete di telecomunicazione, trasporti). Per esempio, frequenti e lunghi blackout nelle Filippine; l'India ha un'insufficiente rete internazionale di comunicazione.

8 RISCHIO BUSINESS CONTINUITY

Deriva dalle interruzioni di servizio o dalla riduzione della sua qualità sui processi business operativi critici e giornalieri nell'eventualità di un 'disastro': blackout elettrico, disastro naturale, inondazione, epidemia, attacco informatico con virus, sabotaggio, terrorismo, guerra. Per esempio: monsoni in Asia, cicloni, inondazioni su uno o più siti.

ment. Infine è possibile sviluppare un piano per gestire i rischi che hanno maggiore probabilità di verificarsi, o un maggiore impatto, producendo un piano RMMM (Risk Mitigation, Monitoring and Management).

I rischi dell'outsourcing offshore dell'application management di applicazioni SAP possono essere classificati innanzitutto in rischi noti, prevedibili e imprevedibili. I rischi noti sono quelli che possono essere scoperti dopo un attento esame del modello di erogazione dei servizi di SAP application management e dell'ambiente aziendale e tecnico da cui il fornitore erogherà il servizio.

I rischi prevedibili possono essere dedotti dall'esperienza, mentre quelli imprevedibili sono assai difficili da individuare in anticipo.

Si può anche distinguere tra rischi generici, cioè rischi comuni a qualsiasi servizio di outsourcing, e rischi specifici

dell'outsourcing di SAP application management e legati all'utilizzo di specifici modelli di erogazione di servizi IT con strutture remote offshore. I rischi possono essere distinti anche tra rischi legati al Paese, rischi legati al modello di global delivery e rischi specifici del modello di business del fornitore. Nel riquadro sotto vengono descritti in dettaglio i rischi specifici dell'utilizzo di strutture di offshore per l'application management di SAP.

Le strategie di gestione del rischio

È bene concentrarsi sia sulle strategie di risk management reattive sia su quelle preventive. Un'ottima strategia reattiva, al verificarsi di un evento definito rischioso, è quella di sapere come attivarsi per limitarne gli effetti dannosi sull'erogazione del servizio, gestire la crisi, correggere gli errori e compensare gli effetti negativi che manifestano. Ma è molto importante anche una strategia preventiva: individuati i rischi potenziali, se ne valutano la probabilità e gli effetti, e si stabilisce un ordine di importanza. Siccome i fattori di rischio sono parte intrinseca e caratterizzante dei servizi di application management, l'approccio proattivo si

concretizza di fatto nella prevenzione, piuttosto che nell'eliminazione totale del rischio.

Insomma il team di offshore di un'azienda che ha deciso di utilizzare questi servizi deve organizzarsi per il piano di governo dei rischi con l'obiettivo primario di evitarli, ma poiché non tutti i rischi sono evitabili, deve anche predisporre un piano che permetta di reagire, in caso di necessità, in modo controllato ed efficace.

In definitiva sono tre i momenti fondamentali del processo di concretizzazione di un rischio: l'evento, il danno e le conseguenze finanziarie. E altrettante sono le strategie per fronteggiare questi momenti: la riduzione delle probabilità, la riduzione del danno e la riduzione delle conseguenze finanziarie. [cw]

Giovanni Mancini è CEO di Blackbirds, società di servizi IT italiana con centri di sviluppo in India e prossime aperture in Romania ed Emirati Arabi

Le strategie reattive

■ RIDUZIONE DELLE PROBABILITÀ

Risk Elusion (o elusione di un rischio) è l'eliminazione di un rischio per mezzo della rinuncia all'attività o alle operazioni che ne stanno all'origine. Questa strategia è spesso impedita dalle norme che regolano il contratto di erogazione servizi, perché equivarrebbe a rinunciare a erogare parte di servizio.

Prevenzione (risk assesment, risk mitigation) è l'insieme delle misure di sicurezza volte a impedire il prodursi di evenienze dannose. La prevenzione è in sostanza una riduzione della probabilità dell'evento a parità di impatto.

■ RIDUZIONE DEL DANNO

Protezione è un insieme di misure di sicurezza (crisis management, business recovery, disaster recovery, business resumption, security plan) volte a

minimizzare il danno di eventi indesiderati, da adottare quando la prevenzione fallisce. La protezione è dunque una riduzione della probabilità del danno a parità di probabilità.

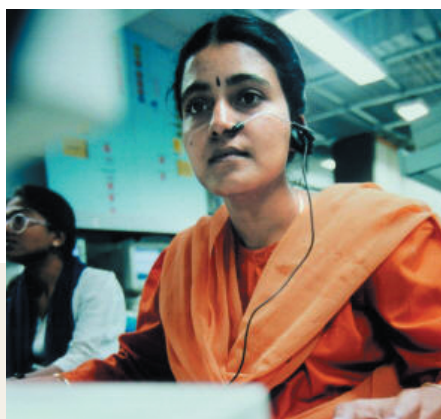
Risk Monitoring e Contingency Plan sono azioni da intraprendere partendo dall'analisi del rischio e delle sue conseguenze. In particolare un contingency plan implica la stesura preventiva di piani atti a fronteggiare eventi, danni e conseguenze finanziarie che possono verificarsi compromettendo la continuità e la qualità del servizio di SAP application management. La stesura di contingency plan è l'opposto della gestione per "emergenze" o "stati di crisi" ancora diffusa in molte aziende. Si tratta di pianificare in anticipo la gestione del "budget delle contingencies" e di sviluppare programmi temporali e di impiego delle risorse alternativi.

■ RIDUZIONE DELLE CONSEGUENZE FINANZIARIE

Assicurazione. Le conseguenze finanziarie dell'evento dannoso vengono trasferite all'assicuratore nei limiti e alle condizioni stabilite nella polizza, in cui viene fissato anche il premio pagato dall'assicurato.

Trasferimento non assicurativo è lo spostamento del rischio su soggetti diversi da una compagnia di assicurazione (altro contratto di subappalto per attività troppo rischiose se svolte da fornitore in offshore, contratti di noleggio operativo per l'hardware in housing presso il fornitore in offshore).

Ritenzione è l'assunzione da parte dell'azienda di una quota o della totalità del rischio. I danni relativi a tale quota sono sostenuti con mezzi finanziari interni. La ritenzione può essere assistita da una pianificazione finanziaria per la distribuzione nel tempo dell'onere delle perdite con effetti che si avvicinano a quelli offerti dalle assicurazioni. Non a caso la tecnica di ritenzione più evoluta mira proprio a riprodurre in casa il meccanismo assicurativo.



9 RISCHIO SICUREZZA E PRIVACY

È il rischio legato alla sicurezza sul capitale intellettuale e di infrastrutture fisiche - aspetti molto importanti nella gestione di progetti offshore. Molti sono i possibili rischi su questo fronte, che resta fuori del controllo del cliente e fuori dalla protezione legislativa di norme del Paese.

10 RISCHIO TRASFERIMENTO E GESTIONE CONOSCENZA

È il rischio legato al fatto che i contratti offshore riguardano grandi numeri di professionisti coinvolti su diverse zone del mondo senza nessuna conoscenza preventiva dei sistemi, della cultura d'impresa, del settore industriale. Per esempio: lo staff offshore non ha la corretta produttività per mancanza di conoscenza o ha un alto livello di turnover.

11 RISCHIO CHANGE MANAGEMENT

Questo rischio riguarda le organizzazioni del cliente e dei fornitori offshore. L'accettazione del cliente è

essenziale. Bisogna avere un piano effettivo per le transazioni, l'organizzazione, la comunicazione, la gestione e la nascita di nuovi processi organizzati per stabilire nuovi modelli organizzativi tra le parti coinvolte in un servizio in offshore. Esempio: alcune Business Unit del cliente rifiutano di utilizzare fornitori offshore e insistono ad utilizzare più professionisti localmente; impiegati preoccupati della sicurezza del loro posto di lavoro non partecipano propriamente ai processi di trasferimento conoscenza e/o di documentazione durante la fase critica di transazione.

12 RISCHIO SERVICE MANAGEMENT

È il rischio propriamente legato alla gestione dei servizi di application management in offshore. La gestione del servizio con i relativi service manager coinvolti influenzano la qualità, i costi, il rispetto dei parametri di qualità dei servizi definiti contrattualmente. Il bisogno di ottimi service manager aumenta con il disperdersi dei team di erogazione servizi.

13 RISCHIO SAP APPLICATION MANAGEMENT

Si tratta di un rischio legato al servizio di SAP application management che si è scelto di erogare da centri remoti in offshore e ai processi organizzativi coinvolti. Servizi con molte interazioni

tra i team del fornitore offshore e il cliente e con funzionalità poco chiare sulle modifiche software sono poco indicati per essere sviluppati in offshore. Esempio: i rischi della gestione di SAP R/3 sono diversi di quelli dell'application management di SAP Business Warehouse?

14 RISCHIO MODELLO ORGANIZZATIVO

È quello legato al determinato modello organizzativo scelto per erogare i servizi di SAP application management, considerando che i servizi possono essere erogati in parte o totalmente nelle sedi del cliente (onsite), in centri esterni negli stati nazionali delle sedi del cliente (offsite) e in un centro remoto dedicato alla erogazione dei servizi (offshore). Per esempio bisogna valutare quali rischi comporta avere team delocalizzati nel mondo; qual è la più idonea composizione dei team onsite/offshore; quali processi di application management sono più appropriati per essere erogati in offshore anziché onsite. E poi quali sono i rischi legati ai meccanismi di controllo e coordinamento dei vari team delocalizzati? Si perde il comportamento collaborativo e la fiducia se i team sono dispersi?

15 RISCHIO ANALISI FORNITORE

Instaurare una relazione di business con un fornitore non conosciuto precedentemente, estero,

che opera su un corpo di leggi diverso comporta dei rischi. Per esempio: quale può essere l'affidabilità a lungo termine di un fornitore di servizi IT di 1.000 professionisti localizzato a Minsk (Bielorussia)?

16 RISCHIO INFLAZIONE E PREZZI

Deriva dalle particolari congiunture economiche che si vengono a verificare nel corso di tutto il contratto di durata pluriennale o prezzi superiori alle attese o ai valori di contratto per motivi legati alle mutate condizioni al contorno dell'organizzazione cliente-fornitore. Esempio: prezzi che aumentano nel muovere persone/risorse onsite per scelte del management durante il contratto di servizi; un numero maggiore di utenti che si collega sul sistema SAP rispetto ai valori medi dichiarati al momento dell'acquisto della licenza SAP; spostamento su altro stabilimento di personale per far fronte ad attacco terroristico.

17 RISCHIO LEGALE

Questo rischio è legato a eventi esterni o a particolari condizioni che possono impedire l'erogazione del servizio come contrattualizzato secondo una legislazione diversa da quella italiana. Esempio: dopo un sabotaggio terroristico, come viene applicata la causa di forza maggiore per regolare le attività e come un giudice obbliga una parte a ripristinare i servizi.