



# **L'OUTSOURCING IT: BEST PRACTICE E AUDITING**

## **L'esecuzione dell'audit – Gli strumenti: le checklist**

*Alessandro Dellepiane, CISA, CIA  
UniCredit Audit SpA*



## **Gli strumenti: le checklist di controllo**

- opportuno approntare alcuni strumenti utilizzabili dall'auditor per effettuare verifiche a fronte delle principali categorie di rischi prese in considerazione
- presi come riferimento quelli (checklist) già proposti nel Gruppo di Ricerca AIEA "L'Auditing ISO17799/BS7799", in quanto tali checklist sono risultate efficaci

## Guida per la compilazione delle checklist

Ci sono due domande base che potrebbero riguardare ciascun requisito di controllo.

**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.

LA GOVERNANCE				
argomento	Controlli sui punti qualificanti generativi dell'outsourcing e sul governo del contratto			
OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggestimenti
	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?				

LA GOVERNANCE					
argomento	Controlli sui punti qualificanti generativi dell'outsourcing e sul governo del contratto				
OBIETTIVI DI CONTROLLO	Q1			Q2:	Rischi & Suggestimenti
	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.)?					

LA GOVERNANCE					
argomento		Controlli sui punti qualificanti generativi dell'outsourcing e sul governo del contratto			
OBIETTIVI DI CONTROLLO	Q1			Q2:	Rischi & Suggestimenti
	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)?					
Sono state specificate le misure di sicurezza relativamente ai dati ed alle modalità di accesso ai dati (incluse le modalità di accesso da remoto)?					



GLI SLA E IL LORO MONITORAGGIO					
Argomento		Controlli sul processo di identificazione dei servizi oggetto di outsourcing			
OBIETTIVI DI CONTROLLO	Q1			Q2:	Rischi & Suggestimenti
	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)?					
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?					

IL CONTRATTO E LA PARTE LEGALE					
argomento		Definizione dei Service Level Agreement			
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 raggiungimento delle stesse?					
Sono stati previsti i seguenti requisiti di qualità? <ul style="list-style-type: none"> <li>• Durata delle operazioni batch,</li> <li>• Puntualità dell'apertura dei servizi on-line,</li> <li>• Integrità e correttezza formale dei supporti contenenti gli output prodotti,</li> <li>• Tempo di risposta ai malfunzionamenti,</li> <li>• Tempo di intervento e di ripristino,</li> <li>• Tempestività di risposta on-line,</li> <li>• Disponibilità.</li> </ul>					
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?					
È stata prevista, a scadenze prefissate (p.es. annuali), una verifica della qualità e delle modalità di erogazione dei servizi?					

LA SICUREZZA				
argomento	Gestione della Sicurezza			
OBIETTIVI DI CONTROLLO	Q1			Q2: Rischi & Suggestimenti
	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? <i>(Considerare le modalità e la periodicità con cui il cliente viene informato o ha la possibilità di conoscere le autorizzazioni di accesso alla sistema)</i>				
Il cliente viene informato di eventuali incidenti e delle azioni di gestione e risoluzione poste in essere dall'outsourcer? <i>(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)</i>				
La sicurezza della rete del cliente viene monitorata? <i>(Considerare modalità e periodicità)</i>				
Vengono effettuati dei vulnerability assessment periodici e il risultato viene comunicato al cliente? <i>(Considerare modalità e periodicità)</i>				