

Il Sistema di Controllo Interno

Indice del contenuto

1. Definizione e Componenti

- Definizione del Controllo Interno
- Che cosa ci si può attendere dal Controllo Interno
- Che cosa non ci si può attendere dal Controllo Interno
- Componenti del Controllo Interno
- Ruoli e responsabilità
- Efficacia

2. Ambiente di controllo

- Fattori dell'ambiente di controllo
- Integrità e valori etici
- Differenze e relative conseguenze
- Applicazione alle piccole e medie aziende
- Valutazione

3. Valutazione dei rischi

- Obiettivi
- Rischi
- Gestione del cambiamento
- Piccole e medie aziende
- Valutazione

4. Attività di controllo

- Tipologia delle attività di controllo
- Integrazione delle attività di controllo con la valutazione dei rischi
- Controlli sui sistemi informativi
- Controlli peculiari alla specifica azienda
- Valutazione

5. Informazioni e comunicazione

- Informazioni
- Comunicazione
- Applicazione alle piccole e medie aziende
- Valutazione

6. Monitoraggio

- Attività di monitoraggio continuo
- Valutazioni specifiche
- Rapporti sulle disfunzioni
- Applicazione alle piccole e medie aziende
- Valutazione

7. Limiti del Controllo Interno

- Giudizio
- Disfunzioni
- Deroghe dei dirigenti
- Collusione
- Rapporto costi-benefici

8. Ruoli e responsabilità

- Persone e organi responsabili
- Consiglio di Amministrazione
- Terzi

Il Sistema di Controllo Interno

Attività di controllo

Le attività di controllo si possono definire come l'applicazione delle politiche e delle procedure che garantiscono al management che le sue direttive siano attuate.

Esse assicurano l'adozione dei provvedimenti, necessari per far fronte ai rischi che potrebbero pregiudicare la realizzazione degli obiettivi aziendali.

Le attività di controllo si attuano in tutti i livelli gerarchici e funzionali della struttura organizzativa.

Tali attività includono un insieme d'attività diverse, come approvazioni, autorizzazioni, verifiche, raffronti, esame della performance operativa, protezione dei beni aziendali e separazione dei compiti.

Le attività di controllo sono l'applicazione delle politiche e delle procedure, ovvero le azioni svolte dalle persone per realizzare le politiche, destinate ad assicurare l'attuazione delle direttive emesse dal management per la gestione dei rischi.

Le attività di controllo si possono suddividere in tre categorie in base agli obiettivi generali dell'azienda: attività di controllo relative agli aspetti operativi, attività di controllo sulle informazioni di bilancio e attività di controllo sul rispetto dei vincoli legali e regolamentari.

I controlli possono riguardare specificatamente un'area o, come spesso accade, più aree. In effetti, secondo le circostanze, una data attività di controllo può contribuire alla realizzazione di obiettivi comuni a più categorie.

Così, le attività di controllo relative all'area operativa possono anche contribuire ad assicurare l'affidabilità delle informazioni di bilancio, i controlli sulle informazioni di bilancio possono contribuire al rispetto dei vincoli normativi e così via.

Per esempio, il direttore commerciale di un centro di distribuzione di parti di ricambio riceve giornalmente dei rapporti informativi sintetici dai capifiliale. Siccome il direttore commerciale raffronta i rapporti ricevuti con le vendite e con le provvigioni contabilizzate, questo controllo consente di soddisfare sia gli obiettivi dell'area operativa sia quelli relativi alle informazioni di bilancio.

In un'attività di commercio al dettaglio, le note di credito emesse per merce resa dai clienti sono controllate numerando sequenzialmente i documenti e riepilogando gli stessi in vista della contabilizzazione e quindi della predisposizione dei bilanci. Questo riepilogo fornisce anche un'analisi per prodotto, utilizzata dal responsabile degli acquisti per decidere sui futuri approvvigionamenti e per il controllo delle scorte.

In tal modo, le attività di controllo, essenzialmente connesse all'elaborazione delle informazioni di bilancio, hanno fornito un importante contributo alla realizzazione di obiettivi connessi con l'operatività aziendale.

Sebbene queste categorie siano utili per studiare il sistema di Controllo Interno, la particolare categoria nella quale un controllo può essere classificato non è tanto importante quanto il ruolo

che il controllo stesso assume per il raggiungimento di determinati obiettivi aziendali.

Tipologia delle attività di controllo

Sono stati descritti diversi tipi di controllo, come per esempio: controlli preventivi, investigativi, manuali, informatici, di gestione. Le attività di controllo possono essere classificate in funzione di obiettivi specifici, come quello di assicurare la completezza e l'accuratezza dell'elaborazione dei dati.

Qui si espongono alcune attività di controllo, ordinariamente svolte dal personale a vari livelli organizzativi. Tale descrizione viene fatta al fine di illustrare la varietà delle attività di controllo, senza suggerire alcuna particolare suddivisione in categorie.

- **Analisi svolte dall'alta direzione.** Le performance realizzate sono analizzate raffrontandole con i budget, con le proiezioni, con i risultati dei periodi precedenti e con i risultati dei concorrenti. Si esamina l'andamento delle principali iniziative adottate (come campagne di marketing, miglioramenti di processi produttivi, programmi di contenimento o di riduzione dei costi) per determinare in che misura gli obiettivi siano stati conseguiti. Si supervisiona la realizzazione dei piani per lo sviluppo di nuovi prodotti, di joint-venture o di finanziamenti. Le azioni intraprese dal management per analizzare e seguire questi componenti costituiscono attività di controllo.
- **Gestione delle attività o delle funzioni.** Tutti i responsabili di funzioni o attività procedono all'analisi delle performance. Per esempio, in una banca un manager responsabile dei prestiti personali analizza i rapporti elaborati per filiale, per regione e per tipo di prestito (incluse le garanzie), controlla le sintesi, identifica le tendenze, raffrontando i risultati ottenuti con le statistiche economiche e con i target. A loro volta, i direttori di filiale ricevono i dati relativi a nuovi affari ripartiti per funzionario e per segmento di mercato. I direttori di filiale verificano inoltre il rispetto delle norme di legge, esaminando, per esempio, le relazioni richieste dalle autorità tutorie in merito a nuovi depositi che eccedono specifici importi. I flussi giornalieri di tesoreria sono riconciliati con le situazioni nette comunicate alla sede centrale, per consentire a quest'ultima di gestire i trasferimenti e gli investimenti.
- **Elaborazione dei dati.** Numerosi controlli vengono eseguiti per verificare l'accuratezza, la completezza e l'autorizzazione delle operazioni. I dati inseriti sono sottoposti a procedure automatiche di controllo o confrontati con archivi di verifica approvati. L'ordine di un cliente, per esempio, viene accettato solo dopo il raffronto con un file clienti autorizzato e la verifica del fido concesso. Si controlla la sequenza numerica delle operazioni, per rilevarne la completezza. I totali dei *files* sono confrontati e riconciliati con i saldi iniziali e con i conti di controllo. Le anomalie che richiedono delle verifiche sono trattate da personale amministrativo e, se necessario, segnalate ai responsabili. Lo sviluppo di nuovi sistemi e le modifiche di quelli esistenti sono soggetti a controllo, così come l'accesso ai dati, agli archivi e ai programmi. I controlli sul trattamento dei dati saranno approfonditi nel prosieguo di questo studio.
- **Controlli fisici.** Attrezzature, scorte, titoli, liquidità e altre attività sono protetti fisicamente e periodicamente inventariati e confrontati con le risultanze contabili.
- **Indicatori di performance.** L'analisi comparata di diversi insiemi di dati, operativi o finanziari, l'esame delle correlazioni e le conseguenti azioni investigative e correttive costituiscono attività di controllo. Gli indicatori di performance includono, per esempio, le variazioni dei prezzi di acquisto, la percentuale degli ordini "urgenti" e l'incidenza dei resi sul totale degli ordini emessi. Indagando su risultati imprevisti o su tendenze anomale, il management identifica le situazioni in cui gli obiettivi connessi all'attività di ap-

provvisionamento rischiano di non essere realizzati. Se le suddette informazioni sono utilizzate unicamente per prendere decisioni gestionali, l'analisi degli indicatori di performance serve esclusivamente ai controlli operativi; mentre, se le stesse sono utilizzate per verificare risultati inattesi evidenziati dal sistema contabile, l'analisi degli indicatori di performance contribuisce anche al controllo delle informazioni di bilancio.

- **Separazione dei compiti.** Al fine di ridurre il rischio di errori e irregolarità, i compiti vengono ripartiti tra più persone. Per esempio, l'autorizzazione delle operazioni, la loro contabilizzazione e la gestione dei beni corrispondenti devono essere svolte da persone diverse. La persona che autorizza vendite a credito non sarà responsabile della tenuta della contabilità clienti né avrà accesso agli incassi. Analogamente, gli addetti alle vendite non devono avere la possibilità di modificare gli archivi relativi ai prezzi dei prodotti e alle percentuali delle provvigioni.

Gli esempi esposti illustrano solo alcune delle innumerevoli procedure svolte giornalmente nelle aziende, che servono a garantire l'aderenza delle attività ai programmi operativi e a mantenere l'organizzazione in rotta verso la realizzazione degli obiettivi.

Politiche e procedure

Le attività di controllo si basano normalmente su due elementi: le politiche che definiscono ciò che si deve fare e costituiscono la base per il secondo elemento; le procedure, che realizzano in pratica le politiche.

Per esempio, in una banca una politica può prevedere l'esame, da parte del direttore di filiale, delle operazioni in titoli effettuate per conto di clienti. La procedura consiste nello svolgere nei tempi richiesti questo esame, utilizzando i parametri indicati nella politica, come per esempio la natura e i volumi dei titoli trattati in relazione al patrimonio personale del cliente e agli anni del suo rapporto con la banca.

In molti casi, le politiche da adottare vengono comunicate verbalmente. La politica non scritta può risultare efficace se è di applicazione consolidata e molto chiara oppure, nel caso in cui si tratti di piccole aziende, in cui i canali di comunicazione coinvolgono solo un numero limitato di responsabili facilitando un'interazione e supervisione del personale.

Scritta o no, in ogni caso, una politica deve essere attuata totalmente, seriamente e con coerenza. Una procedura seguita meccanicamente, se perde di vista la ragione per la quale è stata adottata, sarà sicuramente una procedura inutile.

E' essenziale inoltre che i rilievi emersi dall'applicazione delle procedure siano esaminati e siano oggetto, se necessario, di appropriate azioni correttive. Tali azioni variano a seconda delle dimensioni e della struttura aziendale.

In una grande società, esse si basano su processi di reporting formalizzati (le divisioni indicheranno le ragioni per cui gli obiettivi non sono stati conseguiti ed i provvedimenti adottati per rimediarvi) mentre in una piccola società padronale il titolare incontra personalmente il direttore di produzione per determinare le cause dei problemi e gli interventi da attivare.

Integrazione delle attività di controllo con la valutazione dei rischi

Parallelamente alla valutazione dei rischi, il management deve definire e attuare un piano di azione destinato a gestire i rischi stessi.

La definizione di questo piano consente di individuare le attività di controllo che possono garantire che le azioni siano svolte correttamente e nei tempi previsti.

Per esempio, un'azienda può fissare come obiettivo di "conseguire o superare un certo volume di vendita". Tra i rischi identificati figura quello di non avere una conoscenza adeguata dei bisogni attuali e futuri dei clienti.

Per gestire questo rischio, il management può, peraltro, rilevare l'andamento storico dei comportamenti d'acquisto dei propri clienti ed effettuare un nuovo studio di mercato. Queste azioni o interventi servono anche a definire le attività di controllo da svolgere.

Le attività di controllo fanno parte integrante dei processi attraverso i quali l'azienda cerca di conseguire i propri obiettivi.

Le attività di controllo non sono fine a se stesse e non esistono semplicemente "perché è giusto o corretto". Nell'esempio precedente, il management deve adottare dei provvedimenti per assicurare che i suoi obiettivi di vendita siano conseguiti.

Le attività di controllo sono meccanismi che facilitano la realizzazione degli obiettivi. Tali attività possono consistere nel seguire gli sviluppi delle vendite per cliente in rapporto ai tassi di crescita previsti, come anche in interventi per garantire l'accuratezza dei dati pervenuti. Il controllo, in questo caso, è parte integrante dei processi gestionali.

Controlli sui sistemi informativi

Dato l'ampio affidamento fatto sui sistemi informativi, è necessario che gli stessi siano tenuti sotto controllo, quali che siano le loro dimensioni e le informazioni prodotte, contabili, operative o connesse al rispetto delle leggi.

La maggior parte delle organizzazioni, comprese le piccole aziende o le divisioni delle grandi aziende, dispone di computer per gestire l'informazione. Di conseguenza, i commenti che seguono si riferiscono a sistemi informativi sia automatizzati che manuali.

I controlli applicati ai sistemi informativi gestiti con mezzi esclusivamente manuali differiscono da quelli applicati ai sistemi computerizzati. Tali controlli, sebbene diversi, si basano su concetti identici.

Le attività di controllo relative ai sistemi informativi si possono ripartire in due gruppi. Il primo riguarda i controlli generali, che si applicano alla quasi totalità dei sistemi e assicurano il loro corretto e continuo funzionamento.

Il secondo gruppo riguarda i controlli applicativi, che includono le procedure automatizzate e le relative procedure manuali per controllare l'elaborazione delle diverse operazioni. L'insieme di questi controlli consente di assicurare la completezza, l'accuratezza e la validità delle informazioni contabili o di altre informazioni immagazzinate nel sistema.

Controlli generali

I controlli generali riguardano normalmente le operazioni svolte dal CED, l'acquisizione e la manutenzione del software di sistema, la protezione degli accessi, lo sviluppo e la manutenzione del software applicativo. Questi controlli si applicano a tutti i sistemi: mainframe, minicomputer e stazioni di lavoro individuali.

Controlli sul CED I controlli sul CED includono l'organizzazione e la pianificazione dei lavori, gli interventi degli operatori, le procedure di backup e recupero e i piani di sicurezza (*contingency* o *disaster recovery plan*).

Negli ambienti più sofisticati, questi controlli si riferiscono anche alla pianificazione dei carichi di macchina e alla ripartizione d'impiego delle risorse. In un ambiente ad alta tecnologia, la "schedulazione" dei lavori avviene automaticamente e l'operatore può intervenire on-line.

Gli strumenti di gestione degli archivi dei dati caricano automaticamente i *files* su un'unità di lettura ad alta velocità prima che inizi il lavoro successivo. Il responsabile della gestione dei turni non ha più bisogno di siglare il giornale macchina, in quanto questo non viene più stampato, ma memorizzato direttamente dal sistema.

Centinaia di messaggi passano ogni secondo su una *console* che supporta più unità centrali. I minicomputer funzionano tutta la notte senza sorveglianza.

Controlli sul software di sistema Questi controlli riguardano l'acquisizione, l'installazione e la manutenzione del software di sistema (sistema operativo, sistema di gestione del data base, software di rete, software di sicurezza e sistemi di supporto) che assicurano il funzionamento del sistema nel suo complesso e del software applicativo.

Il software di sistema, vero centro nevralgico dell'attività del centro elaborazioni, assicura le funzioni di accesso alle risorse e di impiego e controllo delle stesse.

Può fornire informazioni sull'uso dei sistemi di supporto in modo che gli accessi non autorizzati, effettuati per esempio per alterare dati, siano registrati e segnalati per eventuali indagini.

Controlli di accesso Questi controlli hanno assunto un'importanza crescente con lo sviluppo delle reti di telecomunicazione. Gli utilizzatori del sistema possono essere in parte sparsi per il mondo e in parte in locali diversi dello stesso edificio.

Se sono efficaci, i controlli in questione permettono di proteggere il sistema contro accessi e utilizzi non autorizzati. Se ben concepiti, possono difendere dai cosiddetti pirati informatici.

Adeguate procedure di controllo degli accessi, come il cambiamento frequente dei numeri di telefono per il collegamento remoto o l'installazione di un dispositivo di richiamata dell'utilizzatore a un numero di telefono autorizzato (*call back*), che evita l'accesso diretto al sistema, possono costituire efficaci metodi di prevenzione di accessi non autorizzati.

I controlli di accesso permettono agli utenti di utilizzare solo le applicazioni o funzioni di cui hanno bisogno, contribuendo così ad attuare una separazione dei compiti. I profili degli utenti autorizzati o interdetti all'accesso a un'applicazione o a una certa funzione, devono essere esaminati periodicamente e ogni volta che è necessario.

Difatti, il personale licenziato o scontento o insoddisfatto può rappresentare una minaccia per il sistema molto più grave di quella dei pirati informatici; le *password* e i profili degli utenti licenziati devono essere immediatamente annullati. Non consentendo l'utilizzo del sistema e le sue modifiche a persone non autorizzate, l'integrità dei dati e dei programmi viene protetta.

Controlli sullo sviluppo e manutenzione del software applicativo Per gran parte delle organizzazioni, lo sviluppo e la manutenzione del software applicativo sono molto costosi. I costi dei sistemi informativi gestionali (MIS, *Management Information Systems*), i tempi spesi, le competenze richieste, l'hardware e il software necessari, rappresentano investimenti d'entità notevole.

Al fine di gestire questi costi, numerose organizzazioni hanno messo a punto delle metodologie di sviluppo dei sistemi che consentono di esercitare un controllo sui progetti di sviluppo o di manutenzione, fornendo un piano che va dalla progettazione alla realizzazione, indicando le fasi specifiche, la documentazione richiesta, le approvazioni necessarie e le modalità di controllo sullo stato di avanzamento delle diverse attività.

La metodologia deve prevedere adeguati controlli sulle modifiche da apportare al sistema: procedure per le richieste di approvazione dei progetti di modifica, analisi di questi ultimi, convalide, test e modalità di avviamento in produzione, che assicurino che le modifiche siano realizzate correttamente.

Un'alternativa allo sviluppo interno è costituita dall'utilizzo di pacchetti applicativi standard, la cui diffusione è in continua crescita. I produttori forniscono sistemi flessibili e integrati, che permettono di eseguire le necessarie personalizzazioni utilizzando le opzioni inserite nei sistemi stessi.

Molte metodologie di sviluppo prevedono l'acquisto di pacchetti standard come alternativa allo sviluppo e includono i passi necessari per controllare i processi di selezione e implementazione.

Controlli sui sistemi applicativi

I controlli sui sistemi applicativi servono per verificare il funzionamento dei programmi, assicu-

rando la completezza e l'accuratezza dell'elaborazione delle operazioni, la loro autorizzazione e la loro validità.

Particolare attenzione deve essere dedicata alle interfacce di un'applicazione, poiché queste sono spesso collegate con altri sistemi che a loro volta devono essere controllati, per assicurarsi che tutte le informazioni da elaborare siano ricevute e distribuite in modo appropriato.

Uno dei contributi significativi dell'informatica al controllo è la sua capacità di prevenire l'inserimento di dati erronei nel sistema, come anche di individuare e correggere quelli che vengono inseriti.

Per fare ciò, gran parte dei controlli sono supportati da procedure automatizzate (*edit check*) che includono controlli sul formato, l'esistenza, la ragionevolezza e altre verifiche sui dati incorporate nell'applicazione nel corso del suo sviluppo. Se queste verifiche sono state ben progettate, possono favorire il controllo dei dati inseriti nel sistema.

Relazioni tra controlli generali e controlli sui sistemi applicativi

Queste due categorie di controlli del sistema informatico sono interdipendenti. I controlli generali sono necessari per assicurare il funzionamento dei controlli sui sistemi applicativi, che a loro volta dipendono dall'affidabilità del processo elaborativo.

Per esempio, controlli sui sistemi applicativi, come riscontri automatizzati e controlli di stampa, esaminano in tempo reale i dati inseriti nel sistema, segnalano immediatamente le anomalie individuate o i formati errati permettendone l'immediata correzione. A tal fine, messaggi d'errore appaiono al terminale o sono rilevati su un tabulato delle anomalie.

L'insufficienza dei controlli generali non consente di fare affidamento sui controlli automatizzati, che richiedono che il sistema funzioni correttamente, utilizzando i file appropriati o includendo nelle apposite stampe tutte le anomalie.

Un altro esempio dell'equilibrio necessario tra controlli sui sistemi applicativi e controlli generali è costituito dai controlli di completezza, frequentemente utilizzati per certi tipi di operazioni per le quali sono adottati documenti prenumerati.

Questi sono generalmente documenti interni come gli ordini di acquisto. I numeri duplicati sono segnalati o respinti dal sistema. Per attivare questo controllo, il sistema rifiuterà l'informazione che presenta anomalie oppure la terrà in sospeso in un apposito file, mentre l'utente riceverà un tabulato che elenca tutti i numeri mancanti o doppi e tutte le operazioni che si scostano sensibilmente dai parametri stabiliti.

Il sistema risponde correttamente a queste esigenze? In che modo coloro che sono preposti al controllo dei contenuti dei tabulati per il follow-up sono sicuri della completezza delle voci che vi figurano?

La risposta a queste domande è data dai controlli generali. I controlli sullo sviluppo del sistema che prevedono esami e test approfonditi delle applicazioni, consentono di verificare che la logica del programma sia valida e che lo stesso sia stato testato per verificare che tutte le anomalie vengano effettivamente segnalate.

Una volta installata l'applicazione, i controlli sull'accesso e sulla manutenzione assicurano che nessuna persona non autorizzata possa utilizzare o modificare l'applicazione stessa e che le modifiche apportate siano debitamente autorizzate. I controlli sull'operatività del CED e sul software di sistema assicurano che le procedure utilizzino e aggiornino gli archivi in modo corretto.

La relazione tra i controlli sui sistemi applicativi e i controlli generali consiste nel fatto che questi ultimi sono indispensabili al funzionamento dei primi e che entrambi sono necessari per garantire un'elaborazione completa e accurata dei dati.

Evoluzione delle tecnologie

Le nuove tecnologie creano nuovi problemi in termini di controllo. Queste tecnologie, che inclu-

dono strumenti di sviluppo del software (CASE, *ComputerAssisted Software Engineering*), la creazione di prototipi che permettono di generare nuovi sistemi, il trattamento delle immagini e lo scambio automatizzato di dati (EDI, *Electronic Data Interchange*) influenzano il modo in cui i controlli vengono realizzati, ma non cambiano i principi base del controllo.

A titolo d'esempio, nel campo dell'informatica distribuita (EUC, *End User Computing*), l'accrescimento della potenza dei microcomputer e il basso costo dei minicomputer consente una distribuzione diffusa dei dati e della potenza di elaborazione.

I dipartimenti e le unità operative possono così effettuare le proprie elaborazioni con una rete locale autonoma e poco costosa. Si tratta in genere di applicazioni sviluppate e seguite dagli utenti, piuttosto che di software sviluppato centralmente.

Per assicurare controlli adeguati sui sistemi di informatica distribuita, è necessario che siano definite e applicate norme per lo sviluppo, la manutenzione e l'operatività dei sistemi. L'ambiente d'informatica distribuita dovrà essere sottoposto a un'attività di controllo simile ai più tradizionali ambienti mainframe.

L'intelligenza artificiale o i sistemi esperti costituiscono una tecnologia in sviluppo. In futuro, quando queste tecnologie saranno integrate in molte applicazioni (sviluppate dal settore sistemi informativi, dagli utenti finali o acquistate) sorgerà il problema di decidere quali tra queste siano più adatte, quali strumenti debbano essere utilizzati e in che maniera debba procedere il controllo.

Molti pensano che questi sistemi saranno alla fine controllati allo stesso modo in cui si controlla attualmente l'informatica distribuita. All'epoca in cui questi iniziavano a svilupparsi rapidamente, la gente si poneva la stessa domanda prima di rendersi conto che il controllo sarebbe stato effettuato allo stesso modo di prima, cioè tramite adeguate attività di controllo.

Controlli peculiari alla specifica azienda

Poiché ogni azienda ha propri obiettivi e realizza proprie strategie, esistono differenze nella struttura degli obiettivi e nelle relative attività di controllo. Anche se due organizzazioni hanno obiettivi e strutture identici, le loro attività di controllo non saranno simili. Ogni azienda è gestita da individui diversi, che utilizzano il loro giudizio personale nell'attivare il Controllo Interno.

Inoltre, i controlli riflettono l'ambiente e il settore nei quali l'azienda opera, come anche la complessità della sua organizzazione, la sua storia e la sua cultura.

L'ambiente nel quale l'azienda opera influenza i rischi cui la stessa è esposta e può presentare obblighi particolari in merito ai rendiconti esterni o richiedere il rispetto di leggi o regolamenti specifici. Un'azienda di prodotti chimici, per esempio, deve gestire dei rischi legati all'ambiente in misura maggiore di una tipica società di servizi e deve trattare la questione dell'eliminazione delle scorie nell'informativa di bilancio.

La complessità di un'azienda, la natura e l'ambito delle sue attività influenzano le relative attività di controllo.

Le organizzazioni complesse con attività diversificate devono affrontare problemi di controllo più difficili rispetto a organizzazioni più semplici e con attività meno articolate. Un'organizzazione con attività decentralizzate che favorisce l'autonomia locale e l'innovazione richiede tipologie di controllo diverse da quelle messe a punto da un'organizzazione fortemente centralizzata. Altri fattori che influenzano la complessità di un'organizzazione, e pertanto la natura del suo sistema di controllo, sono: la localizzazione e la dispersione geografica, la portata e la complessità delle attività e i metodi di elaborazione delle informazioni.

Tutti questi fattori influenzano le attività di controllo, che devono essere progettate in vista di un'efficace realizzazione degli obiettivi dell'organizzazione.

Piccole e medie aziende

I concetti fondamentali delle attività di controllo svolte nelle piccole e medie aziende non differi-

scono sostanzialmente da quelli delle grandi aziende, ma diverso è il grado di formalizzazione con il quale tali attività vengono svolte.

Inoltre, certe attività di controllo non saranno mai adottate dalle piccole e medie aziende, perché spesso il controllo attivato dal loro management è efficace.

Per esempio, il coinvolgimento diretto dell'Amministratore Delegato e di altri dirigenti nell'elaborazione di un nuovo piano di marketing, la scarsa delega di autorità in materia di credito ai clienti, di acquisti e variazioni delle linee di credito, consentono un controllo rigoroso, riducendo o evitando la necessità di mettere a punto controlli di maggior dettaglio.

La conoscenza dei dati relativi ai principali clienti, direttamente ottenuta sul lavoro, e un esame attento degli indicatori di performance, consentono spesso di ridurre il livello delle attività di controllo praticate nelle grandi aziende.

Un'appropriata separazione dei compiti sembra spesso presentare delle difficoltà nelle piccole aziende, almeno in apparenza. Anche le aziende che hanno poco personale sono generalmente in grado di ripartire le responsabilità in modo che il controllo incrociato sia assicurato.

Ma se ciò non è possibile, come può accadere in certe circostanze, la supervisione diretta del titolare dell'azienda su attività incompatibili può assicurare il necessario controllo.

Per esempio, non è raro, allorché esiste un rischio di pagamenti irregolari, che sia il titolare dell'azienda la sola persona autorizzata a firmare gli assegni o che si richieda alla banca di inviare al titolare gli estratti conto mensili in busta chiusa per una verifica degli assegni emessi.

I controlli sul sistema informatico, in particolare i controlli informatici generali e più specificamente i controlli di accesso, possono causare problemi nelle piccole e medie aziende.

Ciò a causa del modo informale con cui le attività di controllo sono spesso svolte. Ancora una volta, la soluzione può venire dal forte coinvolgimento del vertice delle piccole aziende nelle operazioni di gestione.

Una ragionevole sicurezza che ogni errore significativo sarà individuato, deriva spesso dall'utilizzo continuo da parte della dirigenza delle informazioni generate dal sistema e dalla valutazione di queste informazioni alla luce della loro conoscenza diretta dell'attività aziendale, unitamente a certi controlli chiave effettuati da altre persone.

Valutazione

Le attività di controllo dovranno essere valutate nel contesto delle direttive impartite dal management per gestire i rischi connessi agli obiettivi prefissati per ogni attività significativa.

La persona incaricata di questa valutazione dovrà determinare se le attività di controllo siano correlate al processo di valutazione dei rischi e se siano adeguate alle direttive.

Questa valutazione sarà effettuata per ognuna delle attività aziendali importanti, inclusi i controlli generali del sistema informatico.

La valutazione dovrà riguardare non solo la pertinenza dell'attività di controllo in relazione al processo di valutazione dei rischi, ma anche la modalità della loro applicazione.
