Anno LXXXIV – luglio e agosto 1984 – numeri 7 e 8 (fascicolo doppio) – periodico mensile

Introduzione all' EDP Auditing

dell'ing. Bernardo Nicoletti

Premessa

In questo momento, le aziende stanno vivendo intensamente un dibattito tra informatica accentrata e/o decentrata, automazione dell'ufficio e robotizzazione delle linee di produzione, ed un processo di presa di coscienza da parte degli utenti del proprio ruolo di attori principali nella realizzazione e gestione dei sistemi informativi. Si sta anche riscoprendo, o scoprendo per la prima volta, il ruolo importante del Revisore o *Auditor EDP* (*Electronic Data Processing* = Elaborazione Elettronica dei Dati). Questa figura può rappresentare una risposta efficace alla necessità di verificare la funzionalità dei nuovi o dei vecchi sistemi EDP in crescente e continuo sviluppo, con lo scopo di controllare l'aderenza/conformità dei singoli sottosistemi e di tutto il sistema nel suo complesso agli obiettivi aziendali ed alle esigenze di controllo interno.

1. Introduzione

La revisione interna (*Auditing*) è un istituto relativamente recente nelle aziende italiane. Essa mira a verificare l'esatta applicazione dei principi contabili e di revisione nell'ambito delle procedure amministrativo-contabili. A differenza della certificazione di bilancio, l'azione di revisione interna è svolta da personale *interno* dell'azienda. Così mentre la certificazione mira a garantire il diritto degli operatori economici (azionisti, banche, sindacati), fisco e organi della programmazione e controllo, di ottenere informazioni attendibili sui bilanci aziendali, la revisione interna mira a garantire le stesse possibilità agli amministratori centrali delle società. L'istituto della revisione interna ha trovato rapida diffusione nelle grandi aziende, nelle banche, nelle assicurazioni, anche in vista dell'obbligo di certificazione esterna dei bilanci e dell'introduzione di Enti quali la Commissione per la Borsa, meglio nota come CONSOB.

Le difficoltà di lavoro dei revisori interni non sono state poche. Basti qui citare il fatto che solo recentemente in maniera ufficiale è stato possibile disporre di una delibera della CONSOB sui principi contabili e di revisione. Ancora meno attenzione sembra essere stata dedicata alla metodologia concreta di lavoro degli enti di revisione interna nelle aziende. In questa dire-

zione, uno degli aspetti più interessanti riguarda il collegamento tra revisione interna e l'EDP.

Infatti una nuova e differente categoria di rischio, quella dei reati tramite sistemi informativi basati su elaboratore, minaccia e sfida le aziende a fornire nuovi tipi di garanzie. È relativamente facile infatti commettere frodi in questo ambito, utilizzando il sempre maggiore sviluppo delle reti di comunicazione ed elaborazione dei dati.

La ancora più recente diffusione di macchine per l'elaborazione dei testi, e di altre attrezzature basati sull'elaboratore e su reti di telecomunicazione, rende ancora più facile sottrarre o modificare dati ed informazioni aziendali. In risposta ad una crescente ondata di reati sulle informazioni, un sempre maggiore numero di società sta intensificando i suoi metodi per la sicurezza delle informazioni. Un'informazione immagazzinata elettronicamente è infatti più rapidamente accessibile e più facile da rubare di una scritta su pezzi di carta.

2. L'elaborazione elettronica dei dati

Le tecniche EDP variano notevolmente, a seconda degli obiettivi di utilizzo, della progettazione del sistema e del tipo di macchinario e di utilizzo che se ne fa. Concettualmente è però possibile distinguere un certo numero di fasi fondamentali:

— l'ingresso dei dati nel sistema;
— la trasmissione dei dati;
— l'elaborazione iniziale;
— l'archiviazione su mezzi magnetici, in banche dati;
— la produzione di un'informazione in unità, come un tabulato o una risposta ad un terminale.

Nelle applicazioni cosiddette « *batch* », o di massa, le fasi elaborative sono discrete: vengono letti tutti i dati, viene effettuata l'elaborazione e viene prodotto un tabulato. Nell'applicazione in linea, cosiddetta « *on-line* » si utilizzano dei terminali video o scriventi per colloquiare con l'elaboratore. L'informazione in uscita viene normalmente ottenuta direttamente al terminale, o come si suol dire « in tempo reale ».

Non tutte le fasi precedenti sono praticamente presenti in tutte le elaborazioni. Concettualmente lo sono. La suddivisione è comunque importante perché frodi o perdite si possono avere in ciascuno degli stadi indicati. Di conseguenza, è necessario verificare l'esistenza di opportuni controlli in ciascuna di esse.

3. I controlli nei sistemi informativi basati sull'elaboratore

L'evoluzione rapida nelle tecnologie e nelle apparecchiature per l'elaborazione elettronica dei dati ed il risultante accrescimento delle capacità logiche e di potenza hanno, infatti, consentito allo strumento elaborativo di assorbire una parte sempre maggiore dell'elaborazione dei dati e della produzione delle informazioni. I vantaggi che se ne sono ottenuti sono stati enormi soprattutto nel campo gestionale ed amministrativo. In effetti, la rapida diffusione, dapprima dei grossi/medi elaboratori e successivamente dei mini/micro elaboratori, è da sé testimonianza dei vantaggi che è possibile ottenere dall'uso di questi strumenti, soprattutto in termini di rapidità di risposta, capacità elaborativa, vantaggi rispetto alla concorrenza ed al carico crescente di incombenze fiscali/civilistiche. In questa rapida diffusione spesso non si è data particolare importanza al fatto che i sistemi EDP possono avere impatti significativi sui controlli interni. È questo un elemento da non trascurare giacché l'elaborazione automatica dei dati risulta oggi così strettamente integrata con le strutture operative delle aziende, da rappresentare una condizione essenziale per la loro efficienza anzi spesso per la loro sopravvivenza.

Alcuni dei cambiamenti, introdotti dall'elaborazione elettronica dei dati, nei controlli contabili sono facilmente identificabili.

La tradizionale segregazione dei compiti può venir meno, giacché una sola persona può svolgere funzioni apparentemente incompatibili, quali far compiere un'operazione fraudolenta al sistema e nascondere il fatto. Così il numero di persone che trattano un certo fatto contabile viene ad essere ridotto, spesso semplicemente all'individuo che introduce dati nell'elaboratore. Al diminuire del numero di persone coinvolte, un livello di controllo soddisfacente può essere assicurato solo se controlli addizionali vengono inclusi nel sistema EDP. Così, nel trattare una fattura passiva, una sola persona può svolgere il lavoro di protocollo, controllo ed autorizzazione al pagamento di un fornitore che, ad esempio, potrebbe non aver fornito proprio niente.

Inoltre è spesso difficile identificare i fabbisogni di coordinamento e controllo. In un ambiente semplice, un solo capo può essere il responsabile della raccolta, dell'elaborazione e dell'utilizzo dei dati. Egli assicura la qualità del risultato. In un sistema EDP, spesso un capo è responsabile solo di una fetta del processo e dei relativi controlli. Questa distribuzione di responsabilità può portare ad una perdita di controllo, a meno di definire chiaramente e formalmente i fabbisogni e le responsabilità di controllo, e successivamente di comunicarli, verificarli ed assicurarne l'uso.

Le frodi nell'ambito degli elaboratori possono essere classificate a grandi linee in tre categorie:

1. azioni sugli archivi o banche;
2. azioni sui processi elaborativi o sui programmi;
3. manipolazione degli ingressi e/o uscite dell'elaboratore.

Ci sono cinque obiettivi che devono essere raggiunti quando si valuta la sicurezza delle operazioni connesse con l'elaborazione elettronica dei dati:

1. minimizzare il rischio;
2. minimizzare la perdita, se si dovesse verificare;
3. individuare le persone e le condizioni responsabili della perdita;
4. descrivere come e perché la perdita si è verificata;
5. imparare da ogni perdita e correggere ogni deficenza.

A fronte di tutte queste sfide, il revisore interno si trova normalmente impreparato. Egli ha posto tradizionalmente la sua attenzione alla verifica delle registrazioni dei fatti amministrativi e dei controlli che assicurano l'accuratezza e la completezza delle scritture contabili. Questa verifica si basava in passato su un'indagine manuale attraverso i libri contabili ed i documenti scritti, a supporto delle scritture. Con l'avvento delle tecnologie e dei nuovi concetti informatici, i revisori interni si trovano di fronte a nuove problematiche, sia nelle grosse che nelle piccole organizzazioni. Infatti la maggioranza dei controlli che assicurano l'accuratezza e la completezza delle elaborazioni sono ora automatizzati e non possono più essere visti e verificati con un'osservazione solo visiva.

4. La figura del revisore EDP

Da ciò che si è detto finora, appaiono chiari due fatti:

1. il centro di elaborazione dei dati gestisce il trattamento di una delle principali risorse aziendali: l'informazione;
2. con il diffondersi del trattamento automatico dei dati, i controlli interni possono essere allentati e comunque richiedono una loro verifica e se necessario un loro ridisegno.

La conseguenza è stata che con la crescita dell'EDP e con l'aumento di importanza e complessità delle elaborazioni legate ad un trattamento automatico, il ruolo del revisore interno è venuto pertanto cambiando ed assumendo una nuova importanza nel campo dell'informatica. L'Alta Direzione guarda alla revisione EDP come all'ente che verifica l'efficacia del sistema di controllo interno e l'attendibilità dei risultati delle elaborazioni. Questa estensione del ruolo è la logica estensione delle responsabilità tradizionali del revisore interno.

5. L'organizzazione della revisione EDP

Per quanto riguarda l'inserimento dell'ente che dovrà svolgere la revisione EDP nella struttura organizzativa, le esperienze delle aziende, nelle quali tale ente è operante in maniera efficace, suggeriscono di collocarlo o alle dipendenze dell'ente che svolge in generale la revisione interna, o come ente di staff alla Direzione Generale. Unica occasione di conflitto all'interno dell'azienda potrebbe essere la funzione « Controllo o assicurazione di qualità dei sistemi EDP », se questa già esiste. Tale conflitto può essere facilmente evitato o facendo coesistere le due funzioni sotto un'unica responsabilità, o fondendole insieme, in un unico organismo che consenta il controllo dei sistemi informativi, dello sviluppo delle applicazione e della diffusione delle tecnologie innovative (Microelaboratori personali, banche di dati, elaborazione distribuita, reti di trasmissioni, automazione dell'ufficio, robotica, ecc.) in un'ottica di globale aderenza alle strategie di sviluppo complessivo dell'azienda e teso ad armonizzare le diverse dimensioni del processo di crescita dei sistemi (tecnologica, organizzativa, sociale, economica, ecc.) ed a privilegiare gli obiettivi di efficacia e di efficienza.

6. Preparazione professionale della funzione di revisione EDP

Con il continuo ricorso ai revisori interni per valutare e verificare importanti funzioni di controllo nell'EDP, la qualità e la quantità delle loro responsabilità in questa materia stanno continuamente crescendo. Molte aziende, con un ampio numero di applicazioni su elaboratore, necessitano di un maggiore ed un migliore addestramento dei revisori EDP nel contesto della rispettiva funzione di revisione interna.

Occorre anche osservare che il mercato non offre un sufficiente numero di revisori muniti delle caratteristiche necessarie per soddisfare le esigenze.

I risultati evidenziati da una ricerca condotta dallo *Stanford Research Institute* fanno ritenere che sia preferibile scegliere le persone tra i revisori interni che abbiano uno specifico interesse all'informatica ed addestrarle in questo settore. Una volta costituito questo nucleo, il gruppo potrà essere affiancato da altri revisori spinti ad un maggior coinvolgimento nell'EDP.

L'attività di questo gruppo di revisione EDP potrebbe comprendere il supporto all'intera funzione di revisione interna e la conduzione di *revisioni* specialistiche su delle applicazioni nell'ambito dello stesso centro elaborazione dati.

Può anche essere opportuno, se il coinvolgimento nell'EDP aumenta, affiancare loro delle persone che forniscano un'assistenza specialistica in aree specifiche, come ad esempio quella della telecomunicazione dei dati.

Nell'ambito della revisione EDP, acquista particolare importanza la garanzia dell'integrità dei dati. Oltre alle tecniche di supporto al controllo interno, i revisori EDP debbono essere preparati sulla problematica della sicurezza nel campo degli elaboratori. Generalmente, essi non hanno una conoscenza completa in entrambi i campi. Una buona fase di formazione nell'elaborazione dati è necessaria per prepararsi alla problematica della sicurezza nell'ambito dell'elaborazione dati. Esistono peraltro delle scuole specialistiche che possono fornire corsi adatti a formare su argomenti quali: introduzione alla sicurezza, principi per la prevenzione delle perdite, indagini sulle violazioni, sicurezza fisica. Per migliorare ulteriormente la conoscenza della sicurezza nell'EDP, dovrebbero essere presi in considerazione anche dei corsi sulla sicurezza ambientale, la salvaguardia e la prevenzione dalle fiamme e la protezione dagli incendi industriali e dagli eventi naturali (fulmini, inondazioni, etc.).

7. Compiti e responsabilità del revisore EDP

Purtroppo la professione di revisore EDP è stata sempre considerata piuttosto nuova e poco definita e soltanto nel corso di recenti convegni, quali la sesta Conferenza internazionale della *EDP Auditors Association*, avvenuta nel giugno del 1978, sono stati per la prima volta analizzati in maniera abbastanza completa i compiti e le responsabilità della funzione di revisione EDP. È quindi oggi possibile definire abbastanza chiaramente l'organizzazione, le priorità e le responsabilità della funzione di revisione dei sistemi informativi, al fine di utilizzare le risorse in modo efficace e di raggiungere gli obiettivi fissati dai responsabili aziendali. Le funzioni più importanti sono:

Controlli interni ai sistemi applicativi: revisione dei controlli installati nei sistemi applicativi, al fine di accertare che essi producano informazioni tempestive, accurate e complete.

7.1. *Protezione logica*

Circa la protezione logica dei processi elaborativi, l'attività di controllo deve assicurare l'insieme delle misure rivolte a salvaguardia dell'integrità, della correttezza e della riservatezza delle informazioni contro i rischi di alterazioni derivanti da fattori accidentali o dolosi, dall'utilizzo non autorizzato di procedure operative, programmi ed archivi, o dall'accesso non autorizzato ai dati.

Ulteriori elementi di rischio, a copertura dei quali il controllo interno deve essere rivolto per evitare significativi danni nelle elaborazioni, possono essere costituiti da:

— carenza di documentazione nei programmi applicativi;
— ritorno in produzione di programmi revisionati e non sufficientemente collaudati;
— distruzione di archivi conseguente all'impiego nelle operazioni di test;
— procedure non rigorose sulla tenuta e movimentazione dei supporti magnetici.

7.2. *Organizzazione e gestione dell'EDP*

Obiettivo primario della funzione EDP è la creazione di procedure e modalità operative, coerentemente con le politiche aziendali, atte ad assicurare al « sistema azienda » la fornitura di un servizio informatico ottimale, attraverso la gestione appropriata delle risorse a disposizione.

Pertanto, una razionale ed efficente struttura organizzativa e di mezzi, ed una precisa definizione degli obiettivi da raggiungere sono il presupposto fondamentale per un'efficente gestione ed un razionale funzionamento.

L'analisi del settore implica la revisione dei criteri di pianificazione e di gestione del servizio EDP, per accertarne l'adeguatezza ai fini del raggiungimento degli obiettivi aziendali.

È necessario anche dare notevole importanza alle valutazioni tecnico-economiche delle prestazioni dei sistemi elaborativi e delle risorse, per una sempre migliore ed economica utilizzazione degli stessi.

In quest'area, l'attività di controllo interno è rivolta principalmente a garantire:

— la predisposizione dei piani a lungo e a breve termine nel rispetto della normativa prevista dalla metodologia di pianificazione in atto presso l'azienda, con evidenziazione dettagliata delle esigenze sia degli utilizzatori del sistema informativo, sia dell'EDP. In particolare, l'approvazione dei piani deve sempre essere formalizzata da parte dell'alta direzione e degli utilizzatori;
— la rispondenza della struttura EDP alle esigenze in essere, il rispetto dei compiti e delle responsabilità, gli obiettivi fondamentali da perseguire, la formalizzazione delle interrelazioni fra le varie funzioni e la separazione dei compiti;
— la fornitura di un servizio efficente atto a soddisfare le mutevoli esigenze degli utilizzatori, garantendone la continuità e la precisione tecnica dei risultati elaborativi. In relazione a ciò, deve essere adottato, e ne deve essere garantita la manutenzione; un *software* di base, od operativo, che permetta l'espletamento del livello di servizio che l'EDP deve garantire;
— il corretto andamento della gestione negli aspetti fondamentali di esercizio e di investimento, in aderenza alle formulazioni iniziali di *budget* e con analisi critica delle eventuali varianti e delle relative motivazioni;

— l'adozione di metodologie e di procedure che garantiscano la corretta gestione dei programmi e delle applicazioni informatiche, oltre che la loro protezione, in presenza di modifiche, richieste ed autorizzate dagli utilizzatori;
— la congruità delle risorse umane rispetto alle risorse elaborative ed alle esigenze del settore EDP, nonché l'esistenza dei piani di addestramento, al fine di assicurare un continuo aggiornamento professionale e tecnico degli operatori;
— che le acquisizioni, nell'ambito della funzione EDP, di servizi, macchine, programmi, siano corredate di adeguate analisi economiche.

7.3. *Sviluppo e manutenzione dei sistemi informativi*

Si fa qui riferimento alle attività necessarie per la realizzazione del *software* applicativo e per il mantenimento dello stesso in esercizio.

In questo campo, tre aspetti vanno in particolare tenuti sotto controllo:

Ciclo di sviluppo dei sistemi applicativi: revisione delle procedure inerenti il ciclo di sviluppo dei sistemi applicativi, al fine di accertarne l'aderenza agli *standard* istituiti nell'azienda.

Sviluppo delle applicazioni: revisione dei sistemi in fase di sviluppo, al fine di accertare l'adeguatezza e la completezza dei controlli in essi progettati e, se necessario, suggerire controlli addizionali.

Manutenzione dei sistemi: revisione del processo di manutenzione dei sistemi esistenti, al fine di accertare che esso sia in accordo con le norme organizzative.

Per assicurare l'esistenza di controlli adeguati e l'aderenza della logica applicativa alle politiche aziendali, si rende necessario entrare nel merito delle applicazioni automatiche.

Condizione indispensabile per l'efficenza di un sistema di controllo interno sui sistemi informativi è la chiara leggibilità dei programmi elaborativi (attraverso una valida ed accurata documentazione) e la possibilità di analizzare i dati, i metodi di gestione ed i sistemi di controllo in essi inseriti in qualsiasi momento ed a qualsiasi livello. In sostanza, il requisito essenziale è la « trasparenza delle procedure ».

Un ulteriore presupposto di razionalità dei controlli è rappresentato dall'esistenza di una metodologia per lo sviluppo dei sistemi, tale da permettere l'individuazione di prodotti finiti significativi e da rappresentare una più agevole traccia per le analisi a consuntivo.

In quest'ambito, l'attività di controllo è rivolta principalmente a garantire:

— che lo studio di fattibilità, condotto dalla funzione utente con la collaborazione dell'EDP, sia completo ed in linea con gli obiettivi aziendali e i fabbisogni degli utilizzatori;
— che lo studio fornisca all'alta direzione un valido supporto decisionale per la realizzazione del progetto. In tal senso, lo studio deve sempre includere un'analisi del rapporto costi/benefici, ivi compresi i costi di realizzazione e di gestione;
— che l'analisi del sistema applicativo, condotta dall'EDP in stretta collaborazione con la funzione utente, risponda alle esigenze degli utilizzatori ed agli obiettivi aziendali in termini gestionali. Vi debbono inoltre essere strumenti di controllo e di verifica che permettano di accertare la validità e l'integrità dei risultati e dei dati elaborati. In questo contesto, è necessario dare particolare attenzione alla continuità del sistema di controllo interno nelle fasi di interfaccia con attività/procedure manuali o con altri sistemi applicativi;
— che le specifiche di dettaglio sviluppate dall'EDP soddisfino gli obiettivi del sistema informativo e procedurale e siano documentate secondo modalità standardizzate. Inoltre, il controllo deve garantire che i programmi elaborativi siano sviluppati e scritti secondo metodologie definite e linguaggi di programmazione in linea con le scelte aziendali;
— che i programmi applicativi, prima, e l'intera applicazione, poi, siano sottoposti a prove singole e di sistema onde accertare che quanto realizzato sia conforme a quanto progettato in sede di analisi. Nello svolgimento di questa attività, non devono essere usati dati effettivi, ma dati di prova o *test* appositamente costruiti;
— che le modifiche di applicazioni già approvate siano apportate solo a seguito di specifiche autorizzazioni della funzione utente. Le modalità di realizzazione e di prova devono essere identiche a quelle usate per lo sviluppo delle nuove applicazioni.

7.4. *Gestione operativa delle procedure applicative*

È l'insieme delle attività necessarie per il trattamento automatico dei dati, ai fini del raggiungimento dei risultati previsti nelle fasi di sviluppo dei sistemi applicativi, nei tempi e nei modi concordati e nel rispetto delle norme e degli standard previsti.

L'attività di controllo interno rivolta a quest'area ha principalmente l'obiettivo di accertare che le applicazioni siano elaborate in un ambiente adeguatamente controllato. Si tratta quindi in particolare di assicurare che:

— la gestione delle procedure garantisca la correttezza e l'affidabilità (operativa e tecnica) delle informazioni;
— le procedure in atto per:
  – la ricezione dei dati e la spedizione degli elaborati,
  – la trasmissione dei dati per/da l'elaborazione, offrano sufficienti tutele, anche in termini di tempestività operativa;
— siano definite e rispettate le modalità di gestione degli archivi, le procedure di accesso e di salvaguardia degli stessi, i controlli operativi e le normative riguardanti i tempi di conservazione dei supporti.

Al tempo stesso è necessario dedicare attenzione a:

Sicurezza: revisione dei metodi e delle procedure istituite, al fine di assicurare l'adeguata protezione di programmi, dati e apparecchiature. Di questo aspetto, si parlerà più diffusamente in un seguente capitolo.

Programmi di sistema: revisione dei controlli inerenti ai programmi di sistema, al fine di assicurare l'aderenza alle norme previste.

8. La maniera di affrontare la revisione EDP

Sulla base delle verifiche condotte dai revisori esterni, sia nell'ambito dell'EDP che nell'ambito della funzione di revisione interna, a fronte delle carenze evidenziate e delle raccomandazioni fornite, le aziende hanno messo in atto tutte quelle azioni tendenti a migliorare lo stato dei controlli interni.

I revisori EDP sono qualche volta accompagnati da timore quando affrontano un certo settore dell'azienda. Questi timori possono essere superati seguendo poche e semplici regole. La gestione EDP dovrebbe richiedere un incontro con il gruppo di revisione prima di iniziare la revisione stessa così da raggiungere un accordo su quale tipo di controllo debba essere applicato e su quale sistema. La gestione dovrebbe stabilire un criterio in base al quale i revisori riferiscano le risultanze delle loro indagini e le loro raccomandazioni. Dopo questo incontro iniziale, la gestione EDP dovrebbe essere informata della revisione. Potrebbe essere utile nominare una persona dell'ente EDP come collegamento con i revisori. Un piano dell'intervento di revisione serve per valutare quali risorse EDP sono necessarie e quali dovrebbero essere sviluppate. Il gruppo di revisione normalmente fornisce un rapporto di commento e di raccomandazioni, a cui sia la funzione interessata dal particolare sistema EDP preso in esame (ad esempio la gestione fornitori, nel caso di un sistema di contabilità fornitori) che i responsabili dell'EDP dovrebbero rispondere per iscritto. La continua comunicazione tra revisori e personale dell'EDP rende l'operazione un'esperienza positiva e produttiva. D'altra parte, molti gestori di sistema temono l'avvento dei revisori EDP.

Parte di questo timore nasce come naturale reazione umana a non volere qualcun'altro che controlli il proprio lavoro. Spesso, il reale timore è causato dal fatto che i gestori EDP hanno la consapevolezza che i revisori possono trovare qualcosa di errato. Storicamente la gente ha sempre odiato il relatore di cattive notizie non la causa stessa della cattiva notizia. Le revisioni comunque, sono indispensabili e dovrebbero essere preventivate. Se i gestori EDP non collaborano alle indagini dei revisori, sicuramente ne trarranno un rapporto di revisione negativo.

Un gestore EDP che si ponga per la prima volta di fronte ad un'azione di revisione può prepararsi ad essa con cura, così che non vi siano sorprese e si possa ottenere un'esperienza costruttiva. Il gestore EDP dovrebbe considerare il revisore come un alleato che l'aiuta nello sviluppare piani per ottenere risultati validi dal punto di vista aziendale. Le revisioni di un sistema EDP normalmente sono concentrate in tre aree: gestione, sistemi ed operazioni. Ognuna di queste aree dovrebbe essere preventivamente controllata dal revisore e specificamente gli obiettivi dovrebbero essere sviluppati attraverso quelli. Il revisore EDP quindi può agire come una seconda opinione e rendere noti questi obiettivi ai responsabili del settore EDP. Una revisione EDP può essere usata per rendere scorrevoli le aree EDP e per assicurare l'affermazione ed il supporto reciproco degli obiettivi EDP. Ciò può essere fatto solo se esiste una relazione mutua e costruttiva fra l'EDP e la funzione di revisione EDP.

Perché revisione e certificazione possano adempiere in pieno le proprie funzioni si deve poter contare, in sintesi, sui seguenti presupposti:

a) Procedure contabili redatte su basi comuni di riferimento.
b) Procedure contabili verificate su basi comuni di riferimento.
c) Utilizzo di adeguati strumenti professionali del revisore.

È interessante esaminare come l'elaboratore intervenga in ciascuno di questi punti. Nelle aziende di media e grossa dimensione, l'utilizzo dell'elaboratore per le procedure contabili-amministrative è ormai molto diffuso. È chiaro, pertanto, che l'intervento dei revisori interni deve partire sin dal momento del disegno e della progettazione delle nuove procedure basate sull'elaboratore.

Di qui l'opportunità della partecipazione del revisore interno ai gruppi di progetto che definiscono i requisiti da rispettare, studiano le funzioni, disegnano tecnicamente e realizzano le nuove procedure.

In molte aziende, vi è stata una limitata partecipazione allo sviluppo dei sistemi informativi da parte dei revisori interni.

Alcuni revisori interni pensano di dover rivedere i sistemi solo dopo il loro sviluppo; ciò in quanto ritengono che una partecipazione attiva produca

una riduzione della loro dipendenza ed obiettività. Altri revisori interni credono che la loro partecipazione allo sviluppo dei sistemi sin dall'inizio, sia la chiave per assicurare l'esistenza di controlli efficaci nel sistema da realizzare.

Questi stessi revisori ritengono che sia troppo costoso modificare il sistema quando è ormai completato, e che intervenendo nelle fasi iniziali possano cogliere l'unica occasione che permetta effettivamente di influire sull'adeguatezza del sistema di controllo. Il timore di perdita dell'obiettività è superato se la responsabilità operativa del controllo interno è posta là dove deve essere, presso gli utenti.

In passato la mancanza della necessaria interfaccia tra utente ed ente sistemi informativi durante le fasi del progetto, comportava:

— la non completa comprensione del problema da parte dei responsabili dei sistemi informativi;
— la non sufficente sensibilità alle problematiche di tipo trattamento elettronico dei dati da parte dell'utenza con conseguente scarso coinvolgimento della stessa;
— un lento adeguamento delle strutture alle variazioni del progetto e viceversa;
— difficoltà nell'addestramento dell'utenza all'uso delle nuove tecniche;
— un insufficente livello di sicurezza in fase di prova e rilascio del sistema. Così pure la quasi totale mancanza dell'attiva partecipazione della funzione di revisione nelle fasi di sviluppo dei nuovi sistemi, nella verifica di quelli esistenti, nelle modifiche attuate sugli stessi, nella fase di prova e nella valutazione del livello di utilizzo delle procedure da parte degli utenti, comportava;
— la non considerazione, nella fase di impostazione, di accorgimenti particolari per salvaguardare la sicurezza e la riservatezza dei dati e dei programmi;
— la non previsione di liste intermedie di controllo, o di particolari transazioni che potrebbero essere necessarie ai fini di un *audit*;
— l'assenza di un controllo costante e continuo (preventivo anziché consuntivo) per assicurare che tutto si svolga secondo i piani e gli *standard* assegnati, sotto il profilo della sicurezza e del controllo interno.

La responsabilità del revisore EDP si limita alla raccomandazione di adozione di appropriate tecniche di controllo e di *audit* da inserire nel corpo delle applicazioni.

Solo alcune grandi aziende, hanno programmi di *audit* che prevedono un effettivo coinvolgimento dell'*audit* durante lo sviluppo dei sistemi, mentre nelle aziende di dimensioni ridotte i revisori non sono affatto coinvolti nel processo di sviluppo.

Si ritiene che un efficace coinvolgimento nello sviluppo del sistema sia possibile quando:

— l'alta direzione abbia definito le responsabilità per il controllo e l'ampiezza del mandato della revisione interna in merito alle diverse fasi di elaborazione, ed in particolare allo sviluppo delle applicazioni;
— l'ente EDP accetti che il mandato ed il ruolo dell'*audit* sia esteso alle attività di elaborazione dei dati;
— i revisori interni siano in grado di articolare i loro obiettivi in termini comprensibili al personale EDP;
— gli strumenti e le tecniche di *audit* siano sviluppati come parte integrante del disegno e dell'avvio delle applicazioni.

La verifica dei controlli presenti nelle applicazioni deve avvenire sia prima che dopo la loro installazione. Una volta installato il sistema e verificati i controlli, è importante assicurare che ogni modifica al progetto, non abbia l'effetto di degradare i controlli e di indebolire la verificabilità del sistema. Per questi motivi, i revisori interni debbono essere informati ogni qualvolta una modifica possa influire sul livello di controllo che si è richiesto di adottare.

Ma c'è di più. L'intervento del revisore non si può fermare allo sviluppo di nuovi sistemi o ad loro *follow-up*, ma deve realizzarsi anche sui sistemi e sulle procedure esistenti, già in uso comune. In effetti, il revisore si trova continuamente a confrontarsi con le procedure realizzate su elaboratore elettronico. Egli dovrà verificare la rispondenza di questi ai principi contabili e di revisione e garantirne la conformità agli obiettivi che erano stati fissati al momento della loro adozione. Infine, il revisore dovrà rendersi parte attiva per promuovere le necessarie modifiche e i perfezionamenti alle procedure esistenti.

Molti dei dati contabili per stabilire la disponibilità, la conversione e la distribuzione sono trattati dall'elaboratore. Tutti i controlli non richiedono un'eccessiva abilità nell'elaborazione elettronica dei dati, quindi non è pratico mobilitare gli esperti della revisione quando è sufficente una limitata conoscenza EDP. Un normale ente di revisione EDP ha due livelli di competenza EDP.

1. i revisori EDP che sono professionisti tecnicamente competenti di elaboratori;
2. i revisori non-EDP che operano revisioni finanziarie, operazionali e/o di campi che non richiedono specifiche conoscenze EDP.

Gli *standard* per i *Professional Practice of Internal Auditing* hanno fissato delle caratteristiche essenziali per i revisori interni che includono:

1. obiettività nell'operare le revisioni;
2. possesso della conoscenza, dell'abilità e delle discipline essenziali per operare le revisioni;
3. abilità nelle comunicazioni orali e scritte.

Per avere la competenza EDP, un revisore dovrebbe possedere nozioni di:

1. « *hardware* »;
2. sistemi operativi;
3. « *computerese* »;
4. carte di flusso;
5. gestione degli elaboratori.

Quando lo staff interno di revisione è « EDPizzato », esso crea un team di revisione EDP generalizzato e specializzato.

9. La sicurezza fisica

L'informazione è una risorsa aziendale e, come tutte le risorse, deve essere opportunamente tutelata. Tale concetto rimane valido anche quando l'informazione è immagazzinata e gestita mediante un elaboratore elettronico.

Lo sviluppo dell'elaborazione automatica dei dati, nonché la diffusione e generalizzazione delle moderne tecniche di gestione, impongono che si affronti efficacemente un'analisi dei rischi a cui l'informazione è esposta nella realtà operativa, anche in funzione del tipo di attività dell'azienda. Questi rischi vanno quindi monetariamente valutati, in modo da non affrontare costi per la sicurezza in misura sproporzionata alle situazioni di rischio a cui è esposta l'informazione stessa.

In quest'area, l'attività di controllo deve tendere alla copertura di tutte le possibili condizioni di esposizione al rischio del patrimonio informativo, e più precisamente tutelare:

— l'integrità fisica delle risorse (compresa l'informazione);
— l'efficenza del piano di emergenza,

oltre che ovviamente l'integrità logica dei processi elaborativi, così come esaminato nei capitoli precedenti.

Per quanto riguarda la protezione fisica, l'attività di controllo tenderà a realizzare l'insieme delle misure e azioni atte a prevenire e limitare gli eventi accidentali e dolosi che possono danneggiare le risorse (persone, informazioni, ambienti, impianti e apparecchiature) compromettendo il patrimonio e la funzionalità operativa dell'ambiente EDP.

Le aziende, dotate di elaboratori, sono esposte a grossi pericoli per danni e distruzioni dovuti ad incendi, esplosioni, inondazioni, guasti meccanici, perdite di programmi ed archivi di dati. La sicurezza fisica dovrebbe essere garantita fin dal progetto di costruzione. Vanno considerati in particolare i seguenti aspetti:

1. la collocazione;
2. la costruzione;
3. le riserve di energia;
4. le prevenzioni e le protezioni dagli incendi e dai fulmini;
5. le protezioni dall'acqua.

Altri metodi e procedure di sicurezza non fisica dovrebbero essere stabilite ed impostate dal responsabile del centro. Queste dovrebbero includere:

1. controllo degli accessi;
2. politica del personale;
3. assicurazione di protezione;
4. archivi di sicurezza essenziali;
5. attrezzature di emergenza;
6. procedure di emergenza.

I dati di sicurezza e le procedure operative dovrebbero essere rese effettive.

Il costo degli incidenti nel campo degli elaboratori negli Stati Uniti d'America nel corso del 1982 dovrebbe aver superato i 200 milioni di dollari.

I sinistri nell'ambito dell'elaborazione dati possono avvenire in tempi inaspettati ed in modi imprevedibili. Il bisogno di proteggere le installazioni di elaboratori sta crescendo. Prendendo opportune cautele al momento della progettazione queste disgrazie possono essere superate. Le assicurazioni possono garantire per la perdita patrimoniale connessa con l'elaboratore o con il suo uso fraudolento. Spesso però, la distruzione di un elaboratore o di un suo componente chiave può portare praticamente all'impossibilità per un'azienda a continuare ad operare nel suo campo di attività ordinaria. Si pensi ad esempio al caso di una banca, i cui sportelli siano provvisti di terminali o ad una società aerea che prenota, accetta, controlla e contabilizza i propri voli con l'elaboratore. In questi casi, si può accettare una penalizzazione massima nel non usare l'elaboratore di qualche ora, ma poi bisognerebbe chiudere bottega se non si risce a ripristinare un uso normale dell'elaboratore.

Per proteggersi da questi rischi, è essenziale che l'azienda metta a punto un piano di emergenza. Esso dovrà essere valutato con l'insieme delle azioni e misure formalizzate, atte a consentire il recupero delle attività «vitali». In linea generale, il piano dovrà indicare le azioni da compiere allo scopo di

minimizzare i danni relativi alle macchine ed ai programmi (sia operativi che applicativi) ed agevolare le operazioni di ripristino, i compiti del personale coinvolto e le modalità di trasferimento delle procedure « vitali » ad un centro di calcolo alternativo.

Naturalmente per cautelarsi contro i danni potenziali a cui è sottoposto un centro elaborazione dati è possibile ricorrere alle assicurazioni. Data la rilevanza economica assunta, sempre più numerose compagnie di assicurazione stanno entrando nel campo della sicurezza dei sistemi di elaborazione dati. Ancora insicuri di quali sono i rischi, di quanto può costargli, e di cosa devono coprire, gli assicuratori stanno prudentemente coprendo le perdite per furti e frodi automatizzate, oltre agli affari perduti per guasti ed altre avarie. Altri tipi di assicurazione attualmente disponibili sono:

1. l'assicurazione per l'elaborazione elettronica di dati che si estende fino all'incendio ed a quella che è la polizza generica;
2. la copertura errori ed omissioni per rimborsare gli utilizzatori per perdite dovute alla programmazione o ad altri errori.

Per le aziende, i rischi dovuti a frodi in ambito di elaboratori ed altri reati sono impressionanti. La larga diffusione di elaboratori personali e di video-giochi aumenta notevolmente i rischi, come se un'intera generazione stia per essere sfidata a vincere la macchina. Il mercato per le compagnie di assicurazione è colossale, ma lo è anche l'esposizione al rischio.

I nuovi sistemi di protezione dalle frodi nel campo degli elaboratori sono comprensivi di copertura su alcuni reati generici come disonestà in generale, crimini di cancellazione, sparizione e distruzione, o forme più estese per l'assicurazione del denaro e della sicurezza. Ogni assicurato, con l'eccezione di quelli che sono avvantaggiati dai legami con gli istituti finanziari, può essere coperto.

L'approvazione dei nuovi sistemi di protezione in ambito di elaboratore prevede un'ulteriore assicurazione alla polizza anticrimine a cui sono assegnati. L'approvazione copre la perdita che risulta da ingiustificate sottrazioni di denaro, assicurazioni ed altre proprietà collegate all'uso fraudolento di qualunque elaboratore per trasferimento della proprietà a una persona non autorizzata. Questa nuova assicurazione deve essere usata come supplemento, non sostitutivo, agli attuali sistemi di sicurezza in ambito di elaborazione di dati.

Nei passati venti anni, la crittografia è stata rivoluzionata da veloci, potenti ed economici elaboratori. Mentre nel passato era per lo più di pertinenza militare e governativa, oggi le organizzazioni commerciali hanno un bisogno crescente di trasmettere ed immagazzinare informazioni riservate. I maggiori utilizzatori commerciali sono le banche e gli istituti finanziari. La maggior-

parte del trasferimento quotidiano di miliardi di lire avviene sulla rete telefonica pubblica, richiedendo un alto livello di sicurezza. Due tra i più diffusi sistemi commerciali disponibili sono: il *Data Encryption Standard* (*DES*) ed il *Public Key Cryptography*. Il DES prima divide l'intero testo del messaggio in blocchi di dati, che sono poi cifrati trasponendo e sostituendo i *bit* nel messaggio originale. Lo svantaggio del DES è che il ricevente deve avere un identico impianto di cifraggio. Il *Public Key System* si basa sulla manipolazione matematica per cifrare il messaggio. Come sistema è lievemente più difficile da usare rispetto al DES.

Nel caso di distruzione di un centro, per eventi naturali o criminosi, l'essere assicurato garantisce per la perdita patrimoniale, ma è poi necessario garantire la continuazione dell'attività. A questo scopo è possibile fare dei contratti con apposite società che garantiscono la disponibilità di un centro di riserva in condizioni eccezionali e, naturalmente contro il pagamento di un certo canone anche quando non si utilizzi il centro alternativo. Per fare un esempio, una di queste società, negli Stati Uniti di America, la *Sun Information Services Inc.* ha tre installazioni di emergenza perfettamente configurate per utilizzatori di elaboratori IBM. Altre ditte offrono attrezzature di emergenza per clienti di altre marche. I prezzi d'uso di queste attrezzature variano. Il più elevato costo della *Sun* è di 5.500 dollari/mese per tre anni per accedere ad un elaboratore *IBM* 3033, con ulteriori 25.000 dollari poter far uso del centro a sole 4 ore dal sinistro.

10. Gli strumenti

Esistono tre modi fondamentali di lavorare per la revisione EDP:

— intorno all'elaboratore;
— attraverso l'elaboratore;
— con l'elaboratore.

La revisione *intorno* all'elaboratore consiste nell'utilizzare tecniche manuali per verificare l'accuratezza delle elaborazioni svolte dal calcolatore. Non vi è un coinvolgimento diretto del revisore con l'elaboratore all'interno del calcolatore. Usando questa definizione, la revisione *intorno* all'elaboratore include delle tecniche come l'osservazione dei controlli, l'esame rapido del sistema, la revisione della documentazione, il risalire nei passi che hanno portato ad un risultato, la revisione dei risultati dell'elaborazione ed il ricalcolo manuale dei risultati dell'elaborazione. La revisione *attraverso* l'elaboratore implica il coinvolgimento del revisore nel processo dell'elaboratore. Essa include tecniche come la revisione delle istruzioni nei programmi, l'uso dei

diagrammi di flusso della logica dei programmi e l'elaborazione specifica di dati di prova.

Nello svolgimento del lavoro di revisione, l'elaborazione può, a sua volta, essere adoperato come uno strumento per aiutare concretamente chi deve svolgere questo tipo di lavoro. Si tratta in questo caso di effettuare una revisione *con* l'elaboratore, piuttosto che *attorno* o *attraverso* l'elaboratore.

Esistono sul mercato tutta una serie di pacchetti applicativi, di programmi preconfezionati per l'elaboratore. Essi danno un supporto ad indagare la realtà contabile-amministrativa degli enti aziendali attraverso una strumentazione che agevoli l'esame delle « aree » oggetto di verifica da parte dei revisori interni.

L'opportunità di dotare la funzione revisione di supporti di questo tipo scaturisce da una serie di problematiche quali:

— la numerosità dei fatti amministrativo/contabili che il revisore è chiamato a verificare e sui quali deve formulare il suo giudizio obiettivo ed imparziale;
— l'obbligo di garantire un controllo costante nell'ambito delle aree soggette a verifica, tale da coprire l'intervallo di tempo intercorrente tra una verifica e l'altra;
— la necessità di conoscere l'universo, sul quale si centra l'azione, sia in termini di valore che di numero di transazioni;
— la ristrettezza di tempo che condiziona lo svolgimento di una revisione e che quindi impone una ottimizzazione delle risultanze in termini d'efficenza e di costi.

Questi supporti dovrebbero essere visti in maniera integrata nell'ambito di un Sistema Informativo di Revisione. Essi si propongono di facilitare la conoscenza della realtà contabile degli enti aziendali attraverso una strumentazione che agevoli l'esame delle « aree » oggetto di verifica da parte dei revisori interni.

Essi identificheranno due momenti operativi:

a) fase di preparazione dell'*audit*, in cui consentano:

— le analisi statistiche descrittive ed interpretative sull'insieme delle scritture contabili; esse consentono una verifica dell'« universo » delle registrazioni contabili sia a livello di sintesi, sia a livello di dettaglio, sia mediante rappresentazioni grafiche di:
  - distribuzioni di frequenze per numerosità e valori, a vari livelli di aggregazione (conto, ente, centro di responsabilità, etc.);
  - elencazione di scritture con specifiche caratteristiche;

- determinazione di parametri di statistica descrittiva (medie, variabilità, percentuali, etc.);
- visualizzazione di istogrammi delle frequenze;
- il campionamento statistico di tipo stratificato delle scritture stesse;

tramite in particolare quest'ultimo metodo è possibile:

- ridurre il numero delle scritture contabili da esaminare;
- selezionare i valori più rilevanti;
- guadagnare in efficienza, in termini di affidabilità e di precisione;
- individuare il livello di affidabilità più opportuno.

Per quanto riguarda l'archivio « storico », è evidente l'importanza di raccogliere e conservare i risultati delle analisi campionarie e di poter comparare periodi differenti e confrontare i risultati dell'indagine fatta utilizzando i dati campionati negli Enti sotto revisione;

b) fase *audit* e di stesura del rapporto finale, in cui consentano:

— la verifica dell'affidabilità dei risultati ottenuti;
— la creazione di un archivio storico contenente i risultati conseguiti;
— le analisi comparative su analoghi risultati relativi ad indagini precedenti.

Trattandosi di supporti, tesi a migliorare e rendere più efficienti le indagini di revisione interna, si intravvedono diversi benefici, quali:

— riduzione dei tempi di analisi;
— riduzione dei tempi di elaborazione manuale;
— diminuzione delle richieste di tabulati;
— maggiore attendibilità dei risultati;
— minore volume della documentazione di lavoro;
— possibilità di analisi alternative non predeterminate, sia a livello di dettaglio che a livello sintetico.

Questi programmi preconfezionati dovrebbero rendere possibile l'esecuzione di ogni procedura operabile manualmente, e ciò dovrebbe essere indipendente dal regolare lavoro del sistema.

Le considerazioni generali che dovrebbero essere incluse nella scelta di questi pacchetti comprendono:

1. un'indagine per conoscere i pacchetti di supporto alla revisione disponibili;
2. un esame di coloro che li distribuiscono;

3. un esame costo/beneficio. Prezzi minori del pacchetto implicano normalmente spese ulteriori per l'installazione, per l'istruzione e l'uso del sistema;
4. le caratteristiche di ingresso ed uscita dei dati che devono essere fornite per ogni pacchetto proposto, così pure per le caratteristiche delle operazioni logiche ed aritmetiche possibili con il pacchetto;
5. una selezione dei migliori va operata seguendo certi fattori: la compatibilità con le macchine ed il *software* di base su cui si intende adoperarli, le funzioni svolte, e le eventuali referenze.

11. I nuovi campi di applicazione

La tecnologia dell'elaborazione elettronica dei dati sta mutando rapidamente. Questo comporta una necessità di adattamento del revisore a nuove tecnologie e di conseguenza a nuove maniere di effettuare la revisione. Negli ultimi anni, questa situazione si è verificata in particolare per i sistemi in-linea ed i piccoli elaboratori.

11.1. *Revisione di sistemi in-linea*

Le schede sono necessarie. Quando si fanno passare lavori con programmazione « batch », l'elaborazione dei dati avviene in massa su dei dati in ingresso forniti normalmente in formato « scheda ». Gli inconvenienti di questo tipo di approccio sono numerosi:

1. una mancanza di verifica dell'informazione prima di passare un lavoro;
2. « *Flags* » di libero accesso sui lavori di manutenzione normale;
3. errori nel cancellare i « *Flags* » inattivi di accesso.

L'alternativa è costituita da sistemi in-linea, cioè da sistemi accessibili praticamente in continuità via dei terminali, video o scriventi. L'elaborazione non è più di massa, « *batch* », ma praticamente continua. Questi sistemi migliorano indubbiamente l'organizzazione del lavoro, e l'efficacia ed efficienza dell'elaborazione. Dal punto di vista dei controlli interni, questi sistemi tendono ad avere una problematica abbastanza diversa dai sistemi di massa e richiedono quindi al progettista o al revisore una serie di cautele.

I sistemi in-linea sono normalmente accoppiati a sistemi avanzati di banche dati centralizzati. Un sistema di questo tipo è caratterizzato come un sistema che possiede una o più delle seguenti caratteristiche:

1. dati di collegamento;
2. dati di integrazione;
3. lancio di transazioni automatiche;
4. pista con controlli non convenzionali o temporanei.

Queste caratteristiche sono un risultato naturale dell'applicazione dell'elaboratore ad una vasta gamma di metodi informativi per il controllo e la gestione ed il tentativo di garantire un più vasto accesso all'elaborazione a potenziali utilizzatori di disparato tipo organizzativo. Ognuna di queste caratteristiche può essere presente nei sistemi di banche dati centralizzati. L'integrazione di dati inerenti lo stesso argomento ma provenienti da molteplici applicazioni è stato un grosso problema risolto nei sistemi avanzati. Questa aumentata integrazione di dati può portare vantaggi economici ed operativi. Un sistema decentrato esiste quando un'elaborazione in un determinato luogo richiede l'accesso a dati immagazzinati in un altro luogo o quando gli elementi dei dati immagazzinati in collocazioni multiple vengono ad essere messi in relazione tra loro. Gli obiettivi di controllo non cambiano nel caso dell'introduzione di un'elaborazione decentrata, nel caso dei dati di comunicazione, o nel caso di sistemi di banche dati integrate.

Gli inconvenienti dei sistemi in-linea includono:

1. l'accessibilità attraverso parole d'ordine che vengono cambiate di frequente;
2. mancanza di un'accurata conoscenza riguardo alle attività portate fuori per ogni sessione di lavoro.

È necessario anche elevare il livello delle procedure ed installare un sistema di monitoraggio di qualche tipo (analisi, controllo, sorveglianza).

11.2. *Revisione di sistemi su mini-elaboratori*

Il mini-elaboratore ha una vasta gamma di possibilità di impiego, come: l'uso di terminali remoti e in linea, banche dati, aggiornamenti di tempo reale ed immagazzinaggio di dati in memorie virtuali, quindi relativamente piccole fisicamente ma accessibili rapidamente. Sfortunatamente la maggior parte delle installazioni sono effettuate da persone con ridotta esperienza di elaborazione dati. Il coinvolgimento parziale di ciascuno con il sistema, i conflitti di dovere degli impiegati coinvolti, molto frequentemente hanno causato i problemi abituali di controllo interno. Il passo più importante per il superamento di questi problemi è la scelta dei giusti supporti a livello di programmi applicativi.

Il maggior costo in un mini-elaboratore è dato dallo sviluppo dei programmi. Sono disponibili molti pacchetti applicativi, ma solo un piccolo numero è bene progettato e sicuro. Quando si progetta un sistema basato su mini-elaboratore ben controllato, una delle aree da tenere in stretta considerazione è quella dell'ingresso dei dati. Una procedura di ingresso dati ben operata è la principale difesa contro errori e frodi. Si dovrebbe chiaramente stabilire chi è abilitato ad introdurre dati nell'elaboratore. Il sistema più

pratico è quello di usare parole d'ordine. Ogni azienda che installi un mini-elaboratore dovrebbe cercare la guida di un esperto revisore. Egli dovrebbe essere contattato fin dall'inizio del progetto, ma la sua opera è vitale nelle fasi finali quando è implicato effettivamente il disegno degli aspetti di controllo del sistema.

È importante per le organizzazioni valutare i cambiamenti alle apparecchiature di controllo e sicurezza prima di firmare un contratto per un mini-elaboratore. Piccole ditte spesso usano mini-elaboratori per rimpiazzare macchine contabili meccaniche e calcolatrici per ufficio. L'utilizzatore privo di esperienza, comunque, corre diversi rischi acquistando un mini-elaboratore e cioé:

1. mancanza di sicurezza per le macchine ed i programmi;
2. perdita concreta di tracce di controllo (*audit-trail*) dovuta ai rapporti di chiavi di controllo trascurate;
3. inadeguata riserva di dati di *software* e di chiavi personali necessarie.

Alcuni programmi non sono sufficientemente dettagliati a causa della fretta del venditore nel battere la concorrenza. Allo scopo di assicurare l'accuratezza dell'elaborazione dei dati e per prevenire l'effettuazione di operazioni inesatte e non autorizzate, i programmi dovrebbero essere forniti di adeguati controlli interni.

I revisori EDP che lavorano con piccoli sistemi non vedono l'ora di liberarsi di impedimenti come minore disponibilità di pacchetti di controllo *software*, minori controlli realizzabili, mediocri referenze documentabli. I responsabili spesso avallano soluzioni mediocri, sostenendo che l'installazione di un sistema di controllo comporta costi elevati. In realtà, le differenze tra i grandi ed i piccoli sistemi non nascono dalla natura delle macchine, ma dal fatto che chi gestisce piccoli elaboratori, ha normalmente una minore esperienza nelle tecnologie sistemistiche dell'elaborazione dati. I controlli aumentano la capacità realizzativa della gestione fornita dal sistema, ma non necessariamente riducono la possibilità delle frodi. Il controllo del sistema elaborativo delle elaborazioni importanti e delle procedure dovrebbe essere effettuato con programmi ed i controlli sono necessari per mantenere la sicurezza delle procedure programmate. Un aiuto nell'incremento di adeguati controlli si può trovare nella gestione delle funzioni del sistema informativo, nei controlli interni, nei consulenti, nei libri o nei corsi di addestramento. Inoltre, sono disponibili un certo numero di tecniche che permettono di affrontare efficacemente problemi di controllo nell'installazione ed esercizio di piccoli sistemi.

Naturalmente, i mini-elaboratori non sono solo un'ulteriore difficoltà per i revisori nello svolgimento del proprio lavoro. Essi sono anche un'op-

portunità e possono essere adoperati per migliorare la maniera con cui viene svolta l'attività di revisione. I mini-elaboratori, soprattutto se portatili, possono diventare un concreto strumento di lavoro per il revisore ogni qualvolta egli debba recarsi a fare una revisione presso un ente periferico (una filiale, un'agenzia, un'azienda controllata, etc.).

Il mini-elaboratore può diventare la sua lista di verifica delle operazioni da effettuare e dei documenti da ricercare. Può diventare il suo foglio di lavoro su cui memorizzare le risultanze delle sue indagini. Può diventare la sua calcolatrice su cui eseguire calcoli complessi sul momento. Oppure può essere utilizzato per collegarsi con l'elaboratore centrale per ottenere, via linea telefonica, ulteriori dati o informazioni che si rendessero nel frattempo necessari. Il tutto è possibile ad un costo e con un peso da trasportare tutto sommato modesti e soprattutto continuamente decrescente.

BERNARDO NICOLETTI