

Audit sui Sistemi di Gestione basati sull'Elettronica (SGBE)

(Traduzione del documento APG-Auditing Electronic-Based Management Systems (EBMS) del 25 Agosto 2005)

1. Introduzione

La crescente dipendenza delle organizzazioni da mezzi elettronici per l'esercizio ed il controllo dei loro sistemi di gestione richiede agli Organismi di Certificazione (OdC) ed agli auditor di guardare a nuovi approcci per assicurare l'efficacia ed efficienza degli audit. Occorre che essi ridefiniscano il modo di valutare i processi e la relativa documentazione (incluse le registrazioni) per verificare la conformità con i criteri degli audit.

Questo documento è stato sviluppato per fornire linee guida generali per l'effettuazione di audit sui sistemi di gestione che sono basati completamente su mezzi elettronici o nei quali gran parte della documentazione è gestita con mezzi elettronici. Esso fornisce inoltre agli OdC ed agli auditor linee guida a complemento delle normali attività di pianificazione e preparazione necessarie prima di un audit.

Questo documento mette l'accento su quei requisiti della ISO 9001 nei casi in cui è possibile l'utilizzo di documentazione e registrazioni elettroniche ed anche nel caso in cui l'accesso a tale documentazione/registrazioni avviene con sistemi elettronici.

Questo documento è stato predisposto per gli auditor con un'ampia e varia esperienza pratica in sistemi di gestione basati sulla elettronica (SGBE), e cioè in sistemi di gestione che si basano per la loro normale operatività su documentazione, dati e software applicativi elettronici. Il documento, comunque, è scritto in maniera tale da permettere il suo utilizzo anche da parte di chi ha solo un'esperienza limitata con i computer ed i SGBE.

L'organizzazione che effettua un audit, sia essa un OdC di parte terza, o un Organismo di Accredimento o una funzione organizzativa interna, è responsabile di assicurare l'efficacia del processo di audit su SGBE. Questo documento utilizza la guida fornita dalla ISO 19011 e suggerisce approcci che possono essere utilizzati dagli auditor dell'ISO 9001 e di altre norme sui sistemi di gestione, quando verificano la conformità alle norme di riferimento.

Gli auditor e le organizzazioni di audit, nel seguire i passi del processo di audit riportati nella ISO 19011, dovrebbero apportare i necessari aggiustamenti per assicurare un approccio adeguato.

Occorre notare che la competenza negli audit SGBE dovrebbe esser vista non come una scusa per accorciare le durate degli audit ma come un modo per ottimizzare la loro efficacia ed efficienza.

Questo documento non intende fornire linee guida per verificare i controlli associati con le informazioni di sicurezza per i SGBE. Chi fosse interessato in controlli attinenti alle informazioni di sicurezza può consultare la ISO/IEC 17799, che è la norma che tratta complessivamente questi aspetti.

2. Preparazione e pianificazione dell'audit

Nella fase iniziale di un audit (cfr. Stadio 1 dell'audit) chi effettua l'audit dovrebbe individuare la struttura dell'organizzazione sotto audit ed il grado in cui il suo sistema di gestione si basa sull'elettronica. Un'organizzazione con molti siti/stabilimenti e con un SGBE centralizzato, o un'organizzazione "virtuale", richiedono dei piani e dei metodi di audit differenti da quelli per un'organizzazione con sede unica e/o definita fisicamente.

L'organizzazione che effettua l'audit e quella che lo subisce dovrebbero concordare il grado di accessibilità e di utilizzazione del SGBE da parte degli auditor. Questo può comportare l'esame di aspetti quali:

- Dare l'opportunità, ai membri del gruppo di audit, di familiarizzarsi con il SGBE dell'organizzazione (includendo nel piano e programma di audit un tempo sufficiente per permettere tale orientamento).
- Le politiche dell'organizzazione sotto audit per l'utilizzo della sua infrastruttura di Tecnologia dell'Informazione.
- Istruzioni per l'accesso alla pertinente documentazione/registrazioni dell'organizzazione ed i necessari permessi di sicurezza (security) per tale accesso.
- Protezioni e processi per assicurare che gli auditor proteggano la confidenzialità della documentazione e delle registrazioni durante e dopo l'audit.

L'organizzazione che conduce l'audit dovrebbe assicurare che nel gruppo di audit vi siano sufficienti competenze per effettuare un accertamento efficace del SGBE.

3. Riesame della documentazione

In base alla capacità dell'organizzazione sotto audit di render disponibile, o meno, la sua documentazione mediante accesso al suo sito web o tramite e-mail, l'organizzazione che conduce l'audit può condurre, in tutto o in parte, l'esame della documentazione fuori sede o collegandosi direttamente al sito web dell'organizzazione sotto audit o scaricando la documentazione trasmessagli elettronicamente via e-mail.

Potrebbe non essere possibile, per motivi tecnici o di sicurezza, effettuare, prima di accedere alla sede dell'organizzazione, l'esame completo del suo SGBE tramite il sito web o la trasmissione via e-mail della attinente documentazione. In questi casi potrebbe essere necessario effettuare le attività di preparazione dell'audit che implicano l'esame di documentazione elettronica (Fase 1 dell'audit) presso la sede dell'organizzazione sotto audit.

4. Attività di audit presso la sede dell'organizzazione

L'approccio dell'audit per i SGBE dipende molto da quanto le evidenze necessarie per stabilire la conformità sono disponibili sotto forma di registrazioni elettroniche.

Durante lo svolgimento di attività presso l'organizzazione sotto audit, i percorsi degli auditor dovrebbero tipicamente includere i luoghi in cui si svolge il processo sotto verifica. Con un SGBE, però, il tempo necessario a confermare le evidenze se un requisito è stato, o meno, rispettato può essere impiegato alla postazione del computer, che può essere o meno situata in vicinanza a dove si svolge il processo.

Quando le postazioni dei computer sono situate in aree lontane, non accessibili nel luogo in cui si svolge il processo, il tempo effettivo di audit presso il luogo dove si svolge il processo può essere ridotto. Potrebbe, però, non essere necessario ridurre il tempo complessivo delle valutazioni, dato che il riesame delle evidenze elettroniche può avvenire prima o dopo aver riscontrato l'esistenza del processo fisico.

Nel caso in cui la postazione computer associata al processo sia collocata lontano, occorre prestare particolare considerazione al tempo necessario per andare e tornare dal luogo in cui si svolge il processo.

Quando il processo implica interventi dell'uomo, l'auditor dovrebbe valutare i metodi utilizzati per le interazioni tra il processo fisico ed i mezzi elettronici per assicurare l'accuratezza delle informazioni associate.

5. Audit sui controlli della documentazione elettronica

I documenti elettronici che stabiliscono le politiche e le procedure possono presentarsi in una varietà di moduli, in relazione alle applicazioni software utilizzate dall'organizzazione per generare documenti.

Questi moduli elettronici possono includere testi, HTML, PDF, etc. Anche i moduli relativi ai fogli elettronici ed alle base dati sono considerati "documenti" elettronici, soggetti a controllo in fase di verifica del sistema di gestione.

Data la facilità con cui gli utilizzatori possono creare fogli elettronici ed altri documenti elettronici, gli auditor dovrebbero assicurarsi che le politiche sui controlli applicabili alla documentazione del sistema di gestione, in generale, si applichino, mediante appropriate procedure, anche per la documentazione elettronica.

Occorre che le organizzazioni che operano in ambiente elettronico adottino metodi opportuni ed efficaci per assicurare un adeguato riesame, approvazione, pubblicazione e distribuzione della documentazione del sistema di gestione. Queste attività dovrebbero essere coerenti con i metodi per lo sviluppo e la modifica della documentazione elettronica.

In molti casi le misure per tenere sotto controllo i documenti possono essere caratteristiche standard già inserite nelle applicazioni software utilizzate per la loro creazione. Gli auditor quindi dovrebbero capire questi controlli, specifici di tali applicazioni, almeno per quanto questi sono utilizzati come una base per valutare la conformità alle norme del sistema di gestione di riferimento.

Data la sempre maggior capacità di modificare, aggiornare, correggere e migliorare i documenti nell'ambito di un SGBE, gli auditor dovrebbero porre particolare attenzione ad elementi di controllo quali l'identificazione dei documenti ed il loro stato di revisione.

Dato che il mezzo elettronico favorisce l'aumento del tasso di modifiche ai documenti, gli auditor dovrebbero verificare che i controlli adottati per la gestione dei documenti obsoleti rientrino tra le politiche e nelle procedure di controllo dei documenti stabilite dall'organizzazione.

Gli auditor dovrebbero verificare che esista una documentazione sui SGBE in grado di orientare gli utilizzatori per quanto attiene gli aspetti funzionali e di controllo associati ai documenti elettronici. I requisiti sulla disponibilità dei documenti "sul luogo di lavoro" stabiliti dalle norme di riferimento, inoltre, sono normalmente riportati, almeno in parte, tra le politiche di accesso alla documentazione dell'organizzazione. Gli auditor dovrebbero comprendere le politiche e procedure dell'organizzazione sulle prerogative affidate agli utilizzatori, dato che queste rappresentano fattori importanti per una corretta realizzazione dei processi dell'organizzazione.

Lo scambio di comunicazioni elettroniche con l'esterno (fornitori ed altre parti interessate) può comportare lo scambio di documenti. Qualora questi documenti esterni possano contenere parametri essenziali che specificano il funzionamento dei processi dell'organizzazione, gli auditor dovrebbero verificare il grado di acquisizione formale e di controllo di questi documenti nell'ambito del SGBE.

6. Audit sui controlli delle registrazioni elettroniche

Le "registrazioni" elettroniche sono dati relativi ai risultati del processo inseriti nei moduli elettronici che li ospitano. Questi moduli elettronici possono variare da semplici fogli elettronici a più complesse base dati applicative.

Gli auditor dovrebbero sapere che gli elementi di controllo stabiliti dall'organizzazione per i moduli elettronici non sono necessariamente gli stessi che si applicano alle registrazioni elettroniche. Ad esempio, per quanto riguarda la "identificazione", nel caso dei *moduli* elettronici il termine riguarda la nomenclatura stessa del modulo elettronico mentre nel caso di *registrazioni* elettroniche, quando

si parla di “identificazione” si fa riferimento allo specifico utilizzo del modulo elettronico per una specifica raccolta di dati.

Gli auditor dovrebbero rivedere i metodi adottati dall’organizzazione per acquisire i dati, in modo da assicurarsi che vi sia adeguata fiducia sull’accuratezza le attività di inserimento dei dati.

Nel valutare i controlli dell’organizzazione per quanto attiene l’immagazzinamento dei dati, gli auditor dovrebbero verificare se le organizzazioni hanno coscienza di quale debba essere la loro capacità di immagazzinamento dati in relazione a:

- il tasso di produzione delle registrazioni
- le politiche di conservazione delle registrazioni e le relative cornici temporali
- il tasso di eliminazione delle registrazioni

dato che questi fattori possono impattare sul regolare funzionamento del SGBE.

Dato che le basi delle conoscenze e le prestazioni dell’organizzazione possono essere quasi interamente raccolte in registrazioni elettroniche, gli auditor dovrebbero esaminare gli approcci adottati dall’organizzazione per assicurare la protezione delle informazioni contenute in mezzi elettronici. Per maggiori informazioni sulla “Protezione delle Informazioni” vedere la ISO/IEC 17799.

7. **Risorse organizzative**

Quando le organizzazioni si spostano verso utilizzazioni SGBE, il ruolo della Tecnologia delle Informazioni diventa essenziale. Gli auditor dovrebbero verificare se l’organizzazione ha dedicato, al riguardo, appropriate risorse (infrastrutture comprese) per assicurarsi che il SGBE funzioni senza interruzioni ed efficacemente.

Gli auditor dovrebbero anche verificare se l’organizzazione ha individuato opportunamente il livello di interazione, supporto e coinvolgimento del personale esperto in Tecnologia dell’Informazione per quanto attiene la predisposizione, la documentazione, la attuazione e la manutenzione del SGBE.

Nell’ambito delle verifiche sulla attribuzione di adeguate risorse, gli auditor dovrebbero valutare come l’organizzazione ha individuato le competenze richieste al personale per gestire l’hardware ed il software che fanno funzionare il SGBE.

Nella fase di inserimento del SGBE, è necessario che i due sistemi paralleli - documenti cartacei e documenti elettronici - restino entrambi funzionanti per un certo periodo, per dare la possibilità agli utilizzatori di familiarizzarsi. In questi casi gli auditor dovrebbero verificare l’approccio adottato dall’organizzazione per assicurare che il SGBE sia effettivamente assimilato ed utilizzato dal personale dell’organizzazione.

La complessità delle infrastrutture di Tecnologia dell’Informazione delle organizzazioni varia in funzione della natura e della complessità delle attività. Gli auditor dovrebbero verificare le politiche e le procedure di manutenzione del sistema adottate dall’organizzazione per la piattaforma di Tecnologia dell’Informazione. Gli auditor inoltre dovrebbero verificare come l’organizzazione tratta i fuori servizio (e relativi tempi) del sistema, perché questi impattano con il normale funzionamento del SGBE. Gli auditor dovrebbero verificare se l’organizzazione ha attivato, o meno, dei sistemi di *back-up* e se di questi ne viene, o meno, periodicamente rivista e provata l’adeguatezza.

In rapporto al software, gli auditor dovrebbero verificare i controlli stabiliti per il software interno, per quello esterno, per quello su licenza e per i loro aggiornamenti. Dato che il software può essere considerato come un documento elettronico dinamico, anche ad esso si applicano le linee guida riportate in precedenza per gli audit sui documenti.

Nei limiti in cui le organizzazioni utilizzano il software per il suo SGBE, gli auditor dovrebbero esaminare la funzionalità delle applicazioni ed il loro rapporto con gli elementi del sistema di gestione stabiliti negli applicabili criteri.

Dato che dei fattori ambientali possono impattare sul funzionamento della piattaforma di Tecnologia dell'Informazione, le organizzazioni dovrebbero prendere adeguate misure per proteggerla da tali fattori. Questi possono spaziare dalla esigenza di adeguate strutture o alloggiamenti a quella di alimentare le apparecchiature con gruppi di continuità non interrompibile (*UPS*). Gli auditor dovrebbero valutare se i controlli dell'organizzazione tengono conto di aspetti quali la manutenzione, le temperature, l'umidità, etc. delle strutture nei limiti in cui questi elementi possono impattare con l'esercizio del SGBE.

8. Comunicazioni elettroniche interne ed esterne

Man mano che aumentano le opzioni disponibili e la semplicità d'uso delle comunicazioni elettroniche, le organizzazioni dovrebbero assicurare che il sistema di gestione (documentato) si occupi di questi mezzi, al fine di assicurare coerenza di utilizzazione nel soddisfare i requisiti del loro SGBE e della norma di riferimento del sistema di gestione.

Quando sistemi Intranet, E-mail, [Instant Messaging](#) sono utilizzati per soddisfare i requisiti del SGBE, gli auditor dovrebbero verificare che le politiche e le procedure prendano in esame le circostanze in cui questi strumenti andrebbero utilizzati. Se, inoltre, i risultati delle comunicazioni elettroniche interne sono utilizzabili per soddisfare i criteri degli audit, gli auditor dovrebbero verificare ad essi siano applicate le politiche e le procedure di controllo delle registrazioni.

Quando l'organizzazione si affida alla sua infrastruttura di Tecnologia dell'Informazione per le comunicazioni elettroniche con i suoi clienti (ad esempio nel commercio elettronico), con i fornitori (negli acquisti elettronici), con le sedi distaccate e con altre parti interessate, gli auditor dovrebbero verificare che la metodologia, le politiche e le procedure per queste comunicazioni, ed associate transazioni, siano formalmente inquadrati nel SGBE.

9. Sistemi di gestione per più siti

Le organizzazioni che operano attraverso più siti (o da una sede centrale a siti satelliti) mantengono di norma comunicazioni e condividono politiche, procedure e dati di processo con le loro diverse localizzazioni attraverso mezzi elettronici, quali Internet, [Extranet](#), E-mail e [Instant Messaging](#).

Quando la piattaforma di Tecnologia dell'Informazione ed i relativi software applicativi sono utilizzati per scambiare informazioni attinenti ai criteri dell'audit, gli auditor dovrebbero capire i differenti mezzi di interconnessione adottati dall'organizzazione nei limiti necessari per accertare se il SGBE risponde ai criteri dell'audit.

Gli auditor dovrebbero verificare se i controlli sul sistema di gestione a più siti sono adeguatamente trattati e stabiliti nelle politiche e procedure dell'organizzazione.

10. Competenza degli auditor

L'affidabilità del processo di audit di un SGBE dipende dall'abilità degli auditor nel comprendere le tendenze nella Tecnologia delle Informazioni, in quanto le organizzazioni si affidano sempre più ai software per monitorare e tenere sotto controllo le proprie attività.

Le organizzazioni che si occupano di audit dovrebbero prendere le necessarie misure, ivi incluse forme di addestramento, per rispondere alle esigenze generali ed individuali della propria base di auditor con riferimento a:

- Tendenze generali della Tecnologia delle Informazioni che possono impattare sulla operatività dei sistemi di gestione;
- Considerazioni specifiche sugli audit, per ciascun incarico di audit assunto.

Dato che le innovazioni nel settore Tecnologia delle Informazioni sono piuttosto rapide rispetto alle modifiche dei criteri degli audit, gli auditor e le organizzazioni di audit si confrontano con l'esigenza di avere una conoscenza pratica delle relative tendenze e del come queste possono essere applicate ed utilizzate nell'ambito del SGBE.

Alla luce delle innovazioni che influenzano il funzionamento di un SGBE, le organizzazioni di audit dovrebbero stabilire se le esperienze necessarie per essere efficaci in un determinato audit sono in possesso del gruppo di audit stesso o se sarebbe necessaria l'assistenza di un esperto tecnico.
