Rilevazione ed analisi del sistema informatico dell'azienda

Ormai oggi la gestione informatica dei dati aziendali è diffusa a livello di tutte le aree aziendali. In particolare, la parte di gestione dei dati per l'area amministrativa ha avuto un notevole sviluppo, anche di obiettivi.

È inevitabile che al crescere della dimensione aziendale, cresce il livello di informatizzazione ed in particolare degli obiettivi da "coprire":

- corretto adempimento degli obblighi fiscali, previdenziali e civilistici;
- ottenimento di analisi consuntivi sia civilistici che gestionali di dati circa l'andamento aziendale;
- elaborazioni ed ottenimento di previsionali.

Il sistema informatico aziendale diventa quindi il depositario di tutte le informazioni presenti e gestite dall'azienda. Alla luce di tutto questo, è inevitabile per il revisore, nella fase di esame del sistema di controllo interno, procedere con la raccolta di informazioni sul sistema informativo aziendale.

Ma che cosa è un sistema informativo?

Il sistema informativo è un insieme di procedure e infrastrutture che definiscono e supportano il fluire delle informazioni all'interno di una struttura organizzativa basato su un'infrastruttura elettronica. Il sistema informativo consente:

1. la raccolta di dati in archivi organizzati
2. l'estrazione di informazione tramite l'elaborazione dei dati,
3. la distribuzione delle informazioni agli utenti.

☞	***Cosa è un Sistema Informativo*** Insieme degli strumenti, risorse e procedure che consentono la gestione delle informazioni aziendali. - *insieme dei sistemi hardware e software presenti in una azienda;* - *assicura la generazione, l'elaborazione, la circolazione e la memorizzazione delle informazioni su supporti magnetici.*

Lo stesso è composto da:

- Dati:
  - ✓ di configurazione
  - ✓ operativi
  - ✓ di supporto
  - ✓ di stato

- Procedure di:
  - ✓ acquisizione
  - ✓ controllo ed elaborazione
  - ✓ pianificazione
- Mezzi:
  - ✓ server, stazioni di lavoro, terminali di rilevazione dati, apparecchiature di rete.

☞	*Un sistema informatico è considerato sicuro quando è in grado di garantire il soddisfacimento delle proprietà di confidenzialità, integrità e disponibilità.*

Per comprendere in modo adeguato l'ambiente IT, il revisore dovrà valutare la rilevanza e la complessità delle elaborazioni effettuate dai computer nelle principali applicazioni contabili. Ci riferiamo ad esempio ai complicati calcoli svolti dal computer, che generano operazioni significative che non possono essere indipendentemente convalidate a causa della mancanza della relativa traccia contabile.

Spesso il "computer" può essere utilizzato per la creazione di bilanci, bilanci di verifica, mastri generali e altre carte di lavoro. In questi casi, anche se è il computer stesso a "*… provvedere alla stesura del bilancio*", il revisore non dovrà partire dal presupposto che gli importi in bilancio siano automaticamente affidabili.

In conformità a quanto previsto dal principio di revisione nr. 400 "la valutazione del rischio e il sistema di controllo interno", il revisore deve "...valutare l'ambiente informatico nel pianificare le procedure di revisione al fine di ridurre i rischi ad un livello accettabile".

La definizione di "rischio" concettualmente più vicina alla nostra è: "il potenziale che una certa minaccia potrebbe innescare le vulnerabilità di un bene (asset) o gruppo di beni e causare perdite o danni del bene".

L'analisi del rischio consiste nella valutazione sistematica di tutti i fattori di rischio individuati. Normalmente la modalità più diffusa consiste nell'attribuzione di un coefficiente qualitativo (alto, medio, basso), che classifica l'importanza di ogni fattore e di ogni classe di fattori.

Il revisore verifica il grado di correttezza con cui determinate informazioni forniscono adeguata rappresentazione di una specifica realtà aziendale. Un'informazione può considerarsi attendibile qualora, dal suo confronto con altri dati rappresentativi della medesima realtà, emerga una sostanziale, precisa e univoca concordanza.

Il giudizio di attendibilità del sistema informativo è spesso un giudizio probabilistico.

La numerosità di sistemi di rilevazione non garantisce la qualità delle informazioni ottenute in mancanza di un'adeguata suddivisione organizzativa del lavoro tale per cui i diversi sistemi di rilevazione siano gestiti da operatori sostanzialmente differenti. Lo strumento principale è la separazione dei ruoli, rappresentata dal ciclo autorizzazione – esecuzione –

controllo.

Lo scopo del lavoro di rilevazione del sistema IT aziendale è quello di fornire una *review* ad alto livello del sistema informativo dell'Azienda, evidenziando i cambiamenti avvenuti e in corso di attuazione. Le informazioni generalmente riguarderanno le seguenti aree:

- Descrizione generale dei Sistemi Informativi
- Organizzazione della Direzione IT
- Software applicativo
- Modalità di esecuzione delle modifiche/nuovi sviluppi software
- Sicurezza logica e fisica
- Business Continuity e Disaster Recovery Plan
- Conformità legale
- Progetti in corso di attuazione.

Per rilevare le informazioni di cui sopra saranno utilizzate le informazioni già note dalle attività precedentemente eseguite presso l'Azienda e comunque completate con interviste. Alcune attività da intraprendere nello stabilire l'approccio di revisione includono:

a) distinguere tra funzioni automatiche e manuali nella registrazione dei sistemi contabili e di controllo interno;
b) stabilire se il programma utilizzato è conosciuto e affidabile. In questo caso, infatti, il rischio di errore sarebbe basso;
c) valutare se l'ambiente in cui vengono tenuti i computer e conservati i dati è tale da garantire l'accuratezza dell'input dei dati e la sicurezza delle informazioni elaborate (utilizzo di password/back up - copia dei file -);
d) in particolar modo, quando il revisore ha a che fare con programmi conosciuti e utilizzati a livello mondiale, che non hanno mai dato problemi di errori (nel caso vi fossero stati, i media ne avrebbero sicuramente dato notizia), sarà bene valutare la possibilità di ridurre i test applicati con l'unico scopo di rilevare inesattezze di calcoli aritmetici e registrazioni.

Di seguito viene riportato un programma-guida standard, da adattare in base alle specifiche esigenze, per la rilevazione ed analisi del sistema informatico aziendale.

Le informazioni che desideriamo raccogliere riguardano i seguenti argomenti:

Sistema informativo

- breve descrizione degli hardware utilizzati;
- sedi e collegamenti;
- reti Lan – Wan e relativi schemi di rete;
- server aziendali: nome, piattaforma, funzione, applicativi installati.

Ufficio IT

- organigramma, ruoli e responsabilità dell'ufficio IT;

- assegnazione delle responsabilità per tutti gli utenti ai sensi della legge 196/2003;
- adeguamento al d.lgs. 196/2003 - Documento Programmatico sulla Sicurezza Informatica (d.lgs. 196/2003);
- attività di configurazione e manutenzione degli apparati di rete;
- esistenza di formali procedure operative, standard e norme interne come ad esempio il sistema di aggiornamento automatico; la gestione delle licenze; il controllo dei log dei firewall, ecc.

Applicativi

Per ogni software:

- nome del modulo o del pacchetto;
- piattaforma dell'hardware e del sistema operativo;
- eventuali sviluppi;
- documentazione tecnica ed utente (tipo manuali, procedure, ecc.);
- principali funzioni (attivo, passivo, tesoreria, ecc.) supportate.

Sicurezza

- procedure (scritte e non) per l'accesso fisico ai data centers (accesso limitato mediante badge o chiave, sistema anti intrusione, ecc.);
- adeguatezza dei locali dei data centers (esistenza di impianti antincendio o di estintori, sensori anti fumo, ecc.);
- modalità di accesso ai sistemi (esistenza di profili utenti e password personalizzate, modalità di accesso remoto ai sistemi, ecc.);
- procedure di creazione e gestione di profili utente (autorizzazioni per creazione, assegnazione e revoca, periodica rivisitazione dei profili, ecc.);
- gestione delle password (lunghezza minima, scadenza periodica, massimo numero di tentativi errati, ecc.);
- sistema antivirus utilizzato.

Anti disastro

- esistenza di:
  - ✓ un piano antidisastro e tutela dei dati;
  - ✓ procedure relative al backup dei dati;
  - ✓ location cassaforte ignifuga.

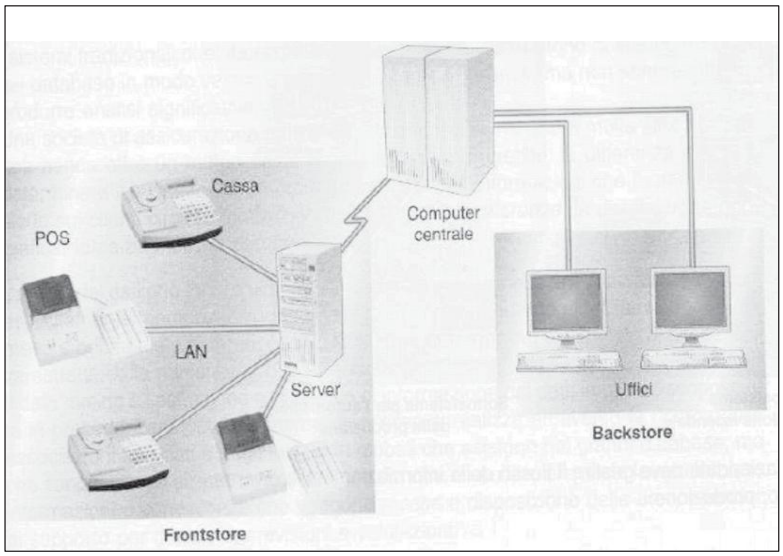
CHECK LIST
Sistemi Informativi Aziendali

1.	**Struttura Organizzativa della Direzione Sistemi Informativi**
	Quante persone lavorano all'interno della struttura.
	Esiste un mansionario della Direzione Sistemi Informativi che identifichi ruoli e responsabilità?
	Vi sono dei piani formativi per le persone dell'IT? Le risorse sono valutate periodicamente?
	Qual'è il livello di turnover della struttura?
	Le attività svolte dai fornitori di servizi sono regolate da procedure che ne vincolano l'operato al fine di assicurare la protezione dei dati e delle strutture IT?
	Sono definiti piani di lavoro a lungo/medio/breve termine, allineati con gli obiettivi strategici aziendali? Sono comunicati?
	Sono periodicamente comunicati al vertice aziendale e/o al board aggiornamenti sull'avanzamento delle attività di implementazione dei Sistemi Informativi?
	La definizione del budget di spesa IT è fatto partendo dai fabbisogni evidenziati dalle singole funzioni aziendali o dalla necessità di interventi di carattere tecnologico? Sono periodicamente monitorati il rispetto del budget e gli eventuali scostamenti?
2.	**Gestione Hardware**
	Esiste una mappatura dell'infrastruttura HW, contenente il numero ed il tipo di macchine utilizzate, dei sistemi operativi installati e quali utenti li utilizzano?
	Viene eseguita una manutenzione programmata dell'Hardware sulla base della criticità assegnata?
3.	**Gestione Software**
	Esiste una mappatura delle applicazioni chiave utilizzate, con la descrizione delle aree funzionali coperte ed il numero di utenti abilitati?
	Quali di queste sono gestite direttamente dalla struttura dei sistemi informativi e quali no?
	Esiste ed è documentata una configurazione HW e SW standard per i PC ed i portatili? Come è gestita l'installazione di updates o patches (push tecnology, manualmente)? È utilizzato un antivirus? È installato su ogni macchina? È periodicamente eseguito uno scan della rete? Tutti i download dalla rete sono analizzati dall'antivirus? Sono previsti dei piani di aggiornamento dei software più importanti?
4.	**Sicurezza fisica e logica dei Sistemi Informativi**
	Quali misure di sicurezza prevengono l'accesso di personale non autorizzato all'interno dei locali della sala macchine?
	Quali misure di sicurezza sono presenti nella sala macchine?
	Sono verificate periodicamente? Sono previsti dei specifici contratti di manutenzione? Sono tracciati gli interventi?
	L'accesso alla console della sala macchine è limitata al solo personale autorizzato? È permesso il controllo remoto della console? È possibile farlo da qualsiasi macchina collegata alla rete?
	Esiste un Log di verifica degli accessi alla console della sala macchine?
	Quali tipi di controllo degli accessi sono in essere (es. password, key card, ecc.)?
	Esiste una specifica policy che li regolamenta? È comunicata a tutto il personale dipendente e non che accede ai sistemi? Descrive le modalità di assegnazione, modifica e cancellazione?
	In particolare per gli utenti c.d. "Super User", ossia che hanno diritti di accesso privilegiati, sono monitorate le loro attività?
	Nel caso di dispositivi portatili (laptop, palmari, blackbarry, ecc.) come sono controllati gli accessi?
	È presente una policy della privacy?
	I dati critici sono archiviati centralmente o sono distribuiti?
5.	**Procedure di Backup**
	Esistono delle procedure scritte che dettagliano le modalità e la frequenza delle attività di backup?

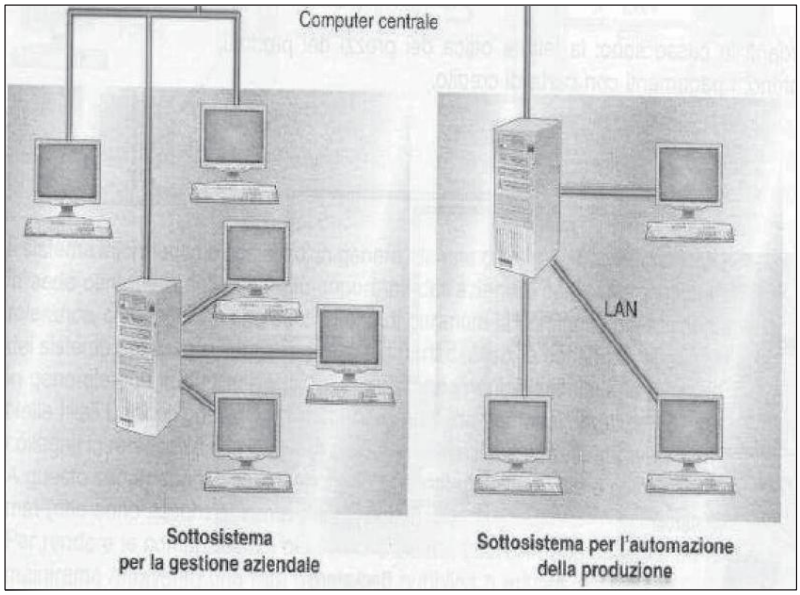
	Quanto spesso i backup incrementali e completi sono effettuati?
	Quali dati sono oggetto di backup? Sono effettuati anche backup dei file di sistema e degli applicativi?
	Dove sono conservate le cassette dei backup? Quanto spesso sono portate lontano dalla sede presso cui si trova la sala macchine?
	Sono effettuati dei test di recupero dei dati dai backup?
6.	**Business Continuity Plan**
	Esiste un piano di ripristino che prevede come gestire le situazioni di emergenza in caso di "disastro" o situazioni di crash di Hard Disk o malfunzionamenti della CPU del server per le applicazioni vitali per la continuazione dell'attività dell'azienda?
	Chi è responsabile della gestione e dell'aggiornamento del piano di ripristino? Esistono delle copie conservate al di fuori della sede?
	Le applicazioni (processi critici e dati relativi) sono identificate e ordinate secondo il grado di criticità dei processi di business da riattivare?
7.	**Procedure di Change Management applicativo**
	Esistono delle procedure che regolamentano le attività di sviluppo di nuove applicazioni o la manutenzione delle esistenti? Chi ne è responsabile dell'aggiornamento, diffusione e applicazione?
	Sono presenti diversi ambienti di lavoro (sviluppo, test, produzione) che devono essere utilizzati per i diversi step di rilascio delle applicazioni?
	Chi è responsabile del passaggio delle applicazioni tra i diversi ambienti di lavoro? Vi è un'adeguata separazione dei ruoli tra chi effettua lo sviluppo degli applicativi e chi li rilascia nell'ambiente di produzione?
	Gli end user sono coinvolti nel processo di test delle applicazioni al fine di certificarne l'accuratezza e validare il loro rilascio?
	Come sono assegnate le priorità per l'evasione delle richieste di modifiche delle applicazioni?
	È monitorato periodicamente lo stato di avanzamento delle modifiche sugli applicativi o la realizzazione di nuovi? È assegnata la responsabilità che tali attività siano completate nei tempi previsti?
	Esistono delle procedure di emergenza per l'esecuzione di interventi correttivi, al di fuori della normale procedura operativa di change management?
	Nell'attività di sviluppo sono utilizzati degli standard di riferimento riguardanti per esempio la naming convention o l'utilizzo del linguaggio di programmazione?
8.	**Accessi remoti**
	Quali tipologie di accesso remoto sono attive?
	Quali utenti utilizzano i diversi tipi di connessioni? Che procedure di autenticazione vengono utilizzate? Una volta connessi gli utenti sono soggetti alle stesse procedure di sicurezza previste per le connessioni in sede?
	Sono utilizzate tecnologie di criptaggio dei dati scambiati da remoto?
9.	**Internet**
	Quanti utenti possono accedere ad internet? La connessione è unicamente attraverso la rete o esistono anche connessioni di tipo dial up? In caso esistano connessioni dial up, prima del loro utilizzo viene effettuata la disconnessione dalla rete?
	Esiste una policy per l'utilizzo delle risorse internet? È distribuita a tutti gli utenti interessati?
	Vengono utilizzati dei software specifici per monitorare l'utilizzo delle risorse internet al fine di bloccare o prevenire la consultazione di siti con contenuti pornografici o che potrebbero portare attacchi alla sicurezza?
10.	**Outsourcing**
	Esistono dei servizi esternalizzati? Sono regolati da contratti?
	La selezione dei fornitori è fatta secondo quanto stabilito nelle procedure aziendali?

11.	**Rispetto di Leggi, regolamenti**
	Quali controlli sono attivi allo scopo di assicurare il rispetto di leggi, regolamenti, normative?
	Quali controlli sono attivi allo scopo di assicurare il rispetto dei principi contabili e delle norme che riguardano la tassazione?
	Quali controlli sono attivi per assicurare il rispetto di quanto previsto dalle policy o procedure interne?

→ Un esempio di SIA (Sistema Informativo Aziendale) di un'azienda commerciale potrebbe essere:



→ Un esempio di SIA (Sistema Informativo Aziendale) di un'azienda industriale, potrebbe essere



→Un esempio di rilevazione del sistema IT con rilievi ed azioni correttive concordate potrebbe essere:

Punto di attenzione	Possibili rischi	Priorità	Suggerimento	Resp.	Soluzione concordata
Gli addetti all'interno della Direzione Sistemi Informativi hanno in ambiente di produzione le massime autorizzazioni concesse dal sistema (Super User).	L'accesso non limitato degli addetti IT all'ambiente di produzione può consentire l'immissione di transazioni non autorizzate.	**A**	È necessario ridefinire i profili degli utenti della Direzione IT lasciando solo ad un numero molto limitato di utenti le massime abilitazioni in ambiente di produzione. È opportuno anche introdurre un controllo compensativo che consenta di monitorare le attività compiute dai Super User	Topolino A.	Sarà limitato al massimo il numero di "Super utenti". Entro 31/12/20xx
L'accesso logico a dati e programmi non sempre è ristretto agli identificativi appropriati per l'esecuzione degli specifici compiti assegnati. Inoltre sono emerse situazioni in cui la segregazione delle funzioni non è garantita.	La mancanza, in alcuni casi, di segregation of duties o di corrispondenza dei profili autorizzativi con la mansione ricoperta dall'utente sottopone l'azienda al rischio di accessi non autorizzati al sistema.	**A**	Si suggerisce di condurre tempestivamente un'attività di revisione completa di: - abilitazioni/disabilitazini utenze - assegnazioni profili ad autorizzazioni speciali - profilazione applicativa delle utenze. In merito a quest'ultima attività si suggerisce di seguire i seguenti passi: - predisporre liste di controllo/mappatura fra "profili informatici" dell'utente e la funzione aziendale ricoperta/mansioni svolte - sottoporla a verifica da parte dei diversi responsabili di aree	Minny A.	Sarà effettuata una review completa dei profili autorizzativi considerando: - abilitazioni/ - disabilitazioni utenti - corrispondenza delle abilitazioni alle mansione ricoperta - segregation of duties di transazioni critiche. Entro 30/06/20xx
Non viene svolta una revisione periodica delle autorizzazioni / disabilitazioni e dei profili. In particolar modo gli utenti che cambiano mansione mantengono le abilitazioni personali in precedenza a loro attribuite.	L'assenza di attività di revisione periodica delle autorizzazioni / disabilitazioni e dei profili determina innanzitutto rischi di disallineamento rispetto a quanto richiesto dalla normativa privacy e nel lungo periodo rende inefficace la segregazione dei compiti e delle responsabilità con conseguente rischio di accessi non autorizzati ai dati ed alle informazioni.	**A**	Vedi punto precedente.	Paperino A.	Vedi punto precedente Entro 30/06/20xx

Punto di attenzione	Possibili rischi	Priorità	Suggerimento	Resp.	Soluzione concordata
In caso di dimissione di un utente, la profilazione dello stesso non viene disabilitata ma cancellata.	La cancellazione di un utente dimesso non permette di risalire, attraverso la verifica degli eventuali log presenti, alla persona che ha eseguito determinate operazioni a sistema.	**M**	Si suggerisce di effettuare mensilmente un salvataggio delle abilitazioni, al fine di poter sempre rintracciare l'esecutore di operazioni all'interno del sistema.	Pippo A.	Saranno archiviate, con cadenza mensile, le informazioni relative alle abilitazioni degli utenti. Entro 31/12/20xx
Non è impostato un Time out dei lavori lasciati inattivi	Senza un meccanismo di Time Out, con obbligo di identificazione per proseguire i lavori, è possibile un accesso non autorizzato al sistema se un terminale è lasciato incustodito per un tempo abbastanza lungo (per esempio la pausa pranzo)		Implementare un meccanismo di time out utilizzando gli strumenti forniti dal Sistema Operativo.	Pluto A.	Sarà attivato il meccanismo di Time out presente in Windows, impostandolo a 30 minuti. Entro 31/12/20xx

Molto utile è ottenere ed allegare alla carte di lavoro un elenco degli applicativi utilizzati in azienda. Di seguito un esempio per l'azienda ABC SpA:

Applicativo	Funzionalità	HW	Liguaggio	Anno	Fornitore	Manutenzione
Diapason ModuliFM e FA	Contabilità Generale e Cespiti	BMI ZSeries	Cobol	1986	Gruppo XYZ	Esterna
CDF	Ciclo attivo	BMI ZSeries	Cobol	1988	Sviluppo interno	Interna
SIA	Ciclo passivo	BMI ZSeries	Cobol	1990	Sviluppo interno	Interna
MAG/PROD	Ciclo magazzino e produzione	BMI ZSeries	Cobol	1989	Sviluppo interno	Interna
Tieffe	Tesoreria	Server Win	-	1988	Gruppo ABC	Esterna
Ecc.	*Ecc.*	*Ecc.*	*Ecc.*	*Ecc.*	*Ecc.*	*Ecc.*

Riguardo poi la sicurezza fisica, bisognerà verificare che l'edificio aziendale sia dotato di adeguati sistemi di antintrusione, con la sala macchine protetta con sistema antincendio a gas estinguente.

Una possibile check list potrebbe essere:

1. Controlli antintrusione
2. Sistema antincendio
3. Sensori temperatura
4. Sensori fumo
5. Sensori acqua
6. Pavimento sospeso
7. Pareti e soffitto antincendio
8. Estintori
9. Condizionamento
10. Generatore corrente
11. Luci di emergenza.

Si può chiudere la "chiacchierata" con la richiesta di eventuali diagrammi di flusso "flow chart" già esistenti in azienda e che ci evita di perdere tempo per prepararli ed avere un quadro più chiaro dell'impianto informatico dell'azienda e la richiesta se ci sono progetti in corso di attuazione e quindi sostituzione/sviluppi di quelli esistenti che possono comportare cambiamenti a breve termine significativi su tutto l'impianto informativo aziendale.

> *Quanto maggiori saranno i volumi delle transazioni tanto più bisognerà delegare più controlli possibili al sistema computerizzato.*