Gestione della sicurezza delle informazioni

L'implementazione del sistema e le procedure di monitoraggio e controllo (*audit*)

a cura dell'**Ing. Francesco Amendola** – Nextel Italia s.r.l.

Profilo del relatore

Francesco Amendola è laureato in Ingegneria Elettronica con Lode presso l'Università degli Studi di Roma Tre ed è un laureato del Collegio Universitario "Lamaro-Pozzani".

Attualmente ricopre la carica di *IT Security Specialist* all'interno della Nextel Italia s.r.l. – www.nextel.it – società multinazionale di telecomunicazioni, specializzata nella progettazione di sistemi VoIP.

Gestisce anche un sito personale all'indirizzo www.ingamendola.com, dove sono disponibili articoli e presentazioni in materia di sicurezza informatica e protezione dei dati personali.

Sommario

1. Da BS7799-2 a ISO 27001:2005

2. Metodologie di *auditing*

3. Conclusioni

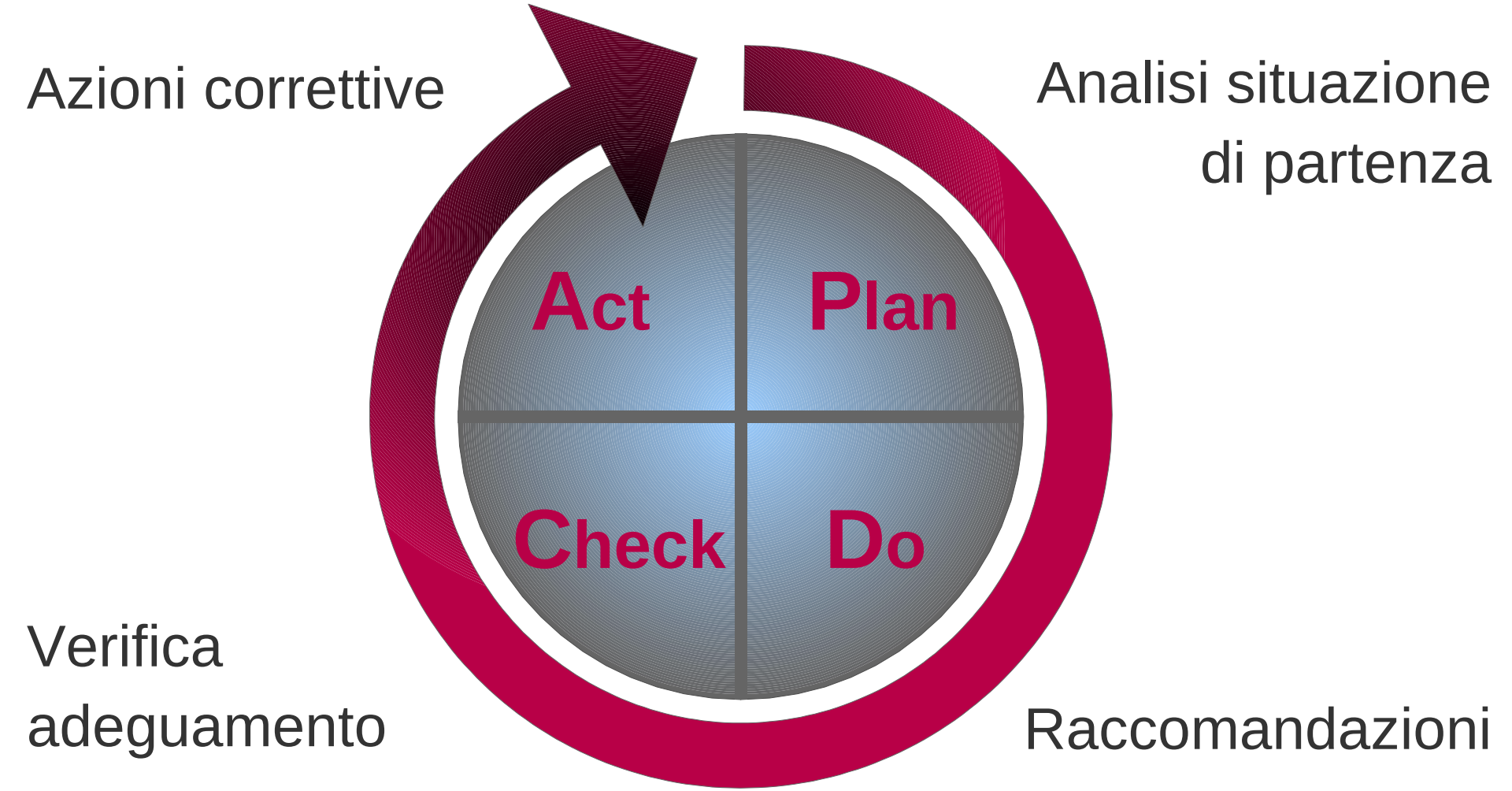
- **Migrazione della certificazione**
  - Le variazioni di contenuti sono limitate
    - da 36 obiettivi di controllo a 39
    - da 127 controlli a 133
  - L'aspetto più importante che si introduce con l'emanazione della ISO 27001:2005 è il riconoscimento internazionale di uno standard localizzato
    - ad oggi il maggior numero di certificazioni lo si riscontra in Regno Unito e Giappone

- **Suite ISO 27000**
  - ISO 27000 Fondamenti e terminologia dei SGSI
  - ISO 27002 Tecniche di sicurezza SGSI – codice di prassi (recepirà la ISO 17799:2005)
  - ISO 27003 Linee guida per l'implementazione dei SGSI
  - ISO 27004 Metrica e misurazione SGSI
  - ISO 27005 Risk Management nei SGSI
  - ISO 27006 Continuità delle operazioni e servizi di ripristino (Disaster Recovery) SGSI

- **Aspettative future**
  - L'aggiornamento dell'ISO 17799 e l'emanazione dell'ISO 27001, entrambi del 2005, nascono dall'aspettativa di diffondere, nei prossimi anni, la cultura della gestione della sicurezza delle informazioni su scala globale e non relegata esclusivamente alle aziende che già fanno sicurezza
  - Ampliamento dei mercati non solo geografici, ma anche tipologici, volendo penetrare in tutti i settori di attività industriale e commerciale

- **Contenuti dell'ISO 27001:2005**
  - Integrazione ed allineamento con le altre norme ISO che specificano i requisiti di un modello di Sistema di Gestione per la Qualità (ISO 9001:2000) e per l'Ambiente (ISO 14001:2004)
  - Modello PDCA
    - Pianificazione
    - Implementazione
    - Controllo
    - Azioni migliorative

Da BS7799-2 a ISO 27001:2005



- **Applicabilità dell'ISO 27001:2005**
  - La norma si applica a tutti i tipi di organizzazione, senza distinzione sul tipo, dimensione e natura
    - Imprese commerciali
    - Enti e agenzie governative
    - Organizzazioni no-profit
    - ....
  - I controlli sono mutuati direttamente dalla ISO 17799:2005, futura ISO 27002

- **Definizioni presenti nell'ISO 27001:2005**
  - Le definizioni sono aggiornate alle nuove norme ISO 13335-1:2004 (Management of information and communications technology security) e ISO 18044:2004 (Information security incident management)
  - Le definizioni sono state riviste e ampliate in modo da evitare il più possibile incomprensioni nella loro interpretazione

- **Requisiti generali**
  - L'organizzazione deve pianificare, implementare, organizzare, controllare, revisionare, gestire, e migliorare un SGSI documentato all'interno del contesto delle attività generali dell'organizzazione e dei rischi che si trova ad affrontare
  - L'approccio per processi che deve essere adottato si basa sul ciclo di Deming (PDCA)

- **Stabilire il SGSI**
  - L'organizzazione deve definire il campo di applicazione ed i confini del SGSI, in termini di caratteristiche dell'attività,dell'organizzazione stessa, del sito, dei beni e della tecnologia, includendo i dettagli e le giustificazioni a supporto di qualsiasi esclusione di controlli dal campo di attività
  - Ogni esclusione di controlli deve essere giustificata e occorre provare e dimostrare che il rischio associato è stato accettato da una persona responsabile

- **Stabilire il SGSI**
  - La definizione della *policy* del SGSI deve, tra l'altro:
    - essere allineata con il contesto di gestione strategica del rischio all'interno dell'organizzazione dove verrà posto in essere il SGSI
  - Viene fatto notare come la *policy* del SGSI rientri nella più generale *policy* per la sicurezza delle informazioni

- **Stabilire il SGSI**
  - L'organizzazione deve definire l'approccio che intende adottare nella valutazione del rischio
    - Dovrà dunque identificare un metodologia di valutazione del rischio che sia adatta per il SGSI
    - Dovrà inoltre sviluppare dei criteri di accettazione del rischio ed individuare i livelli di rischio ritenuti accettabili
  - La metodologa prescelta deve garantire che i risultati siano confrontabili e riproducibili
  - Viene richiamata la norma ISO 13335-3 (Techniques for the management of IT Security)

- **Stabilire il SGSI**
  - L'organizzazione, per poter identificare i rischi, deve anzitutto identificare i beni da proteggere all'interno del campo di attività del SGSI e contestualmente i *proprietari* di tali beni
  - Per proprietario si intende colui o coloro i quali responsabilità gestionali nel controllo della produzione, sviluppo, manutenzione, utilizzo e sicurezza del bene in questione
  - Per proprietario non si intende dunque colui o coloro i quali vantano un diritto di proprietà sul bene

- **Stabilire il SGSI**
  - L'organizzazione deve analizzare e ponderare i rischi, non già solamente valutarli
    - Stimare l'impatto aziendale sull'intera organizzazione (già danno aziendale) che potrebbe derivare da una falla nella sicurezza, considerando le conseguenze di una mancanza di riservatezza, integrità e disponibilità del bene

- **Stabilire il SGSI**
  - L'organizzazione deve selezionare gli obiettivi di controllo ed i controlli per il trattamento del rischio
    - La selezione e l'implementazione deve avvenire nel rispetto dei requisiti individuati dalla valutazione e dal processo di trattamento del rischio
    - La selezione deve considerare dei criteri per l'accettazione del rischio, così come i requisiti legali, legislativi e contrattuali
    - L'Annex A non è esaustivo, per cui è possibile selezionare controlli ed obiettivi in esso non catalogati

- **Stabilire il SGSI**
  - L'organizzazione deve ottenere dalla Direzione l'approvazione del rischio residuo proposto
  - L'organizzazione deve ottenere dalla Direzione l'autorizzazione ad implementare e gestire il Sistema di Gestione per la Sicurezza delle Informazioni

- **Stabilire il SGSI**
  - L'organizzazione deve predisporre una una Dichiarazione di Applicabilità (SoA – *Statement of Applicability*) contenente:
    - gli obiettivi di controllo ed i controlli selezionati, motivandoli
    - gli obiettivi di controllo ed i controlli già implementati
    - l'esclusione degli obiettivi di controllo e dei controlli dell'Annex A e la giustificazione dell'esclusione
  - La DdA fornisce un riepilogo delle decisione relative al trattamento dei rischi
  - La giustificazione delle esclusioni fornisce una verifica incrociata che nessun controllo sia stato omesso

- **Implementazione e messa in esercizio del SGSI**
  - L'organizzazione deve:
    - formulare un piano di trattamento del rischio che identifichi le opportune azioni della Direzione, le risorse, le responsabilità e le priorità nella gestione dei rischi legati alla sicurezza delle informazioni
    - Definire come misurare l'efficacia dei controlli selezionati e specificare come queste misure vengono usate per valutare il controllo di efficacia per produrre risultati confrontabili e riproducibili

- **Implementazione e messa in esercizio del SGSI**
  - La misura dell'efficacia dei controlli consente alla Direzione ed ai collaboratori di determinare in che misura i controlli raggiungono gli obiettivi di controllo pianificati
  - L'organizzazione deve gestire le operazioni del Sistema di Gestione per la Sicurezza delle Informazioni
  - L'organizzazione deve gestire le risorse del Sistema di Gestione per la Sicurezza delle Informazioni

- **Monitorare e riesaminare il SGSI**
  - L'organizzazione deve:
    - eseguire procedure di monitoraggio e riesame
    - eseguire controlli per identificare tempestivamente le violazioni e gli incidenti per la sicurezza tentati o portati a termine con successo
    - effettuare riesami periodici dell'efficacia del SGSI
    - misurare l'efficacia dei controlli per verificare che i requisiti di sicurezza siano stati rispettati

- **Monitorare e riesaminare il SGSI**
  - L'organizzazione deve:
    - riesaminare le valutazioni del rischio ad intervalli specificati, i rischi residui ed i livelli di rischi ritenuti accettabili, considerando le variazioni all'efficacia dei controlli implementati e gli eventi esterni, quali il cambiamento del contesto normativo, dei vincoli contrattuali e del contesto sociale

- **Monitorare e riesaminare il SGSI**
  - L'organizzazione deve:
    - condurre *audit* interni ad intervalli pianificati
  - Gli *audit* interni, chiamati anche *audit* di prima parte, sono condotti da o a favore dell'organizzazione stessa per scopi interni
  - L'organizzazione deve inoltre:
    - Effettuare il riesame del SGSI da parte della Direzione con regolarità, identificando i miglioramenti del sistema

- **Monitorare e riesaminare il SGSI**
  - L'organizzazione deve:
    - aggiornare i piani di sicurezza, per considerare i riscontri dalle attività di monitoraggio e riesame
- **Mantenere e migliorare il SGSI**
  - L'organizzazione deve regolarmente:
    - comunicare le azioni ed i miglioramenti a tutte le parti interessate con un livello di dettaglio appropriato rispetto alle circostanze, concordando il modo in cui procedere

- **Requisiti documentali**
  - La documentazione deve includere le registrazioni delle decisione della Direzione, assicurare che le azioni sono rintracciabili rispetto alle decisioni ed alle politiche della Direzione, assicurare ancora che i risultati registrati siano riproducibili
  - La documentazione di un SGSI deve contenere:
    - documenti che dichiarino la politica del SGSI e gli obiettivi
    - il campo di applicazione del SGSI

- **Requisiti documentali**
  - La documentazione di un SGSI deve contenere:
    - procedure e controlli a supporto del SGSI
    - una descrizione della metodologia adottata per la valutazione dei rischi
    - procedure documentate necessarie all'organizzazione per assicurare l'effettiva pianificazione, messa in esercizio e controllo dei suoi processi di sicurezza delle informazioni e per descrivere come misurare l'efficacia dei controlli

- **Controllo dei documenti**
  - I documenti richiesti dal SGSI devono essere protetti e controllati. Una procedura documentata deve essere stabilita per definire le azioni della Direzione necessarie ad:
    - assicurare che le versioni rilevanti dei documenti applicabili siano disponibili nei luoghi di utilizzo
    - assicurare che che i documenti siano disponibili per coloro i quali ne abbiano necessità e vengano trasferiti, immagazzinati ed infine dismessi in accordo con le procedure applicabili alla loro classificazione

- **Controllo delle registrazioni**
  - Le registrazioni devono essere effettuate e conservate alfine di fornire delle prove oggettive di conformità ai requisiti e l'effettivo funzionamento del SGSI. Esse devono essere protette e controllate. Il SGSI deve considerare ogni requisito rilevante in ambito normativo, regolamentare o relativo a vincoli contrattuali. Le registrazioni devono conservarsi leggibili, intelligibili, identificabili e recuperabili

- **Controllo delle registrazioni**
  - I controlli necessari per l'identificazione, la conservazione, la protezione, il recupero, il tempo di conservazione e la disposizione delle registrazioni devono essere implementati e documentati
  - Devono essere mantenute registrazioni della *performance* del processo e di tutte le occorrenze di incidenti per la sicurezza significativi collegati al SGSI
  - Un esempio di registrazione è il registro dei visitatori o i rapporti degli *audit* o i moduli di autorizzazione all'accesso

- **Responsabilità della Direzione**
  - La Direzione deve fornire prove oggettive del proprio impegno nella pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI:
    - istituendo una politica del SGSI
    - assicurando che gli obiettivi ed piani del SGSI siano conseguiti

- **Responsabilità della Direzione**
  - La Direzione deve fornire prove oggettive del proprio impegno:
    - fornendo risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI
    - stabilendo i criteri per l'accettazione del rischio e per i livelli di rischio accettabili
    - assicurando che vengano effettuati *audit* interni al SGSI

- **Gestione delle risorse**
  - L'organizzazione deve determinare e fornire le risorse necessarie a:
    - pianificare, implementare, organizzare, controllare, revisionare, gestire e migliorare il SGSI

- **Gestione delle risorse**
  - L'organizzazione deve assicurare che tutto il personale, a cui siano state affidate responsabilità definite nel SGSI, abbia le competenze ad eseguire i compiti assegnati:
    - fornendo addestramento o intraprendendo altre azioni, quali l'impiego di personale competente, atte a soddisfare le proprie necessità
    - valutando l'efficacia delle azioni intraprese

- ***Audit* interni al SGSI**
  - L'organizzazione deve condurre audit interni ad intervalli pianificati
  - La Direzione responsabile dell'area sottoposta ad *audit* deve assicurare che le azioni per eliminare le non conformità rilevate e le loro cause vengano prese senza ritardi. Le azioni di *follow-up* devono includere la verifica delle azioni intraprese ed il rapporto dei risultati della verifica
  - Un valido ausilio proviene dalla ISO 19011:2003 (*Guidelines for quality and/or environmental management systems auditing*)

- **Riesame della Direzione**
  - La Direzione deve riesaminare il SGSI dell'organizzazione ad intervalli pianificati – comunque almeno una volta all'anno – per assicurare la sua continua adattabilità, adeguatezza ed efficacia. Questo riesame deve comprendere opportunità di valutazione del miglioramento e della necessità di cambiamenti al SGSI, inclusi la politica e gli obiettivi della sicurezza delle informazioni. I risultati del riesame della Direzione devono essere chiaramente documentati e registrtati

- **Riesame della Direzione**
  - Gli output del riesame della Direzione devono includere qualsiasi decisione o azione relativa:
    - all'aggiornamento del piano di valutazione e trattamento del rischio
    - alla modifica di procedure e controlli che impattino sulla sicurezza delle informazioni, quali ad esempio i vincoli contrattuali o i livelli di rischio e/o i criteri per l'accettazione del rischio
    - al miglioramento della misura dell'efficacia dei controlli

- **Miglioramento del SGSI**
  - L'organizzazione deve migliorare continuamente l'efficacia del SGSI attraverso l'utilizzo della politica e degli obiettivi della sicurezza delle informazioni, dei risultati degli *audit*, dell'analisi degli eventi monitorati, di azioni preventive e correttive, infine del riesame della Direzione

- **Miglioramento del SGSI**
  - L'organizzazione deve adottare azioni per eliminare le cause delle non conformità ai requisiti del SGSI al fine di prevenirne la ricorrenza.
  - La procedura documentata per le azioni correttive deve definire i requisiti per:
    - identificare le non conformità
    - determinare le cause delle non conformità
    - valutare la necessità di azioni che assicurino la mancata ricorrenza delle non conformità

- **Miglioramento del SGSI**
  - L'organizzazione deve adottare azioni per eliminare le cause di potenziali non conformità ai requisiti del SGSI al fine di prevenirne l'occorrenza. Le azioni preventive intraprese devono essere commisurate all'impatto del potenziale problema
  - La procedura documentata per le azioni preventive deve:
    - identificare potenziali non conformità e le loro cause
    - valutare la necessità di azioni atte a prevenire l'occorrenza di non conformità

- **Miglioramento del SGSI**
  - L'organizzazione deve identificare i rischi variati ed i requisiti di azioni preventive, focalizzando l'attenzione sui rischi variati più significativi
  - La priorità delle azioni preventive deve essere determinata basandosi sui risultati della valutazione del rischio
  - Spesso le azioni preventive risultano più onerose di quelle correttive

Da BS7799-2 a ISO 27001:2005

- **Annex**
  - ANNEX A (Obiettivi di controllo e controlli)
    - Gli obiettivi di controllo ed i controlli sono stati allineati alla ISO 17799: 2005
  - ANNEX B (Guida all'uso → Principi OECD)
    - Mantenuta solo la tabella B.1 della BS7799-2
    - Il resto è previsto che venga utilizzato nello sviluppo della ISO 27003 (*Linee guida per l'implementazione di SGSI*)
  - ANNEX C (Corrispondenza con le altre norme)
    - E' stato allineato alla ISO 9001:2000 e ISO 14001:2004
  - ANNEX D (Cambi alla numerazione interna)
    - E' stato eliminato

Sommario

1. Da BS7799-2 a ISO 27001:2005

2. Metodologie di *auditing*

3. Conclusioni

Metodologie di *auditing*

- **Definizioni**
  - ISO 19011:2003
    - *audit*, verifica ispettiva: processo sistematico, indipendente e documentato per ottenere evidenze dell'*audit* e valutare con obiettività, al fine di stabilire in quale misura i criteri dell'*audit* sono stati soddisfatti
  - ISACA
    - IS *audit*: processo di raccolta e valutazione di elementi oggettivi per determinare le modalità con cui l'*Information System* aziendale e le relative risorse sono salvaguardate ed avere una ragionevole certezza che siano garantiti

Metodologie di *auditing*

- ***Audit* sul sistema**
  - ISO 27001:2005
    - *audit* sui processi critici per la sicurezza delle informazioni, non si considerano tutti i processi aziendali nella loro generalità
  - COBIT 4.0
    - *audit* sui processi IT e sugli obiettivi di controllo di tali processi, per garantire che la tecnologia sia correttamente gestita e che risulti di supporto a tutti i processi aziendali

Metodologie di *auditing*

- **Linee guida per gli *audit***
  - Adeguata pianificazione prima di avviare il processo di *audit*
  - L'organizzazione deve preventivamente valutare il rischio complessivo relativamente all'area sottoposta ad *audit*
  - L'organizzazione deve preventivamente predisporre un programma di *audit* comprendente gli obiettivi e le procedure per conseguire questi obiettivi
  - Il processo di *audit* prevede che gli IS *auditor* raccolgano evidenze oggettive, valutino la robustezza o meno dei controlli basandosi sulle evidenze raccolte, infine predispongano un rapporto dell'*audit* in cui riportare alla Direzione in maniera oggettiva i risultati del processo

Metodologie di *auditing*

- **Metodologia CISA per gli IS *audit***
  - Fase 1 (Oggetto dell'*audit*)
    - Individuare l'area da sottoporre ad *audit*
  - Fase 2 (Finalità dell'*audit*)
    - Individuare le finalità del processo di *audit* all'interno dell'oggetto
  - Fase 3 (Campo di applicazione dell'*audit*)
    - Individuare gli specifici sistemi, funzioni o unità dell'organizzazione da considerare nell'*audit*

Metodologie di *auditing*

- **Metodologia CISA per gli IS *audit***
  - Fase 4 (Pianificazione preventiva dell'*audit*)
    - Identificazione delle capacità tecniche e delle risorse richieste
    - Identificazione delle sorgenti di informazione per test e riesami, quali diagrammi di flusso, politiche, norme tecniche, procedure e rapporti di precedenti *audit*
    - Identificazione dei luoghi e delle infrastrutture da sottoporre a *audit*

Metodologie di *auditing*

- **Metodologia CISA per gli IS *audit***
  - Fase 5 (Procedure di *audit* e passi di raccolta dati)
    - Identificazione e selezione dell'approccio da dare all'*audit* per verificare e testare i controlli
    - Identificazione di un lista di persone da intervistare
    - Identificazione ed ottenimento dei documenti dipartimentali, quali politiche, norme tecniche e linee guida da revisionare
    - Sviluppo di strumenti di *audit* e metodologie per testare e verificare i controlli

Metodologie di *auditing*

- **Metodologia CISA per gli IS *audit***
  - Fase 6 (Procedure per valutare i test e revisionare i risultati)
    - Dipendono intrinsecamente dall'organizzazione soggetta ad *audit*
  - Fase 7 (Procedure per comunicare con la Direzione)
    - Dipendono intrinsecamente dall'organizzazione soggetta ad *audit*

Metodologie di *auditing*

- **Metodologia CISA per gli IS *audit***
  - Fase 8 (Procedure per valutare i test e revisionare i risultati)
    - Identificazione delle procedure di *follow-up*
    - Identificazione delle procedure per valutare e testare l'efficacia e l'efficienza operativa
    - Identificazione delle procedure per testare i controlli
    - Riesame e valutazione della validità dei documenti, delle politiche e delle procedure

Sommario

1. Da BS7799-2 a ISO 27001:2005

2. Metodologie di auditing

3. Conclusioni

Conclusioni

- **Contesto normativo**
  - Decreto Legislativo 8 giugno 2001, n. 231
    - *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*
  - Confindustria
    - *Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. n. 231/2001*

Conclusioni

- **Linee Guida di Confindustria**
  - *“La legge prevede l'adozione del modello di organizzazione, gestione e controllo in termini di facoltatività e non di obbligatorietà, tuttavia la mancata adozione del modello espone l'ente alla responsabilità per gli illeciti realizzati da amministratori e dipendenti. L'adozione del modello diviene, pertanto, di fatto obbligatoria se si vuole beneficiare dell'esimente”*

Conclusioni

- **Linee Guida di Confindustria**
  - Lo schema seguito nell'elaborazione delle Linee Guida per la costruzione dei modelli riprende i processi di *risk assessment* e *risk management* normalmente attuati nelle imprese e consiste:
    - *nell'identificazione dei rischi in relazione ai reati che possono essere commessi;*
    - *nella progettazione di un sistema di controllo preventivo, realizzato attraverso la costruzione di un sistema organizzativo adeguato e la procedimentalizzazione di determinate attività;*
    - *nell'adozione di un codice etico e di un sistema di sanzioni disciplinari applicabili in caso di mancato rispetto delle misure previste dal modello, al fine di conservarne l'effettività;*
    - *nell'individuazione dei criteri per la scelta di un organismo di controllo, interno all'impresa, dotato delle funzioni necessarie, che dovrà vigilare sull'efficacia, sull'adeguatezza e sull'applicazione e rispetto del modello.*

Riferimenti

- ISO 27001:2005 – note informative e requisiti per la transizione degli *auditor* certificati IRCA secondo lo schema SGSI
  - http://www.irca.org/
- CISA Review Manual 2006
  - http://www.isaca.org/bookstore
- COBIT Security Baseline
  - http://www.isaca.org/
- Linee Guida Confindustria
  - http://www.confindustria.it/

Grazie per l'attenzione!

info@ingamendola.com www.ingamendola.com