Newsletter n. 6 – 2013
Novembre 2013

AUDIT DEI SISTEMI DI GESTIONE ISO/IEC 27001 E ISO/IEC 20000-1: PECULIARITÀ, APPROCCI POSSIBILI, INTEGRAZIONE, FORMAZIONE DEGLI AUDITOR

Care Colleghe, Cari Colleghi,

prosegue la nuova serie di Newsletter legati agli Schemi di Certificazione di AICQ SICEV. Questa volta la "pillola formativa" si riferisce *agli Audit dei Sistemi di Gestione ISO/IEC 27001 e ISO/IEC 20000-1: peculiarità, approcci possibili, integrazione, formazione degli Auditor* che mi ha messo a disposizione il collega e amico Fabrizio Cirilli, che in ambito AICQ SICEV, opera come Commissario di Esame e come Auditor Certificato per lo Schema ISO/IEC 20000-1. Troverete i Suoi riferimenti, in calce all'articolo, che Vi consentiranno di contattarlo qualora necessitiate di chiarimenti e ulteriori informazioni.
Buona lettura e buon lavoro.

Roberto De Pari
Direttore AICQ SICEV

Know how in pillole:

AUDIT DEI SISTEMI DI GESTIONE ISO/IEC 27001 E ISO/IEC 20000-1: PECULIARITÀ, APPROCCI POSSIBILI, INTEGRAZIONE, FORMAZIONE DEGLI AUDITOR

Le recenti modifiche alle norme per la gestione degli audit (ISO 19011 e ISO/IEC 17021), unitamente alla sempre più frequente integrazione dei Sistemi di Gestione, pone gli Auditor di fronte a competenze via via più articolate e ad attività di audit sempre più specifiche. A questo dobbiamo aggiungere l'atipicità delle norme ISO/IEC 27001 e ISO/IEC 20000-1 che hanno addirittura sviluppato: una norma per la gestione integrata dei due sistemi, 3 linee guida per la conduzione degli audit specifici per i SGSI e generato una serie di altri fattori che impattano sulla formazione ed addestramento degli Auditor, siano essi interni o esterni.

Questa newsletter, tratta da un articolo di Fabrizio Cirilli, pubblicato sul n. 4/2013 della rivista "Qualità" di AICQ, prova a dare un quadro di riferimento a supporto dei colleghi che iniziano questo percorso o che intendono ampliare le loro conoscenze specifiche.

Le innovazioni introdotte dalla ISO/IEC 17021:2011
Le recenti innovazioni alla ISO/IEC 17021 hanno avviato un processo di aggiornamento che coinvolge tutti gli Auditor, indipendentemente dallo schema sul quale operano.

Qui ci limitiamo a focalizzare l'attenzione sugli impatti che tale aggiornamento induce sugli Auditor dei Sistemi di Gestione per la Sicurezza delle Informazioni - in breve SGSI.

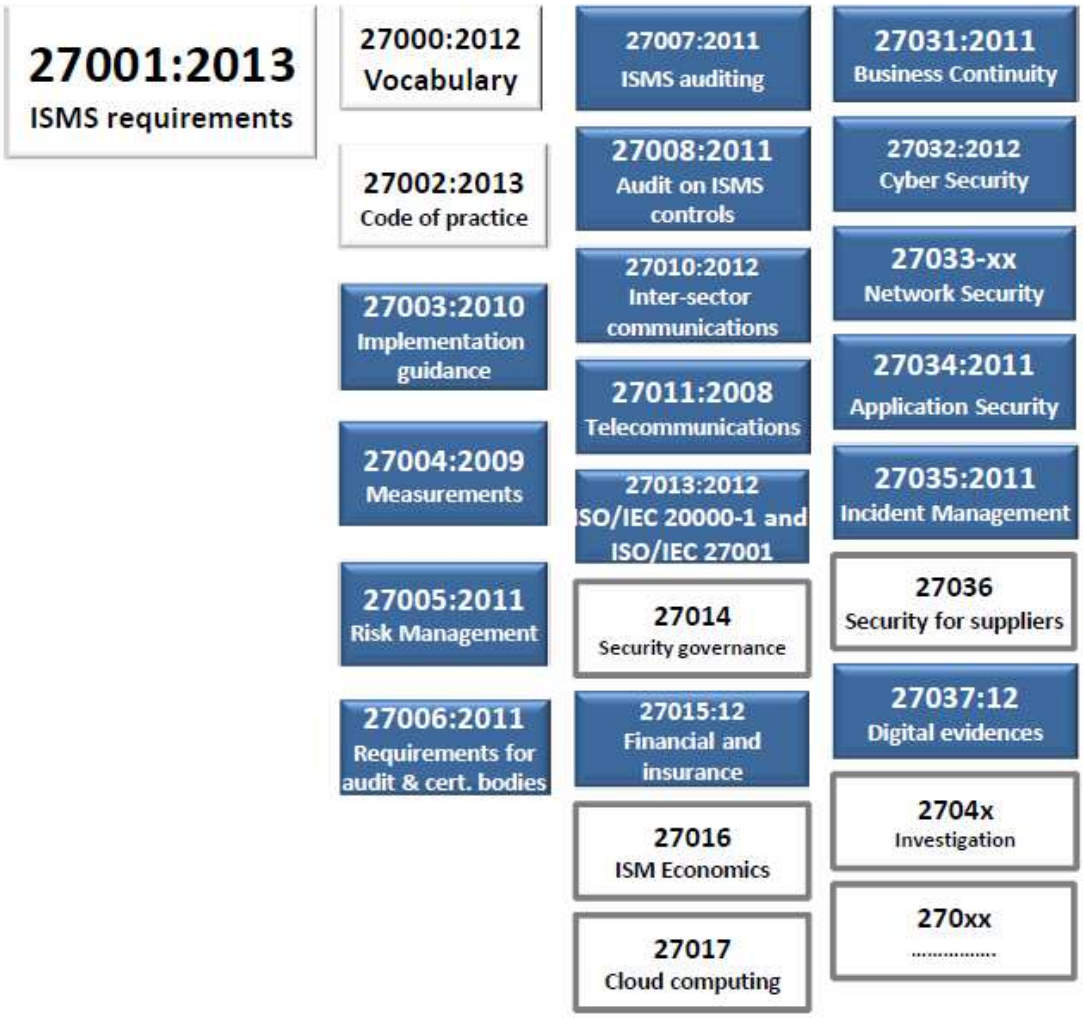
La principale innovazione per quanto concerne gli Auditor riguarda il concetto di "aree di competenza"introdotto al requisito 7.1 della ISO/IEC 17021:2011. In buona sostanza viene avviato un nuovo processo di qualificazione degli Auditor non tanto su settori di competenza (EA/NACE) quanto invece sulle effettive competenze nello schema specifico, intese come competenze operative e lavorative maturate sui temi dello schema specifico.

Facciamo un esempio semplice ma efficace: per verificare processi e servizi inerenti il "cloud computing" l'Auditor dovrà avere dimostrare di avere esperienza lavorativa diretta nei temi del "cloud computing". Quindi l'esperienza costruita sulla base dei soli audit non dovrebbe più essere utilizzata.

Questo approccio innalza in modo decisivo l'efficacia degli audit ma d'altra parte limita anche molto l'utilizzazione degli Auditor alle sole aree di competenza censite e dimostrabili. Nel campo dell'ICT questo potrebbe fornire interessanti opportunità di lavoro ai giovani Auditor,soprattutto nel campo delle nuove tecnologie, aprendo così un nuovo ciclo vitale per gli audit delle Organizzazioni.

Ciascun Auditor, oltre all'aggiornamento derivante sui processi descritti nella ISO/IEC 17021:2011, dovrà quindi cimentarsi nella produzione delle evidenze necessarie a dimostrare la copertura delle aree di competenze definite dagli Organismi di Certificazione dei Sistemi di Gestione per i quali opera.

La famiglia delle ISO/IEC 270xx
La famiglia degli standard ISO/IEC 270xx è in continua espansione, alla data di redazione di questa newsletter la struttura è sostanzialmente quella descritta nella figura seguente:



Su sfondo scuro gli standard già pubblicati. Su sfondo chiaro gli standard in fase di revisione e/o in fase di scrittura.

È significativo l'aggiornamento della ISO/IEC 27001:2013 e della ISO/IEC 27002:2013, avvenuto in anticipo rispetto alla pianificazione, il 25 settembre 2013.

Linee guida di particolare interesse per gli Auditor dei SGSI
Per quanto concerne gli Auditor dei SGSI, vi sono alcune delle linee guida della famiglia ISO/IEC 270xx che possono ricoprire un interesse specifico e che costituiscono un valido strumento di supporto per le attività di audit.

La ISO/IEC 27000
Questo standard contiene la terminologia ed il glossario per i SGSI. Non può quindi mancare nel bagaglio delle competenze di un Auditor! Spesso, infatti, i fraintendimenti e le errate interpretazioni di un termine conducono i Sistemi di Gestione, e di conseguenza gli audit, verso situazioni complesse, solo perché un termine utilizzato da una Organizzazione per il proprio SGSI non ha esattamente lo stesso significato inteso

dall'Auditor. Errori di traduzione, similitudini, modi di dire possono influenzare in modo rilevante un audit quando la terminologia non viene ben chiarita o riferita a standard di riferimento come questo.

La ISO/IEC 27002
Ancora oggi è uno degli standard meno compresi nel mondo della certificazione. Lo scopo di questo standard è fornire informazioni per espandere quanto definito nell'appendice A della ISO/IEC 27001 e supportare le Organizzazioni nella realizzazione di contromisure efficaci per rispondere ai rischi identificati.

Non è uno standard auditabile né certificabile, ma nasce con lo scopo di supportare le Organizzazioni nella identificazione e realizzazione delle "contromisure" (o controlli) utili per il trattamento dei rischi identificati. Da notare che l'applicazione di tutte le contromisure definite nella ISO/IEC 27002 non necessariamente trasformerebbe un'Organizzazione in una Organizzazione sicura.

L'ordine e la numerazione dei paragrafi di questo standard riprende esattamente quello dell'allegato A della ISO/IEC 27001 per favorirne l'allineamento e la fruibilità.

La ISO/IEC 27006
Lo standard ISO/IEC 27006 nasce per gli Organismi di Certificazione ed accreditamento. Infatti l'obiettivo di questo standard è integrare la ISO/IEC 17021 per quanto concerne la gestione degli audit sui SGSI.

Le appendici di questo standard (o annex), tutte di carattere informativo, sono però di particolare utilità ed efficacia anche per gli audit di prima e seconda parte.

La ISO/IEC 27007
Vista la complessità dei SGSI e delle difficoltà nella gestione degli audit la nascita di uno standard destinato a guidare le Organizzazioni nell'audit del proprio SGSI appare del tutto naturale. Questo standard ha infatti l'obiettivo di supportare le Organizzazioni nella gestione e conduzione degli audit interni sul SGSI, unita a quanto descritto nella ISO 19011 diventa infatti un modello perfetto per la formazione degli Auditor interni e per la gestione degli audit interni.

La struttura dello standard ricalca quello della ISO 19011, cui si ispira, con specifiche "verticalizzazioni" per i SGSI. Di particolare interesse quanto descritto, a livello esemplificativo, nell'appendice A che contiene esempi pratici per l'efficace gestione e conduzione di audit su particolari punti della ISO/IEC 27001 e del SGSI. Dunque una norma che non dovrebbe mancare in un'Organizzazione interessata all'ottenimento di audit interni efficaci e volti al miglioramento del proprio SGSI!

La ISO/IEC TR 27008
Ecco uno standard veramente interessante! Il fatto che si tratti di un Technical Report ne indica anche la natura specifica ed estremamente tecnica dei contenuti. Ma cosa contiene in effetti? Contiene indicazioni per la valutazione dell'attuazione e del funzionamento dei controlli (o contromisure) adottate in un SGSI, compresala verifica della conformità tecnica.

Dunque uno strumento assolutamente complementare a quanto visto nell'appendice D della ISO/IEC 27006 e a quanto descritto nella ISO/IEC 27007.

Linee guida di particolare interesse per gli Auditor dei SGSM
Per quanto concerne gli Auditor dei SGSM abbiamo almeno due standard che rivestono un particolare interesse e che supportano LA ISO/IEC 20000-1:2011.

La ISO/IEC 20000-2:2012
Una guida alla corretta realizzazione (e verifica) della ISO/IEC 20000-1. Ogni requisito della ISO/IEC 20000-1 viene qui ripreso ed esteso con best practice tratte da altri modelli (ad esempio ITIL) utili ad una corretta implementazione del SGSM. Interessanti le appendici (numerose) utili a chiarire le interazioni tra alcuni dei processi tipici di un SGSM.

La ISO/IEC 20000-3:2012
In questo standard sono contenute informazioni utili alla realizzazione (e verifica) dei SGSM, in particolare vengono definiti i criteri per la definizione dello "scope" del SGSM, tema particolarmente delicato quando si

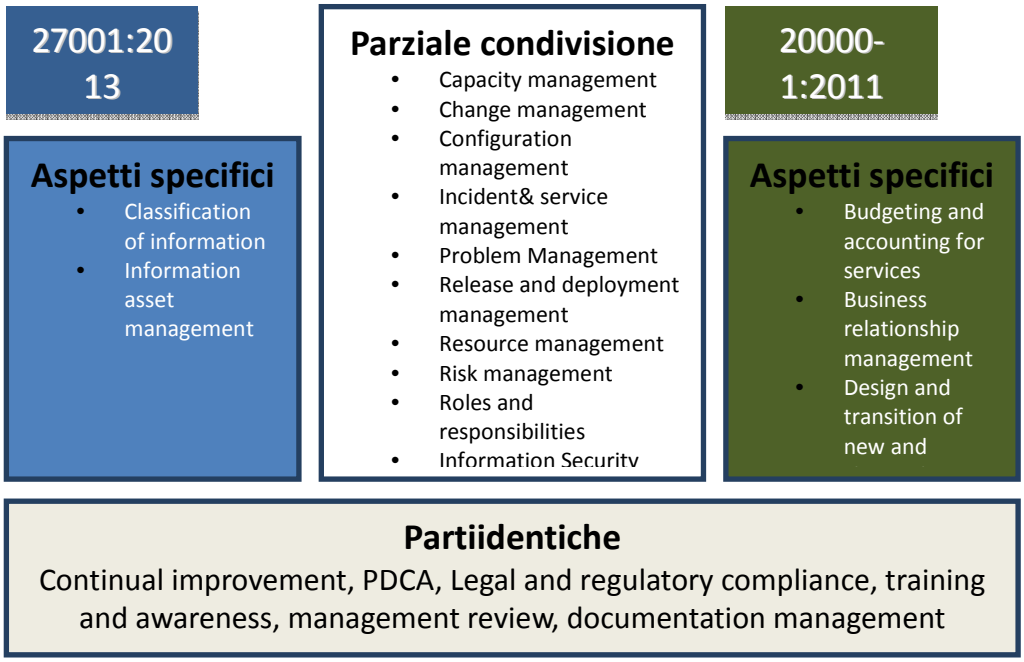
tratta di definire cosa si intende dimostrare e certificare. Altro rilevante aspetto analizzato in questo standard è le supply-chains, cioè le relazioni cliente/fornitore che permettono di assicurare il controllo end-to-end (tipico di questa norma e necessario per assicurare i servizi IT).

Gli audit integrati e la ISO/IEC 27013

La recente diffusione dei Sistemi Integrati basati su ISO/IEC 27001 e ISO/IEC 20000-1 ha condotto il sistema normativo a definire uno standard condiviso per la definizione di un alinea guida in grado di orientare le organizzazione sulle modalità di integrazione più idonee per i SGSI e SGSM.

La nascita della ISO/IEC 27013:2012 sancisce di fatto il primo esempio di integrabilità tra Sistemi di Gestione nell'ICT.

All'interno dello standard vengono analizzati quei temi che potrebbero influenzare l'integrazione dei due Sistemi di Gestione, inclusi alcuni processi e termini potenzialmente in contrasto. Uno schema come quello che segue esemplifica in modo evidente le zone di integrazione e sovrapposizione dei due sistemi di gestione:



Considerazioni tecniche sulle modalità di audit per i due Sistemi di Gestione

L'esperienza maturata in questi anni ci permette di fare alcune considerazioni sulle modalità e sulle tecniche per la conduzione degli audit sui SGSI e SGSM.

In termini pratici l'audit nei SGSI è focalizzato nella comprensione degli aspetti di sicurezza delle informazioni (di cui la sicurezza informatica è solo parte) mentre negli audit dei SGSM la focalizzazione è sui livelli di servizio.

Pur nell'ambito della stessa struttura aziendale, gli audit potrebbero attraversarla in modi diametralmente opposti! Nella medesima Organizzazione infatti i Sistemi di Gestione potrebbero avere ambiti e campi di applicazione diversi ed abbracciare processi diversi. A titolo puramente esemplificativo potremmo dire che mentre un SGSI cura la protezione delle informazioni di una Organizzazione un SGS cura invece i servizi erogati ed i processi che permettono l'erogazione di tali servizi. Dunque è possibile avere all'interno della stessa Organizzazione due Sistemi di Gestione che, pur condividendo alcuni processi, possono non

intersecarsi mai essendo destinati a due diverse destinazioni d'uso. L'unico caso di intersezione potrebbe essere costituito dalla gestione della sicurezza delle informazioni per i servizi IT erogati. In questo caso i due Sistemi si intersecherebbero almeno nei punti requisiti, come mostrato nella figura descrittiva della ISO/IEC 27013.

È chiaro che le competenze necessarie per la valutazione dei due Sistemi di Gestione posso differire enormemente. Infatti non necessariamente chi si intende di information security ha anche competenze nella gestione dei servizi IT! C'è qui da precisare che, almeno in linea teorica, la ISO/IEC 27001 potrebbe essere applicata anche ad un'azienda priva di sistemi informatici che produca beni materiali e che eroghi servizi di qualsiasi tipo. La ISO/IEC 20000-1 è invece orientata esclusivamente ad Organizzazioni dotate di sistemi informativi ed informatici che erogano servizi per mezzo di tali sistemi. Una bella differenza di partenza e di impostazione di cui tenere conto nel corso della gestione degli audit e nella formazione degli Auditor!

Formazione degli Auditor

Da quanto sopradescritto risulta chiaro che la formazione degli Auditor sta subendo profonde trasformazioni ed integrazioni. I corsi per Auditor/Lead Auditor sono largamente diffusi ed utilizzati anche per la formazione del personale non necessariamente destinato agli audit.

Per questo motivo molte Organizzazioni che erogano questi corsi stanno ampliando la gamma e la tipologia dei corsi integrando le varie norme all'interno di corsi specifici per Auditor di prima, seconda e/o terza parte. I partecipanti possono così essere guidati nella comprensione ed applicazione dei vari standard in relazione al tipo di sistema di gestione e del tipo di audit.

Nella formazione degli Auditor ed in particolare per gli Auditor dei SGSI e/o dei SGSM è indispensabile integrare almeno aspetti quali: la legislazione applicabile, il risk management, la business continuity e il disaster recovery, l'incidenth andling, la supplì-chain (per citare i più rilevanti). Argomenti questi oramai inscindibili dai contesti applicativi della ISO/IEC 27001 e ISO/IEC 20000-1 e dagli interessi delle organizzazioni pubbliche e private.

Fabrizio Cirilli
cirillif@tin.it
Amministratore Unico della PDCA Srl e dal 2012 è Head of GRC, Standards & Compliance Unit di Security Brokers SCpA.
E' certificato come Lead Auditor in registri nazionali ed internazionali per gli schemi ISO 9001, ISO/IEC 27001, ISO/IEC 20000 e TL 9000 ed opera con Organismi di Certificazione a livello nazionale ed internazionale.
Progettista e docente dei corsi di qualificazione per Lead Auditor negli schemi ISO 9001, ISO/IEC 27001, ISO/IEC 20000 e ISO 22301 (corsi riconosciuti/accreditati in Italia e all'estero).
Founder del Capitolo Italiano degli Utenti Internazionali dei Sistemi di Gestione per la Sicurezza delle Informazioni (ISMS IUG Italy) e membro attivo del Comitato ISO JTC1/SC27/WG1.
È uno degli specialisti italiani coinvolti nel progetto Domino della Presidenza del Consiglio dei Ministri.
E' membro CLUSIT, ISACA-AIEA, ISSA-AIPSI, UNINFO, ISO, ITSMF, AIIC ecc. e autore di pubblicazioni ed articoli sul tema della sicurezza delle informazioni.