LA NUOVA VERSIONE DELLA ISO27001

Sintesi a cura di Pierluigi Personeni, consultant HSPI

Introduzione

L'articolo si propone di descrivere alcune considerazioni a riguardo della nuova versione della **ISO/IEC 27001**, anticipandone la nuova organizzazione dei contenuti e alcune differenze discriminanti rispetto alla vecchia versione risalente al 2005, in base a quanto emerso nel processo di creazione del **FDIS** (Draft finale di Standard Internazionale).

Lo Standard ISO/IEC 27001 è una normativa internazionale che qualifica quali siano i requisiti essenziali per la gestione e l'impostazione di un Sistema di Gestione della Sicurezza delle Informazioni (ISMS).
A seguito della pubblicazione del draft finale nel mese di aprile, si prevede la pubblicazione della nuova versione per i mesi di Ottobre/ Novembre 2013.

La novità principale del nuovo standard è l'adeguamento alle nuove direttive definite dalla ISO e descritte nell'Annex SL delle ISO/ IEC Directives Supplement di maggio 2012. Tali direttive si prefiggono l'allineamento di tutte le norme dei sistemi di gestione ad un unico schema univoco nell'organizzazione dei contenuti a cui si stanno adeguando gli standard di recente e futura pubblicazione.

L'articolo presenta quindi la nuova struttura della norma che prevede i seguenti capitoli:

- il contesto dell'organizzazione;
- guida e direzione (Leadership);
- pianificazione;
- supporto;
- operatività;
- valutazione delle prestazioni;
- miglioramento;
- annex A.

In seguito, tenendo in debita considerazione che il contenuto di uno FDIS può subire modifiche significative, sulla base di quanto divulgato da Accredia, vengono indicate alcune novità significative rispetto alla versione precedente.

Si citano a tal proposito:

- l'eliminazione del concetto di azione preventiva;
- un testo meno prescrittivo, che dia maggior libertà alle organizzazioni di implementare i requisiti in modalità più aderenti alle proprie peculiarità.

Si ricorda inoltre come il processo di revisione della ISO/IEC 27001 e dei controlli di Sicurezza nell'Allegato A comporti la revisione in parallelo della ISO/IEC 27002, che contiene le linee guida per l'attuazione dei controlli, e la necessità di rimodulare gli attuali SoA (Statement of Applicability).

Lo standard ISO/IEC 27001

Lo standard ISO/IEC 27001 è la norma internazionale che definisce i requisiti per la corretta e funzionale gestione della sicurezza delle informazioni. La ISO 27001 è dunque il documento normativo al quale un'azienda deve fare riferimento per ottenere la certificazione circa il proprio Information Security Management System (ISMS). L'obiettivo ultimo diventa, quindi, la protezione dei dati e delle informazioni da minacce esterne di ogni natura, per assicurarne l'integrità, la riservatezza e la disponibilità, tre concetti must su cui si basa l'intero standard di riferimento.

A gennaio di quest'anno è stato pubblicato un **draft iniziale di standard internazionale (DIS),** al fine di permetterne non solo una prima consultazione pubblica, bensì anche una prima revisione della norma rispetto alle nuove esigenze del mercato. Ciò ha portato, **nel mese di Aprile**, a seguito dell'incontro della commissione internazionale responsabile per la ISO/IEC 27001, alla stesura di un **draft finale di standard internazionale (FDIS)**.

Recentemente, Accredia, l'Ente Italiano di Accreditamento, ha diramato una nota ufficiale in cui ci informa sulla situazione dei lavori di sviluppo e rilascio della nuova ISO/IEC 27001, anticipando al contempo alcune novità della nuova versione dello standard.
Accredia afferma che la nuova ISO/IEC 27001, la cui data di pubblicazione si stima intorno ad ottobre-novembre 2013, segue le **nuove direttive definite dalla ISO e descritte nell'Annex SL delle ISO/IEC Directives Supplement** di maggio 2012.
A tali direttive si è già adeguata per prima la nuova ISO 22301:2012, standard ISO che definisce il sistema di gestione della continuità operativa.

L'obiettivo dell'Annex SL è sostanzialmente quello di arrivare ad un allineamento di tutte le norme dei sistemi di gestione rispetto alla medesima organizzazione dei contenuti, avviando così di fatto il progetto di integrabilità concettuale degli schemi.
L'integrabilità di fatto, sempre possibile in linea teorica, deve essere oggetto di valutazione da parte delle singole organizzazioni interessate, anche per individuarne le migliori modalità in termini di applicazione concreta.
I contenuti della futura ISO/IEC 27001, ad oggi, sono:

- **Il contesto dell'organizzazione:**
  - Capire l'organizzazione ed il suo contesto;
  - Comprendere le necessità e le aspettative delle parti interessate;
  - Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni ;
  - Sistema di gestione per la sicurezza delle informazioni.

- **Guida e direzione (Leadership):**
  - Guida, direzione e impegno;
  - Politica;
  - Ruoli, responsabilità e poteri della organizzazione.

- **Pianificazione:**
  - Azioni per fronteggiare i rischi e le opportunità:
    - *Valutazione del rischio relativo alla sicurezza delle informazioni;*
    - *Trattamento del rischio relativo alla sicurezza delle informazioni;*
  - Obiettivi per la sicurezza delle informazioni e piani per conseguirli.

- **Supporto:**
  - Risorse;
  - Competenze;
  - Consapevolezza;
  - Comunicazione:
  - Informazioni documentate:
    - *Creazione e aggiornamento;*
    - *Controllo delle informazioni documentate.*

- **Operatività:**
  - Pianificazione e controllo operativo;
  - Valutazione del rischio relativo alla sicurezza delle informazioni;
  - Trattamento del rischio relativo alla sicurezza delle informazioni.

- **Valutazione delle prestazioni:**
  - Monitoraggio, misurazione, analisi e valutazione;
  - Audit interni;
  - Riesame della Direzione.

- **Miglioramento:**
  - Non conformità e azioni correttive;
  - Miglioramento continuo.

- **Annex A:**
  - Riferimenti alla ISO/IEC 27002.

Alla luce di quanto sopra esposto, Accredia fa notare la nuova organizzazione delle tematiche in oggetto. A titolo di esempio: si parla di *"informazioni documentate"* e non più di *"procedure documentate e registrazioni"*, le azioni preventive sono state eliminate poiché incluse nelle *"azioni per fronteggiare rischi e opportunità"*, la valutazione e il trattamento del rischio sono presenti sia nella pianificazione del SGSI sia nella sua operatività.

Non è sicuro che l'eliminazione del concetto di azione preventiva possa essere del tutto un beneficio, ma l'attuazione efficace del sistema di gestione è di per sé la madre della prevenzione rispetto a qualsiasi possibile fattore di instabilità organizzativa.

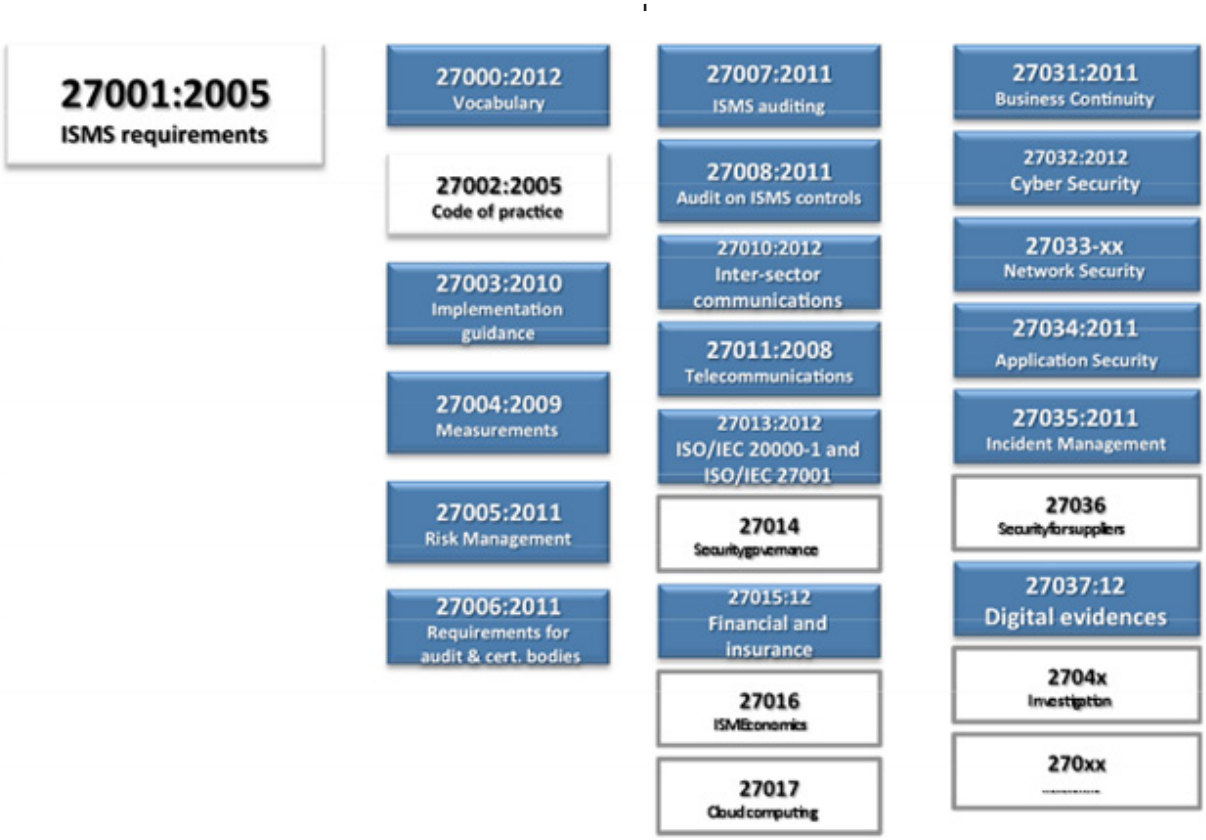
Accredia evidenzia, inoltre, il forte richiamo alla comprensione del contesto nel quale opera l'organizzazione ed alle aspettative delle parti interessate, che dello stesso sistema possono essere le promotrici.
Con la precedente edizione della norma quest'aspetto era poco sviluppato, concentrando da subito l'attenzione in modo troppo immediato sui beni e sulle pratiche di gestione della sicurezza.

Oggi, l'esigenza di definire le finalità, le opportunità ed i rischi relativi al sistema di gestione nel suo complesso, sia strategico aziendale, sia tecnico, risulta ben chiara e permetterà di focalizzare con maggiore efficacia ed efficienza lo sviluppo dei controlli di sicurezza non solo da un punto di vista tecnico, ma anche e soprattutto da un punto di vista organizzativo e gestionale. A solo titolo di esempio si segnala il caso della continuità operativa, che deve essere sì affrontato tecnicamente, ma sulla base di precise scelte strategiche.

Ovviamente, sono in fase di revisione anche la ISO/IEC 27000 e la ISO/IEC 27002 con la speranza di un'uscita contemporanea in modo da favorire l'aggiornamento simultaneo di tutti gli aspetti inerenti i sistemi di gestione per la sicurezza delle informazioni.
In particolare, la revisione della ISO/IEC 27002 si porterà dietro una nuova struttura dell'Annex A, con la conseguente necessità di rimodulare gli attuali SoA, processo che verrà comunque facilitato dalla presenza di un'apposita tabella di correlazione nella stessa ISO/IEC 27002.

Nel complesso, gli attuali SGSI non dovranno essere completamente reingegnerizzati per soddisfare i nuovi requisiti, anche se saranno da un lato necessarie e dall'altro lato possibili delle modifiche significative rispetto a quanto finora implementato dalle diverse organizzazioni.

A titolo informativo riportiamo uno schema che riassume l'insieme degli standard della famiglia ISO/IEC 27000 e del loro stato:



Su sfondo bianco gli standard non ancora pubblicati o in fase di aggiornamento *(situazione aggiornata a metà marzo 2013).*