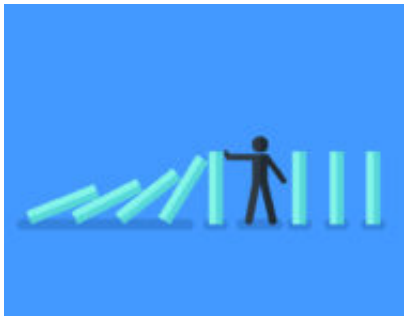
Nuova edizione della ISO/IEC 27005 “Information security risk management”

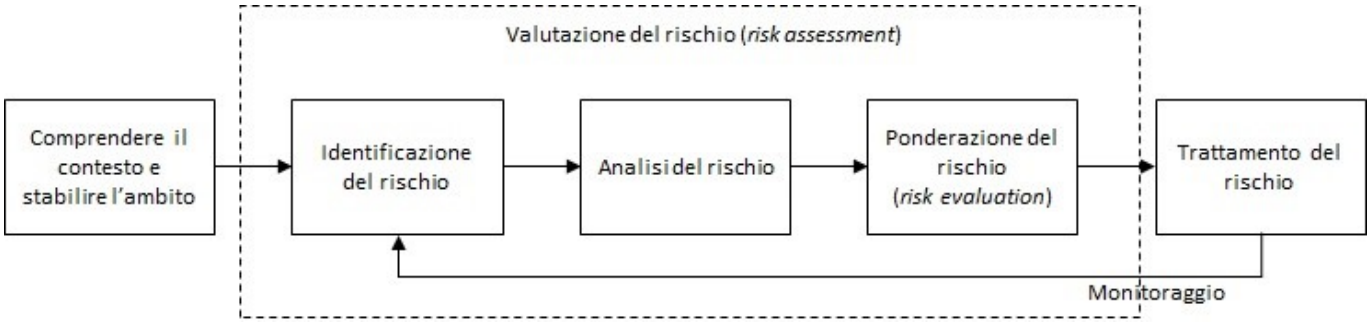
Author : Cesare Gallotti

Date : 2 novembre 2018



A luglio 2018 è stata pubblicata una nuova edizione (la terza) della ISO/IEC 27005 dal titolo “Information security risk management”. Si tratta dello standard internazionale di riferimento per la valutazione del rischio relativo alla sicurezza delle informazioni.

Lo schema della ISO/IEC 27005 è molto noto e si trova sul web impostando la ricerca delle immagini con la parola “ISO/IEC 27005”. Rappresentato in modo leggermente diverso, lo schema è il seguente:



Le modifiche apportate non sono particolarmente significative. Se ne tratta dopo aver presentato la norma stessa e i suoi limiti.

È opportuno ricordare che la ISO/IEC 27005 è una linea guida e non può quindi essere un criterio per valutare e certificare una “metodologia di valutazione del rischio”, anche se alcuni, impropriamente, lo hanno fatto.

La ISO/IEC 27005, trattando di valutazione del rischio relativo alla sicurezza delle informazioni, è applicabile anche alla valutazione del rischio relativo ai dati personali.

Il contenuto della ISO/IEC 27005

Seguendo lo schema, il contenuto della ISO/IEC 27005 è suddiviso in 6 capitoli (quelli dal 7 al 12):

- stabilire il contesto;
- valutare il rischio (a sua volta suddiviso nelle tre sezioni relative all'identificazione, analisi e ponderazione del rischio);
- trattare il rischio;
- accettare il rischio;
- comunicare il rischio e consultare le parti interessate;
- monitorare e riesaminare il rischio.

Molto interessanti sono le appendici. Infatti queste approfondiscono ulteriormente alcuni aspetti della gestione del rischio. Particolarmente utili sono: quella che riporta un esempio di lista di minacce e quella che riporta alcuni esempi per analizzare (ossia per calcolare) il rischio.

I limiti della ISO/IEC 27005

La prima edizione della ISO/IEC 27005 era del 2008. La seconda edizione era del 2011 e si rese necessaria per allinearla alla ISO 31000 dal titolo "Risk management — Principles and guidelines" (all'epoca era disponibile l'edizione del 2009; oggi è vigente la seconda edizione del 2018).

Nel 2013, come noto, fu pubblicata una nuova edizione della ISO/IEC 27001, basata sull'HLS (High level structure) e per questo molto diversa dalla precedente.

L'edizione del 2011 della ISO/IEC 27005 non era quindi più allineata alla nuova edizione della ISO/IEC 27001 e questo la rendeva formalmente scorretta.

La ISO/IEC 27005 promuove un approccio alla valutazione del rischio ritenuto troppo rigido e non sempre consigliabile. Questo approccio è detto "basato sull'identificazione di asset, minacce e vulnerabilità" e in effetti è peculiare della sicurezza delle informazioni ed ha origine, almeno, dalla fine degli anni Ottanta (alcuni metodi basati su questo approccio sono elencati nel documento "Description of automated risk management packages that NIST/NCSC Risk Management Research Laboratory have examined" del 1991), quando la sicurezza delle informazioni era decisamente diversa da quella attuale.

Il gruppo di esperti, a inizio 2014, appena dopo la pubblicazione della nuova ISO/IEC 27001, ha quindi iniziato a discutere di come modificare la ISO/IEC 27005, ma si sono scontrate due scuole di pensiero: una che ritiene ancora valido l'approccio basato sull'identificazione di asset, minacce e vulnerabilità (e infatti ancora oggi si vedono valutazioni del rischio che partono da un "inventario degli asset"), un'altra che promuove altri approcci, denominati "basati sugli eventi" (se ne trova traccia nella ISO/IEC 27003:2017).

Ad onor del vero, già l'ISO/IEC 27005 del 2008 suggeriva di accorpare gli asset, ma promuoveva comunque il miglioramento basato sul raffinamento dell'identificazione degli asset.

Dall’altra parte, l’approccio “basato sugli eventi” non può non considerare gli asset che possono essere impattati dagli eventi stessi.

Come spesso succede, però, le due scuole di pensiero non hanno trovato in tempi ragionevoli il modo per comporre i propri punti di vista in uno standard comune, sebbene da un punto di vista formale la ISO/IEC 27005:2011 fosse scorretta e richiedesse una correzione. Per le regole dell’ISO, superato un certo tempo non è più possibile pubblicare “correzioni” alle norme (come è stato fatto recentemente, per esempio, per la ISO/IEC 27001 e la ISO/IEC 29100) ma è necessario pubblicarne una nuova edizione.

Le modifiche apportate alla ISO/IEC 27005

Per il normale lettore della norma, le modifiche sono quasi invisibili. Per questo non è necessario specificarle nel dettaglio.

La prefazione della norma stessa fornisce l’elenco delle modifiche più significative:

- tolti tutti i riferimenti ai paragrafi della ISO/IEC 27001;
- specificato più chiaramente che la ISO/IEC 27005 non è una guida per l’attuazione dei requisiti relativi alla valutazione del rischio specificati dalla ISO/IEC 27001 (la questione è posta ambiguamente, ma ha l’obiettivo di ricordare che possono essere adottati metodi di valutazione del rischio coerenti con i requisiti della ISO/IEC 27001 e non con quelli della ISO/IEC 27005);
- la ISO/IEC 27001 non è più un riferimento normativo per la ISO/IEC 27005 (ma è comunque nella bibliografia).

L’introduzione ribadisce che la ISO/IEC 27005 si concentra su un approccio basato su asset, minacce e vulnerabilità e che altri approcci possono essere considerati.

Conclusioni

In questi anni ho avuto modo di vedere molti metodi di valutazione del rischio che richiedono un elevato dispendio di risorse per censire e valutare asset, minacce e vulnerabilità, purtroppo compensati da una scarsa significatività dei risultati (questo è facilmente dimostrato quando si vedono attivi progetti per “migliorare” la sicurezza delle informazioni senza però essere associati a rischi “inaccettabili” evidenziati dalla valutazione del rischio). L’approccio basato su asset, minacce e vulnerabilità può essere di difficile applicazione per le piccole o medie imprese.

Negli anni ho mantenuto aggiornato un metodo misto basato su un foglio di calcolo, denominato VERA (Very easy risk assessment). Esso è arrivato alla versione 4.0 nel 2018.

Altri, negli anni, hanno adottato metodi più simili a quello “basato sugli eventi”, adattando, per esempio, metodi di calcolo mutuati dalla FMECA o applicando i semplici principi promossi con la sigla STRIDE.

Per questo la ISO/IEC 27005 può essere considerata come obsoleta ed è un peccato che gli esperti non siano riusciti a trovare un accordo per una nuova versione, più adatta ai tempi.

Articolo a cura di **Cesare Gallotti**