Comunicare il rischio di sicurezza delle informazioni in modo semplice ed efficace, parte 1

Nelle organizzazioni, il tema della gestione dei rischi aziendali presenta un duplice problema, il calcolo del livello di rischio e l'efficace comunicazione ai vertici aziendali. Una corretta valutazione di rischio, perde tutta la sua efficacia, se non viene propriamente compresa dalle posizioni manageriali con potere decisionale. Per una comunicazione efficace, è necessario rappresentare la situazione esaminata, collegando i processi aziendali ben noti ai top manager con le loro minacce più significative. Come descrivere il rischio per la sicurezza delle informazioni in modo semplice ed efficace al top management, affinché prenda le giuste decisioni, è esposto in questo articolo. Una volta comunicato il rischio, le proposte di mitigazione possono essere dettagliate, discusse ed implementate, come trattato in "Comunicare il rischio di sicurezza delle informazioni in modo semplice ed efficace, parte 2"[1].

Selezione dei fattori di rischio

Parlando con il top management non è così insolito di dover cambiare il proprio linguaggio per semplificare i concetti e rendere il contesto comprensibile, così da superare il divario di conoscenze specifiche con l'interlocutore. È necessario doverlo fare per mantenere sempre aperto il canale comunicativo, anche a rischio di tralasciare delle tesi ritenute di valore o di non riuscire ad enfatizzarne l'importanza di altre. Ecco, la domanda è "Quali informazioni sono importanti e per chi?" Questa è una questione da chiarire per poter migliorare la comunicazione a beneficio degli obiettivi aziendali.

La ragione del colloquio con i vertici aziendali non è mai per un'esibizione delle proprie competenze o per sponsorizzare una propria simpatia verso nuove evoluzioni tecnologiche, ma è utile a portare l'attenzione su tematiche di specifico interesse per gli obiettivi aziendali, che richiedono un attenta valutazione, a fronte di un rischio con impatto significativo. Un cambio di prospettiva nella comunicazione può agevolare la comprensione della tematica che si vuole esporre. È utile, anziché focalizzarsi su una vista dettagliata, tecnologica e specialistica, considerare una rappresentazione più generale ed organizzativa, meglio se semplificata, della questione per evidenziare i legami e le conseguenze per gli obiettivi di business.

Luigi Sbriz, CISM, CRISC, CDPSE, ISO/IEC 27001:2013 LA, ITIL v4, UNI 11697:2017 DPO
È stato il responsabile del monitoraggio dei rischi presso un'azienda multinazionale del settore automotive per oltre sette anni. In precedenza, è stato responsabile della gestione dei servizi e delle risorse ICT nell'area Asia-Pacific (Cina, Giappone e Malesia) e, prima ancora, è stato responsabile della sicurezza delle informazioni a livello mondo per più di sette anni. Per quanto attiene al monitoraggio interno del rischio, ha sviluppato una metodologia originale unendo un'analisi del rischio operativo con una conseguente valutazione del rischio guidata dal livello di maturità dei processi. Inoltre, ha progettato uno strumento di cyber monitoring e un sistema integrato per monitoraggio del rischio, modello di maturità e audit interno. Sbriz è stato anche consulente per sistemi di business intelligence per parecchi anni. Può essere contattato su LinkedIn (*https://it.linkedin.com/in/luigisbriz*) oppure su *http://sbriz.tel*.

Le presentazioni sono spesso guidate dal proprio modo di vedere il problema. Sono generalmente redatte da esperti della tematica, con molti dettagli tecnici sugli aspetti progettuali e sul lavoro intrapreso. Però, i dettagli ci sono già nei documenti di progetto, nelle istruzioni operative o nei rapporti sull'attività svolta. Se prevalgono i dettagli sulla visione d'insieme, può sembrare una duplicazione con solamente un cambio di stile.

Per agevolare la comunicazione, l'enfasi non dovrebbe puntare troppo sul dettaglio della tecnologia o dell'operatività ma sul beneficio dell'adozione di quella tecnologia o di quel tipo di lavoro ed anche sui rischi che tutto ciò comporta. Quindi, una buona presentazione ad alto livello, non declina subito il dettaglio della soluzione (e neppure dopo, se non richiesto) ma raffronta in estrema sintesi, tramite una gap analisi, i pro ed i contro per l'organizzazione stessa. Il come si esegue è sempre meno importante delle sue conseguenze. Partiamo quindi dal contesto e dalle minacce potenziali per arrivare alle conseguenze attese, ossia, diamo poca importanza al percorso fatto (concetto della black box).

Le sorgenti dei dati sul rischio

La base di partenza, dove attingere le informazioni da sviluppare nella presentazione, è il risk register[2] per un motivo molto semplice. È il contenitore di tutti gli scenari, delle analisi, delle valutazioni fatte e delle decisioni già prese sui modi e mezzi per raggiungere gli obiettivi aziendali trattando il rischio. La sua sintesi finale è rappresentabile con un grafico a bolle[3] che riassume lo stato del livello di rischio per tutti i processi dell'azienda, valutato tramite un modello di maturità della capacità (CMM[4]).

Il modello di maturità è il passaggio intermedio tra il registro dei rischi e il grafico di sintesi e ha un duplice scopo. Il modello di maturità aggrega opportunamente il rischio e introduce un solido legame tra rischio e controllo, sia che tali processi siano già implementati o solo pianificati. Introduce anche la valutazione della vulnerabilità. La vulnerabilità è una metrica che misura la debolezza di un controllo e le possibili conseguenze.

In tal modo, questo grafico a bolle è in grado di rappresentare uno scenario più ampio di quello originabile da un rischio basato unicamente sui valori di impatto e di probabilità. Il registro dei rischi e la CMM creano un legame ad alto valore, con informazioni aggiuntive, che sono associate al livello di vulnerabilità ed alla capacità di reazione (stato del piano di trattamento del rischio). Però, anche se così ricco di informazioni, è pur sempre una sintesi di alto livello per prioritizzare i rischi sulla gravità per l'azienda nel suo complesso, ma non descrive la soluzione. Il grafico di sintesi dei rischi, consente di analizzare il contesto generale di rischio e ovviamente deve penalizzare i dettagli del contesto operativo, impedendone una chiara comprensione sulle ragioni delle scelte effettuate o dei trattamenti di rischio pianificati. In altre parole, è finalizzato a concentrare l'attenzione sulla valutazione delle questioni più rilevanti (eventi di rischio) che si devono affrontare in relazione agli obiettivi aziendali (prospettiva globale) piuttosto che sul modo di definire la soluzione pratica da adottare (contesto operativo).

Per chiarire ulteriormente l'importanza di avere disponibili le informazioni per analizzare un fenomeno, pensiamo ad un rischio quotidiano: perdere le chiavi di casa. Supponiamo che in linea con gli obiettivi (trovare sempre le chiavi) e con la stessa qualità di protezione (disponibili nel momento che servono), ci siano tre possibili soluzioni legate all'acquisto di un portachiavi:

1. uno dotato di tecnologia GPS (Global Positioning System)
2. uno con un portafoto ed
3. uno con una torcia LED.

Per il risk register, le tre soluzioni sono equivalenti dal momento che tutte soddisfano l'obiettivo. Il proprietario della chiave potrebbe ritenere di avere un beneficio maggiore da una soluzione differente da quella proposta, però, solo se fosse a conoscenza di tutte e tre le opzioni.

Sfumature e dettagli non possono essere aggiunti alla sintesi senza compromettere la finalità di aggregazione e la capacità di comprendere i risultati di rischio evidenziati. È ragionevole aspettarsi dal risk register la capacità di identificare con chiarezza i rischi più significativi, suddivisi almeno per processo ed entità. Se per l'insieme dei rischi critici, si vuole accedere a dettagli operativi di trattamento del rischio, si dovrà procedere in altro modo, con ulteriori prospetti più focalizzati sugli aspetti di interesse. Al primo livello di presentazione si identifica la criticità ma senza pretendere di far

capire contemporaneamente come si andrà a trattarla. La presentazione segue sempre un approccio top-down, da sintesi per avere una prospettiva complessiva dello scenario, a dettaglio per esporre le scelte implementative.

Il processo di valutazione del rischio è generalmente bottom-up. Il responsabile del rischio, prima partecipa alla stesura del risk report con tutto il proprio bagaglio di conoscenza e competenza per giungere a trattare il rischio efficacemente, ma poi deve essere in grado di sintetizzare le soluzioni e le loro criticità con un linguaggio non specialistico per poter divulgare i criteri delle scelte. Il fine è di riuscire a coinvolgere il top management fornendo elementi concreti affinché siano in grado di decidere in modo consapevole sulle conseguenze per l'azienda.

Scenario di rischio per processo

Nel grafico a bolle del risk register, rappresentativo dell'intera mappa dei rischi aziendali, il responsabile di processo seleziona i rischi a maggior severità per il proprio processo, per i quali presumibilmente si prevedono le azioni più onerose, che necessariamente richiederanno il coinvolgimento dei vertici aziendali nel processo decisionale. Le misure di contenimento di questi rischi, per essere comprese appieno dal top management, richiedono una trasformazione dei livelli qualitativi di rischio, impatto, probabilità, maturità ed il sintetico piano di rimedio in uno scenario di cause, azioni e conseguenze.

Selezionati i rischi rilevanti, come passo seguente, si deve evidenziare la severità delle minacce rapportata all'intensità delle conseguenze per il business in un contesto più focalizzato al processo operativo di quanto si possa dedurre dal grafico a bolle del risk register. Intendiamo con contesto operativo una rappresentazione dell'intero processo che evidenzi schematicamente lo scenario operativo da una prospettiva di business, quindi, richiamando le interfacce verso gli altri processi, le tipologie di personale implicato, i beni aziendali coinvolti e tutte le attività in corso.

Per riuscire a chiarire come procedere è necessario scegliere un ambiente di riferimento per contestualizzare tutte le considerazioni seguenti. Pertanto, da qui in avanti, il processo di sicurezza informatica aziendale è usato per descrivere in che modo rappresentare i dati di presentazione ad alto livello, per una narrazione efficace del rischio anche nel rispetto del contesto operativo. La sicurezza informatica è un processo altamente tecnologico, con forti impatti sulla maggior parte dei processi aziendali, sui beni utilizzati e sulle risorse impegnate, umane e non. È un buon candidato, in termini di complessità e completezza, per essere preso come riferimento e per creare una efficace presentazione del proprio processo.

Come evidenziare la severità delle minacce e delle conseguenze

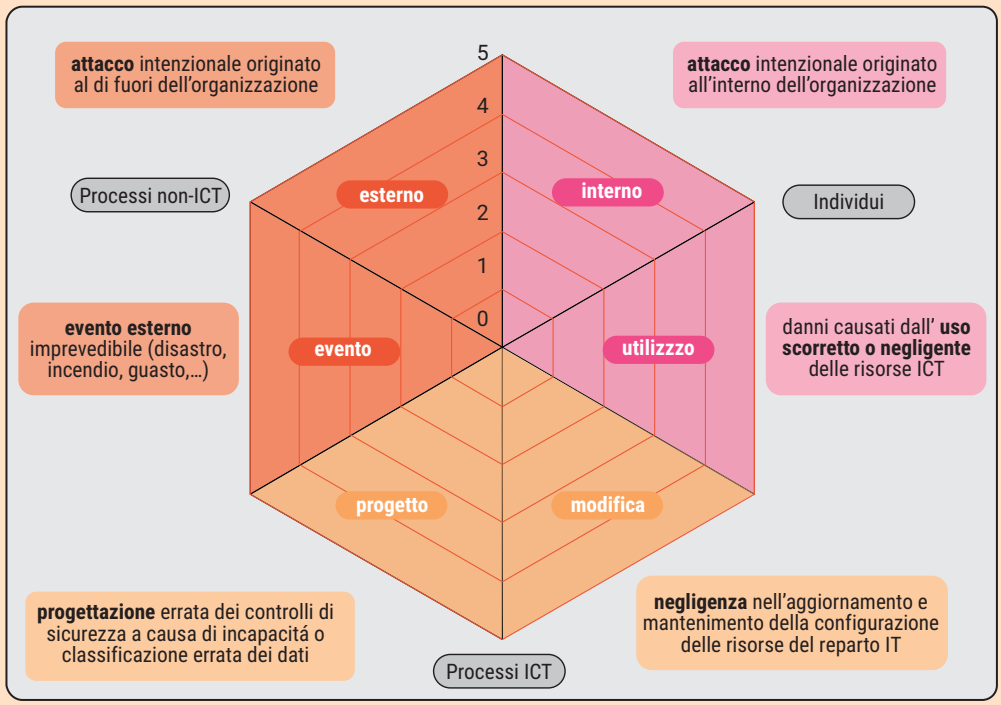
A livello pratico, nel sistema informatico adottato per la gestione del rischio, ai risk owner sarà reso disponibile, per ogni processo gestito, un template (**figura 1**) per selezionare i fattori rischi da portare all'attenzione del top management. Il template, alimentato automaticamente dal risk register sulle minacce per quel processo, serve per inserire delle note ad alto livello per meglio focalizzare l'attenzione sulle criticità.

Le minacce gestite dalla sicurezza delle informazioni sono classificate in base alla natura della causa primaria del relativo rischio da un punto di vista aziendale piuttosto che tecnologico. Sono state identificate sei zone con minacce significative in base ad una prospettiva organizzativa e operativa. Ogni zona rappresenta determinate categorie di potenziali cause di rischio e livelli di gravità delle relative conseguenze (in assenza di gestione del rischio) per l'impresa. Nella **figura 1**, tre differenti colori rappresentano tre macro ambiti—individui, processi non-ICT, e processi ICT—identificati in quanto omogenei rispetto al tipo di sorgente della minaccia, all'ambiente di applicazione delle attività di contrasto ed alla tipologia di destinatario del potenziale impatto.

Individui
In questo ambito, gli attori principali sono le risorse umane. In questo caso, si intende principalmente come causa, diretta o indiretta, del livello di rischio misurato. Le zone di minaccia incluse in questo ambito sono:

- **Interno**—attacco intenzionale eseguito dall'interno dell'organizzazione. Il contrasto a questa causa di rischio richiede mezzi tecnici se si concretizza con un uso mirato di strumenti informatici, mezzi legali se si ravvisa un uso fraudolento delle risorse, mezzi organizzativi se

Figura 1—Modello per rischio di sicurezza informatica e zone di minaccia



sfrutta falle procedurali e mezzi formativi se richiede la collaborazione del personale coinvolto. È la tipologia di rischio più insidiosa perché può minare il rapporto di fiducia con il personale e rendere nulle tutte le altre misure.

- **Utilizzo**—danni causati da un utilizzo scorretto o negligente dei beni ICT assegnati. Il contrasto si attua con una formazione periodica, mirata alla popolazione degli utilizzatori, e con controlli sistematici e specifici. Ad esempio, usando la policy del minor privilegio, scegliendo un'opzione da una lista anziché doverla scrivere per esteso, controllando regolarmente l'autorizzazione e la necessità d'uso, valutando penali nel caso di ripetute violazioni, formando e verificando il livello di apprendimento e così via.

Processi non ICT

In questo ambito, le conseguenze di un evento esterno di rischio principalmente colpiscono processi aziendali non ICT e sono significative per gli obiettivi di business. Le zone di minaccia incluse in questo ambito sono:

- **Esterno**—attacco intenzionale originato all'esterno dell'organizzazione, sia come bersaglio che inconsapevole complice o come effetto collaterale. Le conseguenze possono interessare tutti i processi, proprietari od utilizzatori, delle risorse coinvolte nell'attacco. Il contrasto richiede un'efficace attività preventiva di controllo, come ad esempio, delle valutazioni di vulnerabilità o dei penetration test. Un piano di audit sui processi impattati garantisce la correttezza delle valutazioni effettuate. Le conseguenze possono consistere anche in un impatto sull'immagine dell'azienda di entità superiore al puro costo del potenziale danno fisico. Nel caso di un data breach su dati personali si deve affrontare un problema legale mentre nel caso della perdita di dati di tecnologia segreti si rischia anche la compromissione dell'intero business.
- **Eventi**—eventi esterni imprevedibili non riconducibili ad una precisa finalità di attacco (evento climatico estremo, incendio, pandemia,

interruzione elettrica o idrica, ...). Le conseguenze sono principalmente legate alla continuità del business e quindi possono essere compromesse anche le risorse del servizio IT, sia direttamente come fronte primario dell'incidente che indirettamente per effetto a catena. Il contrasto richiede un realistico piano di continuità operativa (BCMS[5]) sull'intera organizzazione con focalizzazione volta ad attenuare l'impatto sui sistemi IT in dipendenza da quanto emerge dall'analisi di rischio.

Processo ICT

In questo ambito, sia la sorgente del rischio che il destinatario delle conseguenze è sempre interno al processo ICT. Le cause sono legate alle modalità di esecuzione delle attività informatiche svolte internamente. Le zone di minaccia incluse in questo ambito sono:

- **Progettazione**—progettazione errata dei controlli di sicurezza a causa di incapacità progettuale, requisiti insufficienti, inattendibilità delle valutazioni, incompletezza delle procedure o inadeguata classificazione dei dati. In generale, cause di progettazione incompleta o errata che si riflettono sul servizio IT anche se l'origine dell'evento è esterno ad esso. Ad esempio, interruzione elettrica e mancato avvio del sistema di continuità nella sala server per difettosità non rilevata preventivamente, rischio per controllo carente su dispositivi IT. Le conseguenze possono essere effettivamente gravi per eventuali impatti sui processi aziendali critici o sui clienti o sui fornitori o anche sull'immagine aziendale. L'oramai necessaria invasività del servizio IT in tutti i processi aziendali, fa ben capire la rilevanza del problema del corretto disegno dei controlli che può giungere fino alla compromissione della stessa missione aziendale. Il contrasto richiede un'applicazione, sostanziale e non formale, delle metodologie di controllo più idonee alla specifica tipologia di business.
- **Modifica**—negligenza nella configurazione o nella manutenzione dei sistemi o in generale su qualunque cambiamento ai sistemi hardware, alle applicazioni software, alle configurazioni di rete o ai processi interni all'ICT. Le conseguenze sono generalmente delle potenziali vulnerabilità introdotte nei beni interessati dal change management. Il contrasto richiede un rigoroso rispetto degli standard e delle best practice dell'infosec, una formazione adeguata per tutti gli operatori e l'implementazione di controlli efficaci, sia automatici che manuali.

Qualunque evento di rischio di sicurezza informatica può essere intuitivamente attribuito ad una delle sei zone di minaccia. Sebbene questa suddivisione per zone di minaccia ricordi poco le tematiche specialistiche del rischio di sicurezza informatica, ha però il vantaggio di consentire una visione più organizzativa, orientata alle conseguenze verso gli altri processi, ai fattori di rischio umano ed alla capacità di esecuzione dei compiti del processo in analisi. Con l'aggiunta delle spiegazioni predefinite, associate ai colori delle zone ed alle etichette, si aiuta l'osservatore non tecnico a formarsi un'idea generale dello scenario operativo del processo e delle conseguenze per l'azienda.

Fornire dettagli per il processo decisionale

Nella fase successiva, l'obiettivo è assistere la direzione e le parti interessate nel processo decisionale[6]. Quando i processi critici e i fattori di rischio gravi sono già stati identificati, è tempo di fornire un livello di dettaglio più operativo ma comunque comprensibile per le persone che non sono specialisti di processo

L'obiettivo della rappresentazione astratta dei rischi è di creare una vista d'insieme, collegando le aree di operatività aziendale alle tipologie di conseguenze per l'azienda, per ciascun rischio selezionato. Ciò si traduce nella perdita di alcuni dettagli nel piano di rimedio, ma ciò può essere compensato in un nuovo livello di profondità organizzativa. Ora il focus è a livello di sintesi tra rischi, applicazione di regole ed ambito organizzativo.

L'esempio di applicazione di questa particolare rappresentazione dei rischi è riportato nella **figura 2**. Il grafico è estremamente semplice, senza numeri (a parte il livello di rischio, 0–5), per favorire una riflessione sulla causa-effetto tra la minaccia (osservata o potenziale) e l'attesa compromissione

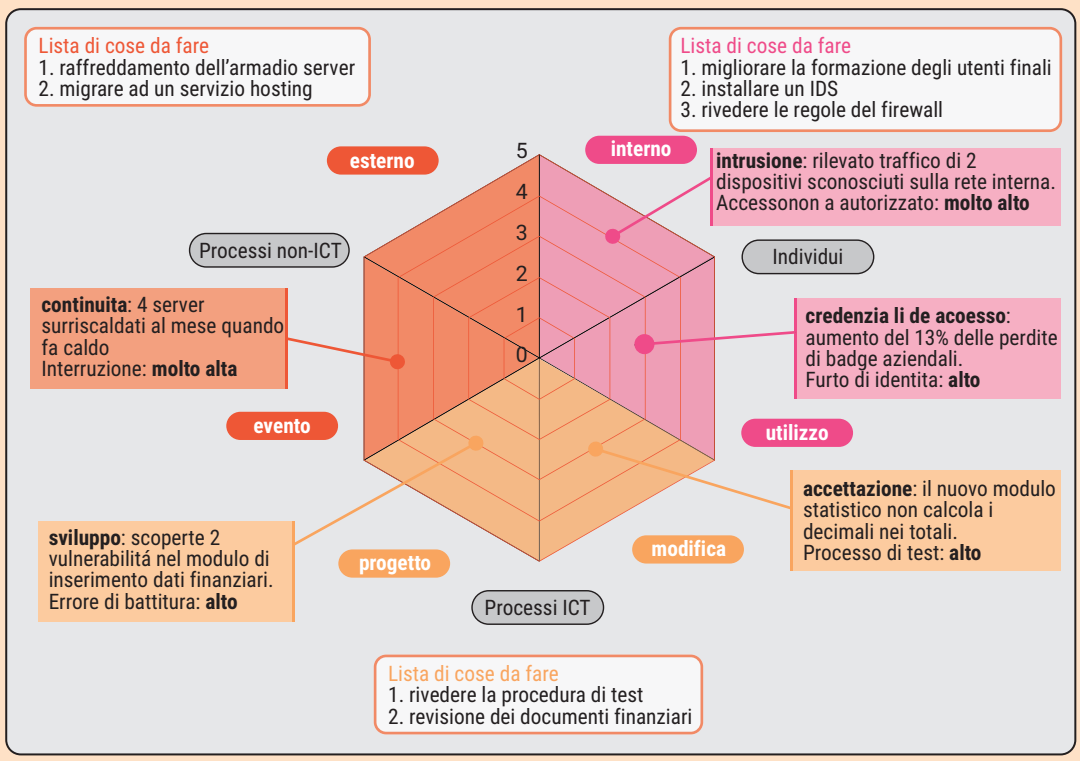
degli obiettivi a seguito del rischio calcolato. La rappresentazione qualitativa, aiuta la creazione di una correlazione mentale tra minaccia e conseguenze sugli obiettivi. Non fornisce il percorso verso la soluzione ma serve a comprendere la reale gravità della minaccia. Se un ulteriore approfondimento è necessario, si prosegue dettagliando in un altro prospetto le misure di protezione proposte ad assicurare il contenimento del rischio.

Dal risk register si estraggono le descrizioni delle minacce ed il livello di rischio. In **figura 2**, le etichette riassumono la minaccia e sulla griglia sono posizionati i punti che indicano il livello di rischio. Ogni etichetta descrive l'evento che introduce il fattore di rischio e, sinteticamente, le conseguenze. La narrazione schematica è un modo semplice per aiutare le persone a comprendere il peso della minaccia.

Il colore della zona di minaccia indica all'osservatore l'ambiente funzionale in cui si materializza la minaccia. L'ambiente funzionale è implicitamente richiamato dal nome della etichetta ed è descritto in modo generale nelle note del template, ma diviene chiaro cos'è nella realtà a chi conosce l'organizzazione. Di conseguenza, permette di associare tra loro i processi che sono implicati, la necessità di formazione o di altri interventi sul personale, il tipo di asset informatico coinvolto, l'esigenza di una revisione organizzativa o l'opportunità di migliorare la comunicazione. Le caselle di testo (elenchi di cose da fare) mostrano le azioni previste per ciascun ambito. Alcune azioni possono interessare più zone, ma è opportuno includerle solo una volta nella zona più rilevante.

È possibile aggiungere altre informazioni a questo grafico, ma ciò potrebbe ridurne la chiarezza complessiva, quindi è importante considerare se

Figura 2—Esempio di significative minacce rilevate



vale la pena farlo. Nell'esagono possono essere utilizzate anche diverse tonalità dello stesso colore per evidenziare diversi livelli di rischio. L'uso di un esagono non è essenziale; funzionerà anche un cerchio o un'altra forma. È anche importante non dominare il testo con una grafica appariscente.

Conclusioni

Questa visualizzazione delle minacce, più focalizzata ad aspetti organizzativi che specialistici di processo, agevola la comprensione ad alto livello delle interazioni con gli altri processi aziendali ed aiuta a concentrarsi sulle conseguenze per l'azienda piuttosto che su particolari tecnici. Successivi approfondimenti saranno necessari per comprendere pienamente i fenomeni dal punto di vista dell'organizzazione anziché da quello tecnico, come trattato in "Comunicare il rischio di sicurezza delle informazioni in modo semplice ed efficace, parte 2".

Endnotes

1 ISACA®, "Communicating Information Security Risk Simple and Effectively, Part 2," *ISACA® Journal*, vol 6, 2021, *https://www.isaca.org/archives*
2 ISACA, *CRISC Review Manual 6th Edition*, 2015, *https://www.isaca.org/resources*
3 Sbriz, L.; "Enterprise Risk Monitoring Methodology, Part 4", *ISACA® Journal*, vol. 3, 2020, *https://www.isaca.org/archives*
4 CMMI Institute, *https://cmmiinstitute.com/*
5 International Organization for Standardization (ISO), *ISO 22301 Security and Resilience—Business Continuity Management Systems—Requirements,* Switzerland, 2019, *https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en*
6 *Op cit* ISACA, 2015