GRC nel 2023: Pilastri, Vantaggi e Sinergie con la Cybersecurity



Coniata oltre 20 anni fa dall'Open Compliance and Ethics Group (OCEG) ma tuttora molto attuale, la sigla "GRC" sta per "*Governance, Risk & Compliance*" e indica una strategia integrata che le organizzazioni possono adottare per garantirsi il perseguimento dei propri obiettivi e l'attitudine ad adattarsi ai continui cambiamenti. Le aziende sono chiamate ad operare all'interno di un quadro sempre più complesso, connotato da vari scenari di rischio imputabili a molteplici fattori, quali ad esempio la volatilità dei mercati finanziari, i dissesti idrogeologici, gli attacchi informatici, i conflitti politici o le modifiche normative (e la conseguente evoluzione delle richieste degli stakeholder interni ed esterni), in cui la capacità di gestire con efficienza i differenti fronti di rischio risulta leva strategica per garantire la solidità del proprio business.

I tre "pilastri" del sistema GRC

Le best practice evidenziano come una strategia vincente per la competitività delle aziende sia imperniata sul paradigma GRC, articolato nei seguenti principali filoni operativi:

- ***Governance*** **–** presidiare le attività decisionali, strategiche e manageriali, dalla definizione degli obiettivi, all'organizzazione dei flussi di lavoro o di comunicazione (interna ed esterna) che indirizzano l'organizzazione mediante politiche, regolamenti ed eventuali standard o framework;
- ***Risk*** – assicurarsi, tramite attività di *auditing* e *risk/vulnerability assessment* sui processi interni ed

eventualmente su quelli delle terze parti critiche, una gestione integrata dei rischi che possono incidere sulle strategie aziendali e/o sulla continuità operativa e, in definitiva, sul perseguimento del business (incidenti di sicurezza, *data breach*, attacchi informatici, violazioni normative/sanzioni, perdite finanziarie, ecc), compromettendo così l'immagine positiva dell'azienda e la fiducia degli stakeholder;

- ***Compliance –*** garantire la conformità delle scelte organizzative, delle modalità operative e dei prodotti/servizi finali al quadro normativo nazionale e internazionale di riferimento, inclusi i vari standard e regolamenti di settore, oltre che ai vincoli contrattuali sottoscritti con Clienti e Fornitori, per mantenere una elevata *reputation* nel mercato di riferimento e presso tutti gli *stakeholder*.

Implementare un sistema di gestione integrato dei rischi sul modello GRC, richiede un approccio multidisciplinare di tipo osmotico, capace cioè di mettere in connessione i vari dipartimenti dell'organizzazione (IT, Security, Risk Management, Legal, Privacy, Compliance, ecc), contaminandone reciprocamente linguaggi e visioni, al fine di produrre una cultura del rischio condivisa e un linguaggio comune, anche attraverso l'uso di piattaforme e strumenti informatici dedicati.

«*La gestione del rischio rappresenta un'attività sempre più centrale.* – osserva Guido Arrigoni, Manager della Business Unit Compliance di 7Layers – L*a ritroviamo nel panorama normativo internazionale in materia di sicurezza (si pensi a regolamenti come il DORA o il GDPR, ma anche alle direttive come la NIS2) e nei principali standard per la sicurezza, come la ISO 27001 o il framework NIST per la cybersecurity. Il processo di risk management, che è per definizione dinamico* – aggiunge – *costituisce il cuore pulsante del sistema, da cui si innescano l'aggiornamento continuo delle misure di*

sicurezza, la ricerca di soluzioni innovative, coerenti con le prescrizioni normative e con le strategie aziendali per favorire ottimizzazioni ed efficienza».

I vantaggi dell'approccio GRC

L'apporto armonico di persone e tecnologie, sostenuto da processi decisionali risk-based e informati, consente alle organizzazioni di governare l'incertezza, nel pieno rispetto delle regole. Ciò permette di:

- Garantire maggior trasparenza nella comunicazione dei propri valori e obiettivi, sia all'interno (dipendenti e collaboratori) sia all'esterno dell'organizzazione (Clienti, Fornitori, Pubbliche Amministrazioni, Organi di vigilanza e Autorità, semplificandone così i rapporti;
- Identificare le eventuali ridondanze e inefficienze e intervenire con soluzioni mirate a valorizzare le sinergie fra i team e a ottimizzare tempi e costi;
- Migliorare la produttività, garantendo più elevati standard di qualità e sicurezza dei prodotti o servizi finali.

GRC e cybersecurity: connubio vincente

Al fine di garantirsi standard di qualità e sicurezza elevati con le ricadute positive sopra descritte su business e reputation aziendale, è necessario saper declinare il modello GRC all'interno della propria realtà organizzativa, coniugandola con sistemi IT all'avanguardia e compliant.

Il differenziale competitivo per le aziende di oggi risulta dunque un modello "GRC – IT" che estende l'approccio "*Governance, Risk & Compliance*" alla gestione dei sistemi e delle risorse informatiche e informative, coniugando l'adozione delle misure di sicurezza proprie della cybersecurity con l'attenzione ai requisiti normativi,

contrattuali e di best practice, nelle scelte delle priorità e nella definizione delle strategie aziendali.

In altri termini, la gestione del rischio cyber diviene parte integrante della gestione dei rischi aziendali e viene affrontato favorendo lo sviluppo di una cultura aziendale più attenta agli aspetti di sicurezza, incentivando la diffusione di un lessico condiviso, stanziando il budget necessario per sostenerne costi, in ottica di investimento.

"*Una governance efficace* – conclude Arrigoni – *può creare i presupposti affinché compliance e cybersecurity finalmente si incontrino per una gestione orchestrata e ottimizzata dei rischi a cui ogni organizzazione è inevitabilmente esposta. Anche i settori storicamente meno attenti alle implicazioni proprie del mondo informatico hanno iniziato un percorso di investimenti importanti nel settore della sicurezza, coerenti con il contesto in cui operano e con gli obiettivi aziendali prefissati*".

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/grc-nel-2023-pilastri-vantaggi-e-sinergie-con-la-cybersecurity/