Controllo interno, cybersecurity e umanesimo digitale

A cura di Carlo Guastone

Il framework COSO

Il framework COSO (acronimo che identifica il gruppo di lavoro che lo ha realizzato nel 1992) è universalmente riconosciuto come la bibbia del Controllo interno delle aziende, concepito come strumento di verifica dell'operato del management nei confronti degli stakeholders (portatori di interesse), azionisti in primis ma anche dipendenti, clienti, fornitori, parti sociali, e così via.

Il framework consiste in un insieme di principi e linee guida per la gestione del controllo interno e della corporate governance nelle organizzazioni, con particolare riferimento ai processi aziendali che assicurano la conformità normativa, la sicurezza, l'efficacia e l'efficienza delle operazioni, la assegnazione di ruoli e responsabilità.

Nel 2013 è stata pubblicata la versione COSO ERM centrata sull' enterprise risk management, che ha l'obiettivo di garantire che le organizzazioni siano in grado di raggiungere i loro obiettivi strategici, operativi, di reporting e di compliance, riducendo al minimo il rischio di non riuscire a raggiungere tali obiettivi.

COSO ERM si basa su cinque componenti chiave (ambiente di controllo, valutazione dei rischi, attività di controllo, informazioni e comunicazioni, monitoraggio delle attività) ed estende la gestione dei rischi a tutta l'organizzazione, non solo ai rischi finanziari, considerando gli obiettivi strategici dell'impresa. Il framework è stato adottato in particolare dalle grandi imprese quotate (ad esempio negli USA in ottemperanza alla legge SOX, in Italia in ottemperanza alla Legge 262/2005 dedicata al Risparmio e al Codice di autoregolamentazione società quotate), ed è utilizzato in molti settori e può essere adattato alle specifiche esigenze di ciascuna organizzazione.

Nel 2023 il COSO ha pubblicato delle linee guida supplementari per le organizzazioni relative alla rendicontazione della sostenibilità (ICSR), mentre nel 2024 ha pubblicato un documento specifico relativo ai controlli della robotica. Per approfondimenti https://www.coso.org/guidance-on-ic.

Fin dalla prima pubblicazione del framework COSO nel 1992, e in particolare dalla versione 2013, la sicurezza informatica era considerata una componente rilevante del Controllo Interno, centrata prevalentemente sulla continuità operativa e sull'integrità delle informazioni, senza una specifica focalizzazione sulla cybersecurity

COSO ERM e rischi Cyber

L'integrazione di COSO ERM e cybersecurity è fondamentale per garantire la sicurezza e la resilienza di un'organizzazione, permettendo di gestire i rischi informatici in modo efficace e strategico. L'integrazione tra COSO ERM e la cybersecurity è cruciale per garantire la sicurezza aziendale e la continuità operativa. Per identificare l'ambito da considerare ci viene in aiuto un recen-

te contributo di ACN di cui riportiamo l'abstract:

"Il dominio Cyber Risk Management consiste nell'insieme di pratiche volte alla gestione del rischio cyber entro un determinato livello conformemente a valutazioni svolte e obiettivi dell'organizzazione. Sviluppare capability di sicurezza all'interno di questo dominio coinvolge diverse attività, tra cui: (i) identificazione e analisi del rischio cyber, (ii) trattamento del rischio cyber, (iii) comunicazione del rischio cyber, (iv) gestione del rischio cyber di terze parti. Il "Cyber Risk Management" si integra all'interno dell'"Enterprise Risk Management" (ERM) per l'intera organizzazione ed ha lo scopo di definire e implementare un programma di gestione del rischio cyber che minimizzi la possibilità che l'organizzazione possa essere danneggiata dal verificarsi di attacchi cibernetici."

L'integrazione tra COSO ERM e la cybersecurity è cruciale per garantire la sicurezza aziendale e la continuità operativa.

Tutti i rischi cyber devono essere considerati, dai rischi relativi alle infrastrutture IT e al software applicativo, ai dati sensibili e alla catena di approvvigionamento, alla implementazione di misure di sicurezza per proteggere i sistemi e le informazioni da attacchi e minacce, al controllo accessi, alla formazione del personale, alla protezione dei sistemi IT e al monitoraggio della rete, alla gestione degli incidenti per rispondere in modo tempestivo e efficace agli attacchi informatici, al monitoraggio e controllo delle misure di sicurezza, etc.

Come sottolineato da ACN, per lo svolgimento del rischio Cyber "possono essere utilizzati i diversi framework di controlli disponibili come, ad esempio, ISO/IEC 27001, il CSF 2.0, l'"Italian Cybersecurity Report – Controlli Essenziali di Cybersecurity", il "CIS Critical Security Controls" o il NIST SP 800-53."

La valutazione del rischio cyber deve coinvolgere (come richiesto per tutti i rischi rilevanti considerati dal framework COSO ERM) le posizioni apicali dell'Impresa, adempimento di compliance richiamato con chiarezza dalla direttiva NIS2, con particolare focalizzazione sui rischi delle subforniture, sulla formazione cyber dei dipendenti e sui controlli di vulnerabilità dei sistemi digitali.

Umanesimo digitale, Intelligenza artificiale e cybersecurity

Consultando i motori di ricerca con la chiave "Umanismo digitale" si ha un' evidenza concreta della attualità del temine in numerose pubblicazioni e in articoli riportati su riviste che trattano tematiche di gestione aziendale e di formazione manageriale.

L'umanesimo digitale promuove un approccio più equilibrato e responsabile alla tecnologia, cercando di sfruttare i suoi vantaggi senza rinunciare ai valori umanistici che caratterizzano la società. Si tratta di un movimento che si rivolge a diverse aree, dall'istruzione alla salute, dal lavoro alla politica, con l'obiettivo di creare un'era digitale più inclusiva e umana.

Per le aziende l' Umanesimo digitale consiste, in particolare, nella progettazione e gestione di soluzioni digitali nel rispetto dell'etica e della sostenibilità, favorendo l'innovazione e uno sviluppo tecnologico inclusivo, utilizzando le tecnologie digitali in modo responsabile per ridurre l'impatto ambientale e promuovere uno sviluppo sostenibile, nel rispetto dei diritti delle persone. Soluzioni che, inevitabilmente, richiedono adeguati approcci metodologici di Controllo interno in grado di favorire anche la governance della tematica "Umanesimo digitale".

Abbiamo lasciato al termine dell'articolo un accenno alle implicazioni del Controllo Interno con l'Intelligenza artificiale, implicazioni che richiedono di considerare il rispetto dell'etica in generale e in particolare i contenuti dell' AI ACT, con l'inevitabile approfondimento dei controlli relativi alla cybersecurity e all' Umanesimo digitale, che rappresenta un nuovo paradigma che potrebbe aiutare le organizzazioni a navigare nel mondo digitale in modo più etico, responsabile e sostenibile.