compet-e

A TESISQUARE® ECOSYSTEM COMPANY

Compliance integrata di normative “risk based”: possibilità o necessità?

Un esempio virtuoso applicato a GDPR, NIS2 e DORA in ambito “rischio delle terze parti”.

04/08/2023

WHITEPAPER

Sommario

Introduzione

Analizzando le normative, le direttive, i regolamenti che hanno visto la luce negli ultimi anni non possiamo fare altro che constatare un preciso filo conduttore: una costante tendenza a chiedere agli enti e alle organizzazioni di adottare un approccio di **prevenzione e responsabilità nell'affrontare i temi delle compliance o conformità**.

Un approccio a queste tematiche non coordinato, a "silos verticali" separati, comporta sforzi e costi considerevoli.

Invece diventa vantaggioso **adottare un approccio integrato che unisca e coordini gli elementi comuni dei vari ambiti di compliance**.

Questa transizione è iniziata già alla fine del secolo scorso, quando il diritto d'impresa ha iniziato a evolversi passando dalla norma tradizionale alla cosiddetta "norma di compliance".

Adesso siamo di fronte alla necessità di operare un'ulteriore evoluzione culturale.

Il quadro storico - normativo

Negli ultimi anni, la normativa europea ha avuto un ruolo determinante nello stabilire il principio di **"compliance aziendale", basato sull'*accountability* e la responsabilità delle entità stesse**.

Questo principio segna in modo netto il passaggio da un approccio formale, basato solo sul rispetto delle leggi e dei regolamenti, a un approccio sostanziale basato sulla valutazione dei rischi (*risk-based approach*).

Il rispetto degli obblighi giuridici diviene veramente efficace quando non si basa più sul "principio di reazione" ma quando la conformità è ricercata tramite misure preventive adeguate, dove l'adeguatezza scaturisce da una sostanziale e non formale gestione dei rischi effettivi, propri di ogni singola organizzazione e relativo contesto.

Un esempio iniziale in Italia si trova nel decreto legislativo 626/94, che ha recepito **varie direttive europee in ambito di sicurezza e igiene sul lavoro, passando da un sistema sostanzialmente risarcitorio a uno di natura prevalentemente preventiva.**

Un passo ulteriore e significativo è stato fatto, sempre in Italia, negli anni Duemila con il decreto legislativo 231/01, che introduce la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*".

Con questa normativa, viene per la prima volta introdotto il concetto di "**colpa di organizzazione**".

L'azienda / ente può essere ritenuto responsabile in caso di mancanza di controllo e vigilanza, oltre alla mancanza di misure preventive e di protezione che hanno permesso la commissione di un reato.

Si assiste quindi a un cambiamento nell'approccio, passando da una responsabilità basata sul rispetto della normativa a un approccio pragmatico incentrato sulla responsabilizzazione.

La filosofia della prevenzione e della responsabilizzazione, tipica dei sistemi di compliance, ha subito un notevole sviluppo.

I legislatori, sia a livello comunitario che nazionale, **hanno esteso gli obblighi di conformità per garantire una maggiore prevenzione di illeciti all'interno delle attività aziendali**.

Pertanto, le aziende devono assicurarsi di essere conformi non solo alle regole stabilite dal decreto legislativo 231/01, ma anche a quelle riguardanti la Crisi di impresa, l'Antiriciclaggio, l'Anticorruzione e la trasparenza, l'Antitrust, la Tutela dei dati personali, nonché aspetti come il Bilancio di sostenibilità e di rispetto dell'ambiente.

Gli elementi dei sistemi di compliance

Nell'ambito dei sistemi di compliance, il privato-imprenditore/operatore economico si trova di fronte a due compiti principali: **valutare i potenziali rischi e adottare misure per ridurli e prevenire la responsabilità organizzativa**.

Molti sono gli elementi comuni che definiscono e costituiscono i sistemi di compliance.

Ad esempio, l'analisi del rischio è necessaria per creare il Modello di Organizzazione e Gestione, come richiesto dal d.lgs. 231/01, e la valutazione dell'impatto per misurare le conseguenze di possibili violazioni dei dati personali, come richiesto dal Regolamento (UE) 2016/679.

Altri settori, come la Salute e sicurezza sui luoghi di lavoro (d.lgs. 81/08), l'Antiriciclaggio, l'Anticorruzione e l'Antitrust, seguono una simile impostazione.

Il nuovo Codice della Crisi di impresa richiede una tempestiva rilevazione degli indicatori di allerta per prevenire o gestire la crisi e stabilire un modello organizzativo adatto.

Dopo aver valutato i rischi specifici per ciascun settore, **l'azienda deve adottare modelli organizzativi e misure tecniche e organizzative**.

Queste misure sono soggette a un frequente auditing per verificarne l'efficacia e il rispetto.

Quindi operare un **corretto, approfondito e continuativo approccio per rischi** è la chiave per rispondere correttamente e in modo adeguato a queste normative.

Se quindi la gestione del rischio è l'elemento fondante delle compliance e contemporaneamente si desidera approdare ad una "compliance integrata" necessariamente occorre rispondere preventivamente alla seguente domanda: è possibile effettuare una "analisi del rischio" integrata?

La risposta è affermativa.

Per appurarlo in modo completo ed esaustivo occorrerebbe una trattazione ben più ampia, che trascende dallo scopo (e dalle necessità editoriali) della presente pubblicazione. Pertanto ci dedicheremo, a tale scopo, unicamente ad una importante categoria di rischi: i "rischi di *supply chain*" che qui chiameremo, per semplicità, i rischi delle terze parti.

Rischi inerenti alle terze parti

Innanzitutto occorre definire con una certa precisione cosa si intende per terza parte.

La **Terza Parte** è un **fornitore esterno di servizi e/o prodotti**.

La terza parte mette a disposizione dell'azienda e dell'organizzazione il proprio *expertise* e le *best practices* del settore in cui opera, spesso integrandosi efficacemente e completamente all'interno dei processi produttivi e/o di erogazione di prodotti / servizi dell'azienda stessa.

Lavorare con una terza parte può introdurre dei rischi importati in una azienda o organizzazione in quanto:

- Se le terze parti hanno accesso a **dati "strategici"** esiste un **rischio per la sicurezza**;
- Se le terze parti hanno accesso a **dati personali**, specialmente se "sensibili o particolari", esiste un **rischio in ambito protezione dei dati;**
- Se le terze parti forniscono un componente o un servizio essenziale per l'azienda esiste un **rischio operativo**.

Pertanto il rischio delle terze parti deve essere monitorato dalle organizzazioni per individuare in quali casi esso superi la soglia di accettabilità stabilita dall'azienda stessa (livello di propensione al rischio o *risk appetite*).

Ma il monitoraggio del rischio delle terze parti è effettivamente una necessità trasversale a più norme?

È evidente che il tema del rischio dei soggetti terzi è centrale in diverse normative (schema alla pagina successiva).

Possono cambiare leggermente i termini con cui ci si afferisce ai soggetti:

- Il GDPR li chiama "**responsabili**"
- La 27001 più semplicemente "***supplie***r" e cioè fornitori, come la NIS2
- Il regolamento DORA li individua come "**terzi**"

ma è assolutamente evidente che il focus di ciascuna normativa è volto ad identificare e presidiare i rischi correlati ai soggetti, esterni all'organizzazione, che offrono a questi servizi strategici.

Il presidiare in modo "integrato" questi aspetti diventa indispensabile per creare efficacia ed efficienza nei propri processi di valutazione del rischio.

Come vegono chiamate le **terze parti**?

GDPR

GDPR art.. 28 par. 1
Il titolare "*…ricorre unicamente a **responsabili** del trattamento che presentino **garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato….*";

ISO 27001

Annex A ISO 27001:2022

- 5.19 ***Information security in supplier relationships***
- 5.20 *Addressing information security within **supplier agreements***
- 5.21 *Managing information security in the information and communication technology (ICT) **supply chain***

NIS2

Articolo 21 comma 2 lettera d. NIS2
Misure di gestione dei rischi di cybersicurezza: "*sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i **rapporti tra ciascun soggetto e i suoi fornitori.***"

DORA

Uno dei 6 pillar di DORA
Rischio Terze Parti (art. 1 comma1 lettera a) adozione di "*misure relative alla solida gestione dei **rischi informatici derivanti da terzi***".

Gli ingredienti indispensabili per adottare un approccio integrato al rischio

Passare da un approccio "a compartimenti stagni" ad un approccio integrato non è propriamente semplice.

Occorre intraprendere un percorso che preveda almeno i seguenti passi:

Evoluzione culturale: dalla compliance di settore alla compliance integrata

L'evoluzione culturale passa per il concetto concreto di "condivisione" delle informazioni. Spesso, all'interno di organizzazioni che hanno sempre operato con funzioni compartimentate, questo primo step non è assolutamente semplice e immediato.

E' quindi indispensabile che DPO, CISO, CIO, Legal, etc.... comincino a **comunicare ed avviare progetti comuni, scegliendo un linguaggio condiviso e comprensibile a tutti gli stakeholders** (non fatto solo né di bit & bytes, né solo di commi di legge).

Revisione / ristrutturazione dell'organizzazione e dei processi

Se ciascuna organizzazione deve strutturarsi per seguire le tematiche di compliance in maniera integrata, anche **i processi devono essere ridisegnati** per poter gestire al meglio le nuove esigenze.

I processi dovranno quindi acquisire un carattere meno "verticale" e più "trasversale" tra le varie aree aziendali.
Pensiamo a come potrebbe dover essere ridisegnato il processo di qualifica e valutazione dei rischi inerenti a un nuovo fornitore: L'*owner* (chi avvia e coordina il processo) potrebbe essere l'ufficio acquisiti ma questi, a seconda dei servizi offerti dal fornitore e delle garanzie che questi deve dare (ad esempio se tratta dati personali per conto dell'organizzazione, se offre servizi in cloud, se tratta informazioni strategiche) dovrà coinvolgere ulteriori figure quali, ad esempio, il DPO o il team privacy, gli esperti aziendali di sicurezza informatica, le aree aziendali che beneficeranno del servizio, ulteriori altri fornitori che dovranno integrarsi o collaborare con il nuovo soggetto esterno.

01 NUOVO FORNITORE

Acquisizione di un nuovo fornitore.

Ufficio acquisti, buyer, portale fornitori, ecc...

02 VALUTAZIONE

Processo di valutazione dei rischi della terza parte.

Ufficio acquisti, team privacy, internal audit, CIO, CISO, ecc...

03 AZIONI CONSEGUENTI

Azioni conseguenti in base al livello di rischio.

Ufficio acquisti, team privacy, internal audit, CIO, CISO, altro fornitore ecc...

04 MONITORAGGIO

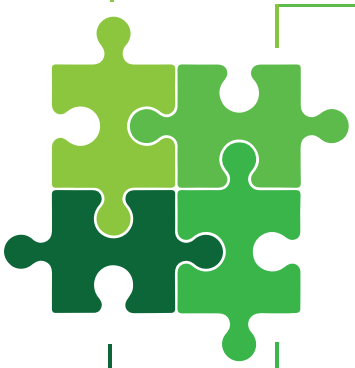
Monitoraggio periodico, audit.

Ufficio acquisti, team privacy, internal audit, CIO, CISO, altro fornitore ecc...

Definizione e attuazione del processo di valutazione del rischio

È chiaro che un approccio integrato tra varie normative al rischio delle terze parti sicuramente deve comportare la scelta di un'unica metodologia di analisi del rischio.
Finché i rischi sono un patrimonio "settoriale" di ogni ambito di compliance non c'è la necessità di approdare ad algoritmi comuni che prevedano anche criteri uniformi per l'accettazione o meno dei valori di rischio.

La metodologia scelta dovrà essere **la più oggettiva possibile**
.
A tale scopo dovrà contemperare, eventualmente anche con pesi diversi, elementi provenienti da almeno queste 4 fonti:



01 EXTERNAL SURVEY

Questionari, interviste di valutazione / autovalutazione devono essere somministrati alle terze parti.

02 INTERNAL SURVEY

Questionari, interviste di valutazione / autovalutazione devono essere somministrati ai soggetti interni che presidiano determinati temi (acquisti, team privacy, security, ecc...)

03 EXTERNAL DATABASE

Devono essere interrogate eventuali fonti esterne che riportano informazioni sulla terza parte.

04 INTERNAL DATABASE

Devono essere scandagliati database e archivi interni per scoprire se esistono già evidenze sulla terza parte.

Scelta e acquisizione degli strumenti utili a supportare i processi di valutazione

Quest'ultimo passo, che deve compiere l'organizzazione, dovrebbe essere il più semplice rispetto ai tre precedenti: spesso, invece, nasconde insidie e criticità.

La scelta di uno strumento "sbagliato" (da intendersi "***non in linea con il contesto e le aspettative dell'organizzazione***") può avere conseguenze devastanti quali il naufragio del progetto stesso. Spesso, nelle aziende, le inerzie settoriali e corporative, ostili all'integrazione, tenteranno di far percepire un errore di mezzo / strumento come un errore di impostazione / obiettivo strategico di base.

Nella valutazione dello strumento di supporto l'organizzazione dovrà innanzitutto fare una prima scelta di campo:

- Affidarsi a modelli di valutazione basati su strumenti di office;
- Affidarsi a tool software appositamente dedicati.

Non esiste una scelta a priori più corretta dell'altra; tuttavia la scelta va operata tenendo conto del contesto dell'organizzazione, delle risorse a disposizione nella fase di startup del progetto e nel "day by day", nella gestione dei processi di valutazione (centralizzati o distribuiti), etc...

	STRUMENTI OFFICE	TOOL DEDICATO
Costi di acquisizione	★★★★★	★★★☆☆
Costi di implementazione	★★★★☆	★★★☆☆
Facilità di rimodulazione degli algoritmi e dei processi	★★☆☆☆	★★★★☆
Facilità nella gestione degli aspetti collaborativi	★☆☆☆☆	★★★★★
Facilità nella gestione delle azioni legate al valore di rischio	★★★☆☆	★★★★☆
Livello di supporto nel «day by day»	★★☆☆☆	★★★★☆
Capacità di conservazione e raffronto dei dati su base storica	★★☆☆☆	★★★★★

(1=livello di supporto basso | 5 = livello di supporto massimo)

Si evince che:

- Gli **strumenti di office** hanno generalmente **bassi costi di acquisizione** e implementazione ma pagano dazio sugli aspetti di rimodulazione, sugli aspetti collaborativi e nella conservazione dei dati su base storica (anche per analisi comparative e raffronti);

- I **tool dedicati** spesso hanno invece **costi significativi** sia di acquisizione che di implementazione iniziale; generalmente però **offrono maggiore supporto** nella rimodulazione degli algoritmi, nel *day by day* (anche collaborativo) e nei processi di raffronto e analisi dei dati su base storica.

Tuttavia non si deve fare l'errore di intendere il soprastante schema come la cartina di tornasole assoluta per la scelta dello strumento di analisi e valutazione dei rischi.

Ciò perché non tutte le direttrici espresse nello schema soprastante hanno lo stesso valore e peso per tutte le organizzazioni; inoltre vi possono essere altre direttrici, qui non indicate, che invece sono strategiche per alcune organizzazioni e il non contemperarle potrebbe minare alla base il processo di scelta.

Conclusioni

Il quadro normativo che impatta le compliance delle organizzazioni è in costante evoluzione.

Dopo il GDPR, la ISO 27001 nell'edizione 2022, NIS2, DORA altre sfide stanno per sopraggiungere (Regolamento e-Privacy, Regolamento su Intelligenza artificiale, etc…).

Tutte queste norme, sia cogenti che volontarie, necessitano di un approccio per rischi, tema che abbiamo visto come sia non solo opportuno ma indispensabile indirizzare in un'ottica integrata.

Come abbiamo visto pure in questa sintetica trattazione: tutto ciò **"si può fare!"**, per citare Gene Wilder in una scena cult del film Frankenstein Junior di Mel Brooks.

Tuttavia, proprio per evitare di generare creature alla **Frankenstein**, il modello integrato va adeguatamente preparato con un'evoluzione culturale, una revisione della propria organizzazione e dei propri processi, un'opportuna metodologia e, "*last but not least*", gli opportuni strumenti operativi di supporto.

Se ciò avviene non solo garantisce maggiore coerenza al sistema di compliance aziendale, ma consente anche di ridurre costi ed energie, evitando sovrapposizioni e duplicazioni, **rendendo il sistema stesso più efficace ed efficiente**.

Risorse utili

Abbiamo parlato del rischio terze parti al Privacy Day 2023.
Guarda lo speech di Piermaria Saglietto (CEO Compet-e)
https://youtu.be/oqClic3Vr7w

Strumenti a supporto: GRC CORA - La suite per la compliance integrata
www.grccora.com

Informazioni su Compet-e e sui servizi offerti
www.compet-e.com

compet-e

La nostra mission è quella di creare soluzioni e fornire consulenza e supporto in ambito GRC e RegTech in diversi ambiti di compliance.

Offriamo soluzioni che aiutano i nostri clienti adutilizzare al meglio le proprie risorse e le proprie informazioni, salvaguardando gli investimenti effettuati nel tempo.

SEDE DI BRA
via Don Luigi Orione, 202/G
12042 - Bra (CN)

SEDE DI ROMA
viale Giorgio Ribotta, 11
00144 - Roma (RM)
)

COMPET-E SRL
Tel: 0172-382763 - Fax: 0172-1832072
C.F. e P.IVA 0276097042
www.compet-e.com