Panoramica di Governance, Risk e Compliance (GRC) di Insight

Insight

Introduzione

In termini semplici, il GRC consiste nel creare fiducia: fiducia nei confronti dei clienti, fiducia nei confronti delle autorità di regolamentazione e fiducia all'interno della propria organizzazione che opera in modo responsabile e resiliente.

I pilastri fondamentali della GRC:

1 Governance

Stabilire il tono dall'alto dell'organizzazione e tradurlo in policy chiare. Questo è l'impegno della leadership a fare le cose nel modo giusto, dall'etica dei dati alla responsabilità aziendale. Una governance forte significa che i tuoi team hanno la capacità di prendere decisioni allineate con gli obiettivi e i valori aziendali.

2 Risk Management

Identificare ciò che potrebbe andare storto (dalla perdita accidentale di dati agli attacchi ransomware) e mitigarlo proattivamente. Si tratta di prevedere cosa potrebbe accadere e di essere preparati. Le aziende che gestiscono bene i rischi hanno meno crisi e, quando si presentano problematiche, le gestiscono in modo rapido ed efficace. Acquisisci sicurezza nel fare scommesse strategiche perché ti sei tutelato contro i rischi al ribasso.

3 Conformità

Rispettare le regole, che si tratti di leggi come il GDPR, di standard di settore come ISO o di codici di condotta interni. Non si tratta solo di "rendere felici le autorità di regolamentazione", ma anche di assicurare ai clienti e ai partner che prendi sul serio la sicurezza e la privacy. La conformità crea fiducia e apre le porte: ad esempio, essere certificati (ad es. ISO 27001) può rappresentare un lasciapassare per fare affari con clienti importanti che esigono la prova delle buone pratiche.

Il business case per la GRC

La trascuratezza della governance, della gestione del rischio o della conformità può esporre un'organizzazione a gravi conseguenze:

- **Perdita finanziaria:** Le violazioni dei dati, le frodi o le sanzioni normative possono comportare costi finanziari diretti (multe, spese legali, spese di correzione delle violazioni) nonché perdite di profitti dovute all'interruzione dell'attività. In particolare, gli studi dimostrano che la non conformità costa alle aziende molto di più del costo della conformità stessa.
- **Interruzione dell'attività:** I rischi non gestiti (come gli attacchi informatici o i guasti dei processi) possono bloccare le operazioni e causare tempi di inattività, compromettendo la produttività e l'erogazione dei servizi. Ad esempio:un attacco ransomware potrebbe bloccare i sistemi critici per giorni. Le pratiche GRC aiutano a identificare e mitigare tali rischi prima che si materializzino, preservando la continuità aziendale.
- **Danni alla reputazione:** La fiducia è difficile da guadagnare e facile da perdere. I difetti di conformità o le lacune etiche rovinano la fiducia dei clienti e degli stakeholder. Una violazione dei dati o uno scandalo di conformità reso pubblico possono danneggiare un marchio per anni, spingendo i clienti ad abbandonarlo. Una governance e una conformità solide dimostrano al pubblico, ai partner e alle autorità di regolamentazione che l'organizzazione è responsabile e affidabile.
- **Sanzioni normative:** Le autorità di regolamentazione stanno sempre più applicando leggi con multe pesanti e persino sanzioni penali per la non conformità. Ad esempio, ai sensi del GDPR dell'UE, le sanzioni possono arrivare fino a 20 milioni di euro o al 4% del fatturato annuo globale in caso di violazioni gravi.

Infatti, dal 2018, le autorità di regolamentazione in Europa hanno imposto sanzioni GDPR pari a 5,88 miliardi di euro, inclusa una sanzione record di 1,2 miliardi di euro nei confronti di una singola azienda.Il GRC aiuta a garantire che tutti i controlli e le segnalazioni richiesti siano in atto per evitare tali sanzioni.

In sintesi, investire nella GRC è molto più economico e sicuro rispetto a gestire le conseguenze di mancate conformità o incidenti gravi. Un programma GRC coerente protegge la **salute finanziaria, la continuità operativa e la reputazione pubblica** dell'organizzazione, consentendo al contempo un migliore processo decisionale e un migliore allineamento strategico. Come ha sintetizzato sinteticamente uno studio, *"la non conformità costa quasi tre volte tanto rispetto alla conformità"*

En moyenne, les organisations dépensent 5,47 millions $ par an pour la conformité, mais 14,82 millions $ en cas de non-conformité – le coût de la non-conformité est environ 2,7 fois plus élevé. Ces pertes incluent les temps d'arrêt de l'activité, la réponse aux incidents et la perte de clients.

Quadri normativi e regolamenti chiave

Nel panorama della GRC, esistono molti standard, quadri normativi e regolamenti che le organizzazioni potrebbero dover seguire. Di seguito una panoramica di quelli principali: cosa sono e come si applicano alle diverse organizzazioni:

Quadro normativo/ Regolamento	Scopo	Applicabilità	Implicazioni chiave della GRC
ISO/IEC 27001	Stabilisce un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) per proteggere sistematicamente le informazioni.	Tutti i settori a livello globale (finanza, tecnologia, produzione, ecc.).	Linea di base per la governance della cybersecurity; spesso si sovrappone alla NIS2 e ad altri framework. La certificazione dimostra un solido livello di sicurezza.
Cyber Essentials Plus	Programma sostenuto dal governo del Regno Unito per una cyber hygiene di base attraverso cinque controlli chiave.	Aziende con sede nel Regno Unito, in particolare PMI e fornitori della pubblica amministrazione.	Fornisce garanzia di protezioni essenziali. Audit indipendente richiesto per il livello "Plus". Spesso un punto di accesso alla sicurezza strutturata.
CAF (Cyber Assessment Framework)	Sviluppato dal NCSC del Regno Unito, il CAF fornisce un approccio strutturato per valutare la resilienza informatica delle organizzazioni che gestiscono funzioni critiche.	Organizzazioni del Regno Unito nei settori delle infrastrutture nazionali critiche (CNI) e operatori di servizi essenziali, in particolare ai sensi delle normative NIS del Regno Unito.	Allinea i controlli tecnici con i risultati di governance. Contribuisce a dimostrare la maturità rispetto ai principi allineati al NIS. Supporta le decisioni basate sul rischio e il dialogo normativo. Spesso utilizzato insieme alla norma ISO 27001 o all'assurance interna.
EU AI Act	Legislazione UE che disciplina i sistemi di AI in base alla categoria di rischio (ad es. sistemi ad alto rischio come il credit scoring).	Qualsiasi organizzazione che offra AI sul mercato europeo.	L'AI ad alto rischio richiede documentazione, gestione del rischio e supervisione continua. Una solida governance dell'AI aiuta a garantire la conformità e l'accesso al mercato.
Direttiva NIS2	Norme sulla cybersecurity a livello UE per le infrastrutture critiche e digitali.	Entità medio-grandi in settori chiave (energia, telecomunicazioni, cloud, produzione, sanità, ecc.) compresi i fornitori extra-UE che servono l'UE.	Richiede sicurezza basata sul rischio, segnalazione degli incidenti, sicurezza della supply chain. Le sanzioni sono in linea con le multe previste dal GDPR. Si sovrappone notevolmente alla norma ISO 27001.

Framework / Regulation	Purpose	Applicability	Key GRC Implications
GDPR	Regolamento UE per la gestione del consenso ai dati personali, dei diritti alla privacy, della notifica delle violazioni, ecc.	Qualsiasi organizzazione che tratta i dati personali dei residenti nell'UE.	La protezione dei dati sta diventando una questione a livello di consiglio di amministrazione. Richiede una governance solida, inventari di dati, DPO e una rapida segnalazione delle violazioni. Sanzioni significative per non conformità.
SOC 2	Quadro di riferimento sviluppato negli Stati Uniti per valutare i controlli interni per la protezione dei dati, in particolare nel cloud/SaaS.	Fornitori di tecnologie e servizi, in particolare nel B2B o SaaS.	Volontaria ma spesso richiesta contrattualmente. Dimostra una solida sicurezza operativa e crea fiducia.
PCI-DSS	Standard industriale globale per proteggere i dati dei titolari di carta e ridurre le frodi.	Qualsiasi entità che archivia, elabora o trasmette i dati di carte di credito.	Obbligatorio per commercianti ed elaboratori di pagamenti. Richiede controlli rigorosi e audit regolari da parte di organismi di valutazione della conformità certificati.
DORA (Digital Operational Resilience Act)	Regolamento UE per garantire che le aziende del settore finanziario possano resistere e riprendersi da interruzioni correlate alle ICT.	Entità finanziarie che operano nell'UE, tra cui banche, assicuratori, società di investimento e fornitori terzi essenziali.	Richiede una solida gestione del rischio ICT, la segnalazione degli incidenti, i test di resilienza operativa digitale e la supervisione del rischio di terzi. Integra NIS2 e GDPR.

Conformità a molteplici normative / quadri normativi

Oggi le organizzazioni raramente hanno a che fare con una sola serie di requisiti di conformità. Più spesso, si trovano ad affrontare un mosaico di legislazioni, obblighi normativi e quadri normativi di settore sovrapposti. Che si tratti di GDPR, NIS2, ISO 27001, DORA o standard specifici del settore come PCI-DSS, il panorama della conformità può diventare rapidamente complesso e impegnativo da gestire.

Tuttavia, ciò che molte organizzazioni non si rendono conto è solo la quantità di sovrapposizione tra questi vari requisiti. Principi fondamentali come la valutazione del rischio, il controllo degli accessi, la risposta agli incidenti e la governance sono i fili conduttori della maggior parte delle normative sulla cybersecurity e sulla privacy. Pertanto, un approccio intelligente e integrato alla conformità può ridurre significativamente la duplicazione degli sforzi.

Invece di trattare ogni normativa in modo isolato, le organizzazioni leader adottano un approccio unificato, mappando i controlli e i processi su più standard e costruendo una postura di sicurezza che li soddisfi collettivamente. Ad esempio, un'organizzazione certificata ISO 27001 è già sulla buona strada per soddisfare i requisiti di sicurezza della NIS2 - forse l'80% del tempo.

Costruendo un quadro di conformità centralizzato e basato sui controlli, le organizzazioni possono semplificare gli audit, ridurre i costi e garantire che la sicurezza diventi una pratica sostenibile e allineata al business piuttosto che un'esercitazione continua.

Strumenti di automazione della conformità

- Tenere traccia dei requisiti normativi come ISO 27001, NIS2, GDPR, PCI-DSS e altri può diventare facilmente insostenibile, soprattutto quando ognuno presenta una propria serie di controlli, richieste di prove e requisiti di audit.
- È qui che entrano in gioco la conformità e gli strumenti di automazione GRC (Governance, Risk and Compliance).
- Queste piattaforme aiutano le organizzazioni a mappare, gestire e monitorare i controlli su più framework, identificando le sovrapposizioni e semplificando gli sforzi di conformità. Invece di duplicare il lavoro per ogni standard, gli strumenti di automazione consentono di implementare un controllo una sola volta, ad esempio per il controllo degli accessi o la risposta agli incidenti, e quindi di mapparlo ai requisiti pertinenti in più normative.

I vantaggi includono:

- **Riduzione delle duplicazioni e delle rilavorazioni:** Implementa i controlli una sola volta e riutilizzali in tutti i framework.
- **Conformità continua:** La raccolta automatizzata delle prove, il monitoraggio dei controlli e la gestione del flusso di lavoro aiutano a garantire che siate sempre pronti per gli audit.
- **Visibilità chiara:** Le dashboard e i report forniscono agli stakeholder una visione in tempo reale dello stato di conformità e dell'esposizione ai rischi in tutta l'organizzazione.
- **Efficienza dei costi:** La documentazione centralizzata e la mappatura automatica dei controlli rendono gli audit interni ed esterni più rapidi e meno fastidiosi.
- **Scalabilità:** Man mano che le normative evolvono o emergono nuovi standard, gli strumenti di automazione possono adattarsi, evitando di dover reinventare costantemente il programma di conformità..

Gli strumenti di conformità ti aiutano a trasformare la corsa annuale alla ricertificazione in un processo solido che funziona tutto l'anno, così da conoscere sempre la tua posizione in materia di conformità e avere il tempo necessario per colmare eventuali lacune.

Fatti e cifre

Costo della non conformità rispetto alla conformità: È ben documentato che la mancata conformità è molto più costosa degli investimenti necessari. Uno studio comparativo ha rilevato il costo medio della conformità (implementazione di politiche, formazione, audit, ecc.) per le grandi aziende era di ~5,5 milioni di dollari all'anno, mentre il costo medio della non conformità (tramite multe, interruzioni aziendali, perdita di produttività e correzione) era di ~14,8 milioni di dollari, quasi 3 volte superiore
Riferimento: **corporatecomplianceinsights.com**

Tendenze normative: Gli enti normativi stanno applicando attivamente la conformità. Per quanto riguarda la privacy dei dati, ad esempio, le sanzioni del GDPR hanno totalizzato **5,88 miliardi di euro** dal 2018 al 2024 in tutta Europa
Riferimento: **dlapiper.com**

Su una nota positiva, le aziende con solidi programmi di conformità possono spesso negoziare sanzioni più basse o evitare del tutto le violazioni. Con l'entrata in vigore di normative come l'AI Act dell'UE e il NIS2, ci aspettiamo che un'iniziale ondata di applicazioni di alto profilo faccia capire chiaramente il concetto, proprio come è avvenuto nei primi anni del GDPR, rafforzando ulteriormente la necessità di funzionalità GRC mature.

Adozione di programmi GRC e di conformità: La maggior parte delle organizzazioni riconosce la necessità della GRC. Secondo l'indagine globale di Accenture, il **95% delle aziende ha creato o sta costruendo una "cultura della conformità"** in tutta l'azienda. Ciò indica una consapevolezza quasi universale a livello di leadership che la conformità e l'etica devono far parte della cultura aziendale. Tuttavia, la maturità varia: solo il 36% delle organizzazioni dispone di un programma formale di gestione del rischio aziendale (ERM). Ciò suggerisce che, sebbene la maggior parte delle aziende intenda essere conforme, molte stanno ancora sviluppando l'infrastruttura e i processi per una GRC completa. Man mano che le organizzazioni si trovano ad affrontare nuovi rischi (minacce informatiche, interruzioni della catena di fornitura, impatti della pandemia), i consigli di amministrazione spingono sempre più a una migliore supervisione dei rischi. Infatti, il **36% delle organizzazioni prevede di aumentare gli investimenti nella gestione del rischio e nella conformità nei prossimi due anni.**
Riferimento: **procurementtactics.com**

Volume delle modifiche normative: Una delle maggiori sfide per la conformità è tenere il passo con le nuove leggi e gli aggiornamenti. A livello globale, sono centinaia le agenzie di regolamentazione che rilasciano aggiornamenti ogni giorno e questo ritmo è aumentato solo con le normative sulla privacy e sulla finanza negli ultimi anni. Questo "tsunami" di normative implica che le organizzazioni abbiano bisogno di meccanismi (spesso basati sulla tecnologia, come feed normativi nei sistemi GRC o abbonamenti a servizi di aggiornamento sulla conformità) per monitorare i cambiamenti rilevanti.

Crescita del mercato e futuro della GRC: Il mercato della tecnologia GRC è in rapida crescita, poiché le aziende sono alla ricerca di software per gestire queste complessità. Secondo alcune stime, il **mercato globale del software GRC** valeva circa 5 miliardi di dollari nel 2023 e si prevede che **quasi raddoppierà entro il 2029** (avvicinandosi a 9-10 miliardi di dollari) con l'aumento della domanda di strumenti di gestione del rischio integrati.
Riferimento: **verdantix.com**

Assicurazione sulla cybersecurity e GRC: Gli assicuratori che forniscono assicurazioni contro i rischi informatici ora esaminano attentamente le misure GRC dei clienti (ad esempio se seguono quadri normativi come ISO27001 o hanno determinate certificazioni di conformità) quando sottoscrivono le polizze. Un solido programma GRC può quindi ridurre i premi assicurativi e fornire un altro incentivo finanziario alle aziende per investire nella conformità e nella gestione del rischio.

Siete pronti per la governance, il rischio e la conformità?

1. Governance - Leadership e responsabilità

- [ ] Hai un modello formale di governance che definisce politiche, ruoli e responsabilità per il rischio e la conformità?
- [ ] Il tuo consiglio di amministrazione/dirigente è coinvolto nel processo decisionale in materia di rischio e conformità?
- [ ] Esegui revisioni regolari delle politiche di governance per garantire che siano allineate agli obiettivi aziendali e ai cambiamenti normativi?
- [ ] Esiste un codice etico e di condotta documentato per i dipendenti e la dirigenza?
- [ ] I fornitori e i partner terzi sono soggetti a governance e supervisione del rischio?

Se hai risposto "No" a una di queste domande, potresti avere delle lacune nella supervisione della governance.

2. Gestione del rischio - Identificazione e mitigazione delle minacce

- [ ] Tieni un registro dei rischi che documenti i rischi aziendali, di cybersecurity, finanziari e operativi?
- [ ] I rischi vengono valutati e classificati in base all'impatto e alla probabilità?
- [ ] Conduci valutazioni regolari dei rischi (cybersecurity, operativi, finanziari, reputazionali, supply chain, ecc.)?
- [ ] Disponi di una strategia formale di mitigazione dei rischi che assegni i responsabili e stabilisca le tempistiche per le azioni correttive?
- [ ] Esiste un piano di continuità aziendale e di ripristino di emergenza per i sistemi e le operazioni chiave?

Se hai risposto "No" a una di queste domande, potresti essere esposto a rischi non affrontati.

2. Conformità - Riunione degli standard normativi e di settore

- [ ] Conosci i regolamenti e i quadri normativi chiave applicabili al tuo settore (ad es. GDPR, ISO 27001, NIS2, PCI DSS, SOC 2, governance dell'IA, ecc.)?
- [ ] Disponi di politiche e controlli formali di conformità per queste normative?
- [ ] La conformità viene regolarmente monitorata e verificata internamente o esternamente?
- [ ] Disponi di strumenti automatizzati di monitoraggio della conformità o di reportistica?
- [ ] Sei in grado di fornire rapidamente una documentazione pronta per gli audit in caso di revisione normativa?

Se hai risposto "No" a una di queste domande, potresti essere esposto a rischi normativi o finanziari.

3. Cybersecurity e protezione dei dati - Operazioni sicure

- [ ] Disponi di una politica di cybersecurity documentata che sia in linea con i requisiti di conformità?
- [ ] Negli ultimi 12 mesi hai condotto una valutazione dei rischi informatici?
- [ ] Gli impiegati sono formati sulla consapevolezza della sicurezza e sugli obblighi di conformità?
- [ ] Disponi di di protocolli di risposta agli incidenti e di segnalazione delle violazioni?
- [ ] I dati sensibili sono protetti tramite cifratura, controlli di accesso e classificazione dei dati?

Se hai risposto "No" a una di queste domande, la tua postura di sicurezza potrebbe non essere allineata alle best practice GRC.

4. Monitoraggio e miglioramento continuo

- [ ] La GRC è integrata nella cultura della tua organizzazione piuttosto che essere trattata come un progetto una tantum?
- [ ] Disponi di una piattaforma tecnologica GRC per gestire governance, rischio e conformità in un unico luogo?
- [ ] Le attività di conformità e rischio vengono regolarmente riviste, testate e aggiornate in base alle nuove minacce o ai cambiamenti normativi?
- [ ] Sei coinvolto in assessment o audit di terze parti continui per garantire la conformità?
- [ ] La reportistica sulla conformità è automatizzata e integrata nelle tue operazioni aziendali?

Se hai risposto "No" a una di queste domande, i tuoi sforzi GRC potrebbero non essere sostenibili ed efficienti.

Come ti aiutiamo - Il tuo partner GRC di fiducia

Noi di Insight siamo consapevoli che un attenzione alle regole di Governance, Risk and Compliance (GRC) non sia solo un adempimento formale. Si tratta di proteggere la tua reputazione, consentire un processo decisionale sicuro e garantire che tu possa crescere senza incorrere in rischi normativi o operativi.

Ti aiutiamo a gestire questa complessità con un approccio olistico, pratico e tecnologico alla GRC che offre resilienza e agilità.

Servizi di consulenza e audit:

I nostri consulenti esperti ti aiutano a comprendere i tuoi obblighi, a confrontarli con gli standard più importanti e a tracciare un percorso chiaro da seguire.
Valutazioni dei gap e revisioni della prontezza: per ISO 27001, Cyber Essentials+, NIS2, CAF e altro ancora
Policy & Framework Design: creazione di programmi scalabili di governance, gestione del rischio e conformità su misura per la tua azienda.
Board & Executive Reporting: tradurre la strategia GRC in informazioni significative sui rischi aziendali per la leadership.
Internal Audit Support: compresa la preparazione delle prove, la pianificazione delle azioni correttive e la garanzia continua.

Servizi GRC gestiti

Se non disponi della larghezza di banda o delle competenze interne, la nostra offerta GRC gestita mantiene il tuo programma di conformità in funzione senza problemi.
Gestione continua del rischio e della conformità: gestiamo i test di controllo, i problemi tracciamento e reportistica.
Virtual CISO or Virtual Information Security Officer : accedi al supporto di esperti senza dover costruire un team interno completo.

Perché i clienti scelgono Insight

Affidabile in tutti i settori: dai servizi finanziari alla sanità, produzione alla tecnologia.
Certificati secondo gli standard che ti aiutiamo a soddisfare, tra cui: ISO 27001 e Cyber Essentials+.
Indipendente dal fornitore: lavoriamo con le principali piattaforme GRC, ma la nostra consulenza inizia con i tuoi obiettivi, non con una presentazione del prodotto.
Allineati al business: parliamo la lingua sia del consiglio di amministrazione che del back office.