Comportamento organizzativo

Requisito Tematico

Topical Requirement

User Guide

The Institute of Internal Auditors

Tradotto da:¶

Associazione Italiana Internal Auditors

Contenuti

Introduzione ai Requisiti Tematici

I Requisiti Tematici sono un elemento essenziale dell'International Professional Practices Framework® (IPPF), insieme ai Global Internal Audit Standards™ e alle Global Guidance. L'Institute of Internal Auditors (IIA) richiede che i Requisiti Tematici siano utilizzati in combinazione con gli Standards, che costituiscono la base autorevole per le pratiche di Audit richieste. All'interno di questa guida sono presenti riferimenti agli Standards che forniscono informazioni più dettagliate.

I Requisiti Tematici formalizzano il modo in cui gli Internal Auditor affrontano le aree di rischio prevalenti, promuovendo qualità e coerenza all'interno della professione. Il Mandato di Internal Audit definisce chiaramente l'ambito e i tipi di servizi svolti dalla funzione di Internal Audit, che includono gli aspetti da valutare dei Requisiti Tematici (Standard 6.1 Mandato di Internal Audit). Essi stabiliscono una base di riferimento e forniscono criteri pertinenti per l'esecuzione dei servizi di assurance relativi alla tematica trattata dal Requisito (Standard 13.4 Criteri di valutazione). La conformità ai Requisiti Tematici è obbligatoria per i servizi di assurance e raccomandata per la valutazione durante i servizi di advisory. Tuttavia, i requisiti non intendono coprire tutti gli aspetti potenzialmente rilevanti per un incarico di assurance, ma forniscono un insieme minimo di requisiti per garantire una valutazione coerente e affidabile dell'argomento trattato.

I Requisiti Tematici sono strettamente collegati al Three Lines Model dell'IIA e ai Global Internal Audit Standards. I processi di governance, risk management e controllo sono i principali componenti dei Requisiti Tematici, in linea con lo Standard 9.1 Comprensione dei processi di governance, risk management e controllo. Con riferimento al Three Lines Model, la governance è connessa al Board o all'organo di governo, il risk management è connesso alla seconda linea, mentre i controlli o i processi di controllo alla prima linea. Mentre il management si colloca nella prima e nella seconda linea, la funzione di Internal Audit si colloca nella terza linea per fornire assurance indipendente e obiettiva, riportando al Board o all'organo di governo (Principio 8 Sottoposta alla supervisione del Board).

Applicabilità, Rischio e Giudizio Professionale

I Requisiti Tematici devono essere applicati quando le funzioni Internal Audit svolgono incarichi di assurance su temi per i quali esiste un Requisito Tematico, oppure quando elementi di tale requisito emergono all'interno di altri incarichi di assurance.

Come descritto negli Standard, il risk assessment è un elemento fondamentale nella pianificazione del Chief Audit Executive (CAE). Definire gli incarichi di assurance da includere nel piano di Audit richiede una valutazione periodica, almeno annuale, delle strategie, degli obiettivi e dei rischi dell'organizzazione (Standard 9.4 Piano di Audit). Nella pianificazione degli incarichi di assurance, gli Internal Auditor devono valutare i rischi rilevanti per l'incarico (Standard 13.2 Risk Assessment dell'incarico).

Se durante il processo di pianificazione risk-based dell'Internal Audit viene identificato e inserito nel Piano di Audit un argomento tra quelli oggetto di un Requisito Tematico, i rispettivi requisiti devono essere applicati in tutti gli incarichi in cui si valuta l'argomento. Inoltre, quando gli Internal Auditor svolgono un incarico (sia esso previsto o meno nel piano di Audit) ed emergono elementi riconducibili a un Requisito Tematico, quest'ultimo deve essere valutato per determinarne l'applicabilità nell'ambito dell'incarico stesso. Infine, se viene richiesto un incarico non originariamente previsto nel piano di Audit, ma che riguarda un argomento coperto da un Requisito Tematico, è necessario valutarne l'applicabilità.

Il giudizio professionale svolge un ruolo fondamentale nell'applicazione del Requisito Tematico. Il risk assessment guida le decisioni dei CAE riguardo agli incarichi da includere nel Piano di Audit (Standard 9.4 Piano di Audit). Inoltre, gli Internal Auditor applicano il giudizio professionale per determinare quali aspetti devono essere inclusi nell'ambito di ciascun incarico (Standard 13.3 Obiettivi e ambito dell'incarico, 13.4 Criteri di valutazione, 13.6 Programma di lavoro) e per identificare le risorse necessarie per raggiungere gli obiettivi dell'incarico (Standard 13.5 Assegnazione delle risorse).

Deve essere conservata evidenza della valutazione di applicabilità di ciascun requisito previsto dal Requisito Tematico, inclusa una motivazione che ne spieghi l'eventuale esclusione. La conformità al Requisito Tematico deve essere documentata secondo il giudizio professionale degli Auditor, come previsto nello Standard 14.6 Documentazione dell'incarico.

Sebbene il Requisito Tematico fornisca una base di riferimento dei processi di controllo da considerare, le organizzazioni che associano all'argomento un rischio elevato potrebbero dover analizzare ulteriori aspetti.

Se il CAE constata che la funzione Internal Audit non possiede le competenze necessarie per svolgere incarichi di Audit su un argomento specifico di un Requisito Tematico, l'incarico può essere affidato a un fornitore di servizi esterno (Standard 3.1 Competenza, 7.2 Qualifiche del Chief Audit Executive, 10.2 Risorse Umane). Gli Standard si applicano a qualsiasi individuo o funzione che svolge attività di Internal Auditing, indipendentemente dal fatto che un'organizzazione impieghi Auditor interni, si avvalga di un fornitore esterno di servizi o entrambi. Il CAE mantiene la responsabilità ultima di garantire la conformità. Inoltre, qualora il CAE ritienga che le risorse interne a disposizione della Funzione siano insufficienti, deve informare il Board sugli impatti derivanti da questa limitazione e alle misure che saranno adottate per ovviare a tale carenza (Standard 8.2 Risorse).

Performance, Documentazione e Reporting

Nell'applicare i Requisiti Tematici, gli Internal Auditor devono anche conformarsi agli Standard, svolgendo il loro lavoro in linea con la Sezione V: Svolgimento delle attività di Internal Auditing. Gli Standard della Sezione V descrivono la pianificazione degli incarichi (Principio 13 Pianificare gli incarichi in modo efficace), la conduzione degli incarichi (Principio 14 Condurre l'incarico) e la comunicazione dei risultati degli incarichi (Principio 15 Comunicare i risultati dell'incarico e monitorare i piani d'azione).

I Requisiti Tematici sono concepiti per supportare pratiche di Internal Audit coerenti e di alta qualità. Essi devono essere applicati congiuntamente a leggi locali, normative, aspettative delle

autorità di vigilanza e altri framework riconosciuti a livello professionale, che possono imporre requisiti aggiuntivi o più specifici. Gli Internal Auditor potrebbero aver già sviluppato programmi di lavoro dell'incarico e procedure di testing in linea con tali normative e framework. Gli Internal Auditor dovrebbero allineare al Requisito Tematico i test previsti per i controlli sul comportamento organizzativo ed eventuali test affidabili forniti da altri assurance provider interni ed esterni (Standard 9.5 Coordinamento e reliance), al fine di garantire un'adeguata copertura.

La copertura del Requisito Tematico può essere documentata nel Piano di Audit o nel programma di lavoro dell'incarico, in base al giudizio professionale degli Auditor. I requisiti possono essere coperti da uno o più incarichi di Internal Audit. Inoltre, i requisiti potrebbero non essere tutti applicabili. È necessario conservare evidenza dell'avvenuta valutazione dell'applicabilità del Requisito Tematico, inclusa una motivazione che spieghi eventuali esclusioni.

Quality Assurance

Gli Standard prevedono che il CAE sviluppi, attui e mantenga un programma di assurance e miglioramento della qualità che copra tutti gli aspetti della funzione Internal Audit (Standard 8.3 Qualità). I risultati devono essere comunicati al Board e al Top Management. Le comunicazioni devono riportare la conformità della funzione Internal Audit agli Standard e il raggiungimento degli obiettivi di performance.

La conformità ai Requisiti Tematici dovrebbe essere tenuta in considerazione nelle attività di supervisione a livello di incarico (Standard 12.3 Supervisione e miglioramento della performance dell'incarico) e sarà valutata nei quality assessment.

Comportamento organizzativo

Ridefinire l'Audit della cultura

Il passaggio dal considerare l'Audit della cultura un argomento astratto e vago al considerarlo una valutazione strutturata e precisa del comportamento organizzativo rappresenta un'evoluzione necessaria e tempestiva nell'ambito della professione dell'Internal Audit. Nonostante il diffuso riconoscimento che le carenze culturali sono spesso alla base di significative carenze nei controlli, questo ambito non ha ancora trovato un reale consolidamento nelle pratiche di Internal Audit. Ridefinire l'Audit della "cultura" come Audit del "comportamento organizzativo non allineato agli obiettivi dell'organizzazione" fornisce una base più chiara, strutturata, precisa e verificabile. Come per qualsiasi rischio, le organizzazioni possono gestirlo progettando controlli appropriati e implementandoli in modo efficace.

Nota

I Requisiti Tematici utilizzano la terminologia generale dell'Internal Auditing come definita nei Global Internal Audit Standards. Si consiglia di fare riferimento ai termini e alle definizioni contenuti nel glossario degli Standard.

Il Requisito Tematico sul Comportamento Organizzativo adotta tale filosofia, stabilendo requisiti minimi obbligatori per valutare il comportamento qualora il risk assessment ne determini l'inclusione nell'ambito dell'intervento. Tali requisiti sono pienamente compatibili con l'approccio tradizionale di Audit risk-based e possono essere applicati, con minimi adattamenti, a tutte le

funzioni di Audit. La presente User Guide fornisce esempi pratici di come questo approccio possa essere integrato negli incarichi di Audit standard, nonché indicazioni per la revisione del framework del comportamento organizzativo nel suo complesso o dei suoi singoli elementi. L'influenza significativa che questo argomento esercita sugli obiettivi dell'organizzazione richiede che venga considerato e gestito in modo proattivo.

Le definizioni dei seguenti termini chiave sono necessarie per comprendere e applicare il Requisito Tematico. Data la limitata maturità dell'argomento, le organizzazioni utilizzano tali termini in modo non uniforme. Le definizioni fornite dovrebbero aiutare gli utilizzatori ad allineare la terminologia delle proprie organizzazioni a quella fornita dal Requisito Tematico e dalla presente User Guide.

- **Incentivi comportamentali**: tutto ciò che può essere offerto per motivare un comportamento, inclusi gli incentivi monetari come aumenti, bonus o stock option; o gli incentivi non monetari come complimenti, incarichi graditi o giorni di riposo.
- **Schemi comportamentali**: schemi di comportamento, in cui il comportamento si ripete o si verifica con maggiore frequenza. Tali schemi rappresentano il modo di agire abituale, contrapposto alle situazioni sporadiche.
- **Rischio comportamentale**: il rischio che un comportamento non sia coerente con gli obiettivi dell'organizzazione.
- **Indicatori di rischio comportamentale**: informazioni gestionali utili per l'adozione di misure concrete riguardanti il comportamento.
- **Board**: il massimo organo di governo dell'organizzazione.
- **Condotta**: comportamento in relazione ai requisiti normativi e alle aspettative.
- **Cultura**: le scelte che i dipendenti compiono nello svolgere il proprio lavoro e il modo in cui si relazionano con gli altri, unitamente ai fattori che guidano tali comportamenti organizzativi. Tali fattori includono meccanismi formali, come incentivi e obiettivi, e meccanismi informali, come valori e convinzioni collettive.
- **Comportamento organizzativo**: le scelte osservabili che i dipendenti compiono nello svolgimento del proprio lavoro e il modo in cui si relazionano con gli altri. Tale comportamento influisce sulle performance e sul raggiungimento degli obiettivi dell'organizzazione. In poche parole, il comportamento organizzativo è "il modo in cui si fanno le cose" ed è considerato un sottoinsieme della cultura aziendale.
- **Valutazione delle performance**: valutazioni individuali o di gruppo in merito all'adeguatezza del lavoro svolto.
- **Stakeholder**: ciascuno dei soggetti aventi un interesse diretto o indiretto rispetto ai risultati o alle attività di un'organizzazione. Gli stakeholder possono includere il Board, il management, i dipendenti, i clienti, i fornitori, gli azionisti, gli enti regolatori, le istituzioni finanziarie, gli Auditor esterni, il pubblico e altri.
- **Valori**: principi che orientano il comportamento atteso delle persone.

Sezioni

I requisiti obbligatori contenuti nel Requisito Tematico sul Comportamento Organizzativo e gli aspetti valutabili indicati nella presente User Guide sono suddivisi in tre sezioni:

- **Governance**: chiara definizione di obiettivi e strategie di base per il comportamento organizzativo a supporto degli obiettivi, delle policy e delle procedure dell'organizzazione.
- **Risk Management**: processi per identificare, analizzare, gestire e monitorare i rischi relativi al comportamento organizzativo, inclusa una procedura per l'immediata escalation degli incidenti.
- **Controlli**: processi di controllo istituiti dal management e sottoposti a valutazioni periodiche per mitigare i rischi relativi al comportamento organizzativo.

In aggiunta al Requisito Tematico e alla presente User Guide, gli Internal Auditor possono consultare ulteriori linee guida professionali in materia di comportamento organizzativo, come le Global Guidance dell'IPPF e altre risorse specifiche del settore.

Aspetti da valutare

Gli Internal Auditor possono considerare i seguenti aspetti a supporto della valutazione dei requisiti previsti nel Requisito Tematico sul Comportamento Organizzativo. La lettera associata a ciascun elemento fa riferimento al requisito corrispondente del Requisito Tematico. Gli aspetti da valutare sono esemplificativi e non vincolanti. Gli Internal Auditor dovrebbero affidarsi al giudizio professionale per determinare cosa includere nelle loro valutazioni.

Le restrizioni agli incarichi di Internal Audit nel settore pubblico, dovute al quadro normativo, alla struttura governativa o al contesto politico, sono riconosciute come potenziali ostacoli alla trattazione di alcuni aspetti del presente lavoro. Gli Internal Auditor del settore pubblico dovrebbero documentare tali limitazioni di ambito nel corso del processo di risk assessment, e applicare il giudizio professionale per definire e comunicare in modo chiaro l'ambito adattato della loro review.

Aspetti da valutare sulla governance

Per valutare la possibile applicazione dei processi di governance al comportamento organizzativo, gli Internal Auditor possono esaminare i seguenti aspetti:

A. Ruoli e responsabilità strutturati per garantire che il Board mantenga visibilità e influenza sulle dimensioni comportamentali dell'organizzazione. Le evidenze possono includere:
   - Un comitato di governance che:
     - Istituisce e mantiene un consiglio o uno o più comitati dedicati al comportamento organizzativo, con chiari termini di riferimento che collegano la supervisione del comportamento organizzativo alla realizzazione strategica.
     - Conduce revisioni periodiche degli indicatori di rischio comportamentale, allineati agli obiettivi aziendali di lungo periodo. Gli indicatori di rischio comportamentale sono parametri per stabilire se siano necessarie azioni al fine di garantire che il comportamento resti coerente con gli obiettivi dell'organizzazione , i valori correlati e lo scopo dell'organizzazione.
     - Include obiettivi comportamentali nelle valutazioni delle performance e nella remunerazione dei dirigenti.
   - Framework di reporting al Board che:
     - Forniscono insight sugli indicatori di rischio comportamentale attraverso dashboard strutturate (ad esempio: coinvolgimento del personale, trend degli incidenti, soddisfazione dei clienti, riconoscimenti basati sui valori).
     - Integrano i parametri relativi alla cultura nel reporting delle performance strategiche a livello di Board.
   - Meccanismi di feedback degli stakeholder, come i sondaggi, che consentono:
     - Al Board di ricevere input diretti da dipendenti, clienti e altri stakeholder sull'allineamento dei comportamenti ai valori e alla strategia.
     - Di utilizzare tali feedback per contribuire a definire la direzione strategica e gli interventi comportamentali.

B. La gestione efficace del comportamento organizzativo avviene tramite una chiara definizione delle responsabilità all'interno dell'organizzazione. Il Board ha la responsabilità ultima di garantire che l'organizzazione promuova e sostenga comportamenti allineati ai propri obiettivi organizzativi , tra cui la definizione di chiare aspettative in materia di condotta, la supervisione del reporting sui rischi comportamentali e la messa in discussione della gestione in caso di disallineamento. Le evidenze possono includere:

- Il Board:
  - Approva la propensione al rischio comportamentale e i principali obiettivi culturali dell'organizzazione.
  - Richiede un reporting regolare sugli indicatori di rischio comportamentale (ad esempio trend, pattern di incidenti, tematiche emerse da whistleblowing).
  - Chiama il top management a rispondere della performance culturale tramite meccanismi quali le strutture di incentivazione e il principio del "*tone at the top*".
  - Incontra le funzioni di seconda e terza linea su questioni relative all'escalation dei rischi comportamentali, alle lacune nella supervisione e all'adeguatezza delle azioni correttive.
- Le business unit e il management di linea integrano le aspettative comportamentali nelle attività quotidiane, garantendo che decisioni, comunicazioni e dinamiche di gruppo riflettano i valori dichiarati dell'organizzazione. Ciò può includere l'assunzione di responsabilità per:
  - dare l'esempio dei comportamenti attesi e il mantenimento di un ambiente psicologicamente sicuro.
  - implementare i controlli che influenzano i comportamenti, come l'assunzione, la remunerazione, la comunicazione e le routine di leadership.
  - identificare proattivamente e fare l'escalation dei rischi comportamentali al loro emergere nei contesti operativi.
  - La mitigazione del rischio comportamentale derivante da comportamenti non allineati all'interno dei propri team e dalla necessità di controlli (formali e informali).
- Le funzioni risk management, compliance, risorse umane, nonché le relative funzioni di supervisione, progettano e mantengono il framework del rischio comportamentale dell'organizzazione, includendo:
  - Definizione di ruoli e responsabilità per la supervisione dei comportamenti.
  - Percorsi di escalation e processi di data analytics.
  - Dashboard, analisi tematiche e valutazioni periodiche volte a fornire una visione prospettica delle condizioni comportamentali nell'intera organizzazione.
  - La capacità di mettere in discussione le prassi in cui gli incentivi, le comunicazioni o i comportamenti della leadership divergono dagli obiettivi dichiarati.

- La consultazione su tutte le modifiche sostanziali ai controlli relativi al personale, ai framework di governance o alle iniziative di trasformazione strategica che possono influenzare la cultura organizzativa.
- La revisione delle tendenze emergenti provenienti da report di incidenti, rilievi di Audit o altri meccanismi di assurance che segnalano problematiche di natura comportamentale.

c. Processo di governance che assicura la supervisione dei comportamenti, il monitoraggio regolare, la valutazione e l'allineamento degli schemi comportamentali agli obiettivi dell'organizzazione . Il processo può includere:

- L'uso di dashboard per fornire dati chiave provenienti da fonti quali i risultati dei sondaggi sulla soddisfazione e l'integrità dei dipendenti, i tassi di uscita e assenteismo, i contenuti dei canali di segnalazione, i dati sugli incidenti e le metriche di performance e innovazione. Le caratteristiche di una dashboard efficace sul comportamento organizzativo includono:
  - Valori soglia definiti per individuare opportunità di miglioramento del comportamento.
  - Separazione dei dati comportamentali (ad esempio quelli provenienti dai canali di segnalazione) dai dati sui driver (come la chiarezza di ruoli e responsabilità) e dai dati sugli esiti (come i reclami dei clienti).
  - Integrazione di dati quantitativi, provenienti ad esempio dai sondaggi, con dati qualitativi, come quelli derivanti da focus group e canali di segnalazione.
- La comprensione da parte del Board di come aspetti attuali del comportamento organizzativo possano essere affrontati per migliorare l'efficacia e le performance dell'organizzazione. Questi aspetti comprendono il modo in cui:
  - Le decisioni vengono prese, anche ricorrendo a prospettive diverse e al confronto critico.
  - I dipendenti comunicano tra loro, anche esprimendo preoccupazioni e aspettative.
  - I dipendenti collaborano, anche tra team diversi e nella gestione dei conflitti.
  - I dipendenti reagiscono ai fallimenti, ad esempio imparando dagli errori oppure rispondendo con colpevolizzazione o negazione.
  - Il comportamento del Middle e Top Management impatta sulle altre categorie comportamentali (ad esempio come i leader reagiscono agli errori e come favoriscono il confronto nei processi decisionali).
  - Strategia e modello di business influenzano il processo decisionale, i codici di condotta e la gestione della performance attraverso incentivi e disincentivi.

- La richiesta da parte del Board di un sistema di apprendimento continuo che individui opportunità di miglioramento e le affronti in maniera attiva e misurabile attraverso:
  - L'uso di insight basati su evidenze e sul comportamento reale dei dipendenti.
  - L'attenzione a ciò che effettivamente accade all'interno dell'organizzazione, piuttosto che a ciò che è previsto o desiderato.
  - La valutazione di un insieme di dati qualitativi e quantitativi, spesso acquisiti tramite sondaggi, canali di segnalazione, conversazioni confidenziali e focus group.
  - L'applicazione dei risultati delle analisi per determinare azioni che rafforzino e affrontino specifici aspetti del comportamento organizzativo.
  - L'integrazione di un piano d'azione volto a combinare interventi mirati nelle aree critiche (ad esempio strategia di comunicazione, formazione, sviluppo della leadership e discussioni a livello di team).

D. Le policy e le procedure relative ai protocolli di rischio comportamentale sono stabilite, periodicamente riviste, comunicate in modo efficace e integrate nelle operazioni aziendali e nei processi decisionali. Le policy e le procedure riguardano etica, risorse umane, compliance, risk management, operazioni e diritti decisionali, al fine di garantire che:

- Le aspettative comportamentali siano formalmente articolate nelle policy pertinenti (ad esempio codice di condotta e/o policy su etica, risorse umane, incentivi e delega di autorità). Tali policy dovrebbero definire i comportamenti accettabili e inaccettabili, con esempi pratici, allineati al risk appetite dell'organizzazione.
- Le funzioni di risk management mappino le aspettative comportamentali rispetto ai principali processi operativi, come assunzioni, valutazioni delle performance, onboarding e gestione dei clienti, assicurando che si riflettano nelle decisioni quotidiane. Le assurance review dovrebbero verificare come queste aspettative influenzino i comportamenti effettivi e quindi riferire al Board.
- Il Board richieda e riceva conferma che le policy dell'organizzazione siano accessibili e chiaramente comunicate attraverso molteplici canali (ad esempio intranet, formazione, riunioni plenarie). L'inserimento di casi di studio e alberi decisionali aiuta a contestualizzare le aspettative comportamentali. Le dashboard possono tracciare le metriche di comprensione e di utilizzo.
- Tutte le policy e le procedure comportamentali siano soggette a un ciclo di revisione programmata e aggiornate in risposta a incidenti, risultati di sondaggi o modifiche normative. Le funzioni di seconda linea dovrebbero mantenere un registro delle lessons-learned per identificare eventuali scostamenti tra i comportamenti e gli obiettivi dell'organizzazione .

- Il Board riceva aggiornamenti regolari sulla copertura, la chiarezza e l'efficacia delle policy. La seconda linea dovrebbe analizzare le violazioni, l'impatto delle policy e l'allineamento ai comportamenti desiderati. L'efficacia delle policy dovrebbe essere verificata attraverso feedback qualitativi e indicatori di rischio comportamentale.

Aspetti da valutare nel risk management

Per valutare l'applicazione dei processi di risk management al comportamento organizzativo, gli Internal Auditor possono verificare se:

A. Il processo di gestione del rischio comportamentale è chiaramente definito e include caratteristiche comportamentali critiche per il raggiungimento degli obiettivi dell'organizzazione. Le caratteristiche del risk management potrebbero includere:
   - L'allineamento di ruoli e responsabilità ai framework di rischio e governance dell'impresa, con linee di reporting che consentono indipendenza e capacità di influenza.
   - La facoltà di contestare decisioni e inoltrare problematiche connesse a rischi comportamentali senza timore di ritorsioni o di vederne sminuito l'impatto.
   - L'indipendenza dal management operativo con accesso diretto al Top Management e al Board.
   - L'accesso a dati sul rischio comportamentale provenienti da più fonti, pertinenti, tempestivi e triangolati tra le fonti. Tali dati comprendono forme strutturate (ad esempio risultati di sondaggi, violazioni di policy) e non strutturate (ad esempio segnalazioni, insight da focus group). Le fonti di dati includono risorse umane (come dati su uscite, retention e sondaggi), whistleblowing, reclami dei clienti e rilievi di Audit.
   - L'uso dell'analisi dei dati per identificare tendenze, anomalie e rischi emergenti.
   - L'uso di dashboard e indicatori di rischio per supportare il reporting al management e al Board.
   - L'uso di indicatori di rischio comportamentale connessi agli obiettivi dell'organizzazione.
   - Lo svolgimento "(diretto/direttamente o in outsourcing) di analisi della root cause degli errori comportamentali e dei disallineamenti culturali.
   - La conoscenza dei fattori, formali e informali, che determinano il comportamento (ad esempio incentivi, sicurezza psicologica e tono della leadership).
   - La credibilità e la fiducia che i vertici aziendali godono presso i team operativi, unite alla capacità di influenzare il processo decisionale in tempo reale.
   - La partecipazione attiva alla progettazione e alla revisione dei controlli relativi alle risorse umane (ad esempio incentivi, assunzioni e formazione).

- Un ruolo di advisory nei programmi di cambiamento strategico e nelle iniziative di trasformazione.
- La relazione con la leadership aziendale per plasmare la cultura attraverso l'influenza, non soltanto tramite l'imposizione.
- La raccolta e l'analisi continuativa dei dati, che può includere:
  - Sondaggi sul coinvolgimento e sul benessere dei dipendenti.
  - Dati sul riconoscimento e sulla premialità legata a comportamenti coerenti con i valori aziendali.
  - Segnalazioni dei whistleblower e reclami.
  - Feedback dei clienti, che evidenziano sia la soddisfazione sia l'insoddisfazione.
  - Valutazioni delle performance che riflettono collaborazione, integrità e innovazione.
- L'uso dell'analisi dei dati per identificare vulnerabilità e rilevare tendenze.
- Un processo chiaramente definito per l'immediata escalation dei rischi e dei comportamenti non in linea con gli obiettivi dell'organizzazione.
- La supervisione della definizione e dell'attuazione dei piani d'azione del management per affrontare i rischi e rafforzare i comportamenti richiesti.

B. I processi di monitoraggio tempestivo del comportamento organizzativo includono la comunicazione dei risultati agli stakeholder. Esempi di indicatori di rischio nelle categorie dei comportamenti, dei driver e degli esiti, nonché di carenze segnalabili includono:

- Processo decisionale: mancanza di confronto critico efficace o insufficiente inclusione di prospettive diverse.
- Comunicazione: attenzione inadeguata alle criticità segnalate dai singoli.
- Collaborazione: ambienti di lavoro frammentati in cui i dipendenti si concentrano esclusivamente sul proprio lavoro.
- Risposta alle carenze: attribuzione di colpe e imposizione di sanzioni per errori non intenzionali.
- Driver formali: ruoli e responsabilità poco chiari o obiettivi contrastanti.
- Driver informali: scarsa sicurezza psicologica o dinamiche inefficaci tra le tre linee.
- Dati di performance: numero eccessivo di reclami dei clienti o ristagno nell'innovazione o nella digitalizzazione.
- Dati sulle risorse umane: alti livelli di abbandono e assenteismo e bassi livelli di soddisfazione nei risultati dei sondaggi.
- Dati di rischio e legali: numero elevato di indagini, violazioni delle policy o alert e situazioni evitate per un soffio.

c. Processi volti a garantire che gli scostamenti tra comportamenti attesi e comportamenti osservati siano identificati e comunicati a coloro che hanno l'autorità e la capacità di intervenire. Gli Internal Auditor possono verificare che:

- La comunicazione efficace sia tempestiva, basata su evidenze e supportata da analisi dei driver sottostanti e delle root cause.
- La progettazione e l'efficacia operativa delle attività di comunicazione evitino soluzioni superficiali, danni reputazionali o fallimenti ripetuti.
- Le informazioni siano raccolte e sintetizzate da più fonti, inclusi feedback dei dipendenti, segnalazioni dei whistleblower, risultati delle attività di Audit e analisi degli incidenti.
- Le tecniche di analisi strutturata — come Audit tematici, modelli delle scienze comportamentali e framework di root cause — vadano oltre i sintomi superficiali e identifichino i driver del disallineamento sottostanti (ad esempio incentivi poco chiari, scarsa sicurezza psicologica o *tone at the top* inefficace).
- I gap siano presentati non semplicemente come violazioni di compliance o incidenti isolati, ma come eventi con root cause comportamentali che riflettono problematiche culturali, sistemiche e/o di leadership.
- Le comunicazioni evidenzino cosa è accaduto e perché, basandosi su dati quantitativi e qualitativi a supporto delle conclusioni.
- L'organizzazione distingua tra schemi comportamentali, vulnerabilità derivanti da driver comportamentali e risultati organizzativi (ad esempio impatto sulle performance, fiducia degli stakeholder), consentendo di intervenire sui comportamenti e sui loro driver. I rilievi siano comunicati ai giusti destinatari, con un livello di dettaglio appropriato:
  - Ai responsabili operativi per la correzione immediata dei processi.
  - Alla leadership apicale per l'allocazione delle risorse, i messaggi e il tono.
  - Al Board o ai comitati competenti per la supervisione e le implicazioni strategiche.
- Strumenti visivi e narrativi come dashboard, heat map o sintesi di casi spieghino i risultati e supportino raccomandazioni e/o piani d'azione.
- Le implicazioni per l'esposizione al rischio e la resilienza dell'ambiente di controllo siano incluse nelle revisioni dei processi.
- La comunicazione delle carenze sia collegata alle azioni correttive e monitorata fino al completamento.
- Gli esiti degli interventi siano valutati e condivisi, completando il ciclo di apprendimento.
- Le comunicazioni siano libere da influenze indebite e allineate ai protocolli di escalation stabiliti, preservando l'indipendenza e la credibilità delle valutazioni.

D. Gli scostamenti tra comportamenti attesi e comportamenti effettivi sono risolti in modo strutturato e partecipativo, al fine di garantire che le azioni correttive siano fondate sul contributo degli stakeholder, monitorate fino al completamento e valutate in termini di efficacia. Gli Internal Auditor possono verificare se:

- Il processo di risoluzione coinvolge in modo significativo gli stakeholder più vicini alla problematica, come i responsabili operativi, le risorse umane, i business partner, i rappresentanti dei dipendenti, i consulenti di compliance e gli individui o i team interessati. Il loro contributo assicura che le azioni siano:
  - Calate nel contesto specifico: sensibili alle realtà operative e alle norme informali che possono aver contribuito allo scostamento.
  - Credibili e accettate: è più probabile che le azioni vengano sostenute e integrate se sono modellate dai soggetti direttamente coinvolti nelle azioni stesse.
  - Critiche in ottica costruttiva: in grado di favorire una riflessione trasparente sui comportamenti della leadership che hanno contribuito al problema, sulle debolezze di progettazione dei controlli o sulle dinamiche di gruppo.
- Il contributo degli stakeholder è richiesto, sintetizzato e integrato nei piani d'azione. I meccanismi di feedback possono includere interviste, focus group, indagini diagnostiche e altri metodi.
- Le azioni di risoluzione sono documentate, con attribuzione di responsabilità, tempistiche e criteri di successo definiti:
  - Le azioni sono proporzionate alla gravità della problematica.
  - Ove necessario, le azioni riguardano i driver formali (ad esempio policy e incentivi) e i driver informali (ad esempio sicurezza psicologica e dinamiche di gruppo).
  - Quando sono coinvolte più funzioni (ad esempio risorse umane per la formazione, risk management per i controlli), l'esecuzione interfunzionale e le relative responsabilità sono coordinate e chiarite.
- I progressi sono monitorati fino al completamento, garantendo che gli impegni siano rispettati e mantenuti. Ciò include:
  - Il mantenimento di un registro delle problematiche comportamentali e delle relative azioni o di un meccanismo equivalente.
  - Lo svolgimento di controlli periodici con i responsabili delle azioni per verificarne lo stato di avanzamento.
  - L'escalation agli organi di governance competenti in caso di eventuali ritardi, completamenti solo parziali o forme di resistenza.
- L'efficacia delle azioni di risoluzione nel colmare il gap e ridurre il rischio comportamentale viene valutata. Ciò può comportare:
  - La rivalutazione degli indicatori di rischio comportamentale dopo l'implementazione.

- La raccolta di feedback dagli stakeholder coinvolti sui cambiamenti osservati.
- La verifica di cambiamenti nei comportamenti tramite osservazione, sondaggi o tecniche di Audit.
- L'aggiustamento delle azioni o l'introduzione di misure di rinforzo quando i risultati rimangono deboli o ambigui.

Aspetti da valutare nei processi di controllo

Per valutare come i processi di controllo siano applicati per mitigare il rischio di comportamenti organizzativi non allineati agli obiettivi dell'organizzazione, gli Internal Auditor possono esaminare:

A. Le revisioni del rischio comportamentale per comprendere il rischio generato dall'attuale comportamento organizzativo (ossia le potenziali conseguenze indesiderate di come le attività vengono svolte). Esempi di tali revisioni sono le valutazioni dei progetti una volta completati, le analisi delle root cause e le revisioni delle operazioni dettagliate nella pratica.

B. I processi strutturati di feedback per comprendere quali meccanismi il management utilizza per comunicare le aspettative comportamentali (ad esempio *riunioni plenarie*, email e incontri tra singoli dipendenti e supervisori) e l'efficacia del *tone at the top* sul comportamento all'interno dell'organizzazione. A tal fine possono essere valutati i processi che colgono e analizzano le percezioni e la comprensione dei messaggi del Board e del Top Management da parte dei dipendenti. Gli Internal Auditor possono aiutare le organizzazioni a perfezionare continuamente le loro strategie di comunicazione e a garantire che il the tone from the top sia recepito efficacemente a tutti i livelli, esaminando controlli chiave quali:

   - Sondaggi, interviste e focus group periodici con i dipendenti, per verificare la chiarezza, la coerenza e l'impatto delle comunicazioni della leadership e per ottenere dati quantitativi e qualitativi sul livello di ricezione e comprensione dei messaggi ai vari livelli dell'organizzazione.
   - Canali aperti per feedback anonimi, che consentono ai dipendenti di condividere opinioni sincere senza timore di ritorsioni. Questi canali dovrebbero essere supportati da piattaforme digitali che consentano feedback e suggerimenti in tempo reale. I dati ricavati da questi canali dovrebbero essere analizzati per verificare se il *tone at the top* sia ben compreso dai dipendenti a tutti i livelli.
   - Feedback provenienti dalle riunioni del Top Management, raccolti tramite sondaggi, interviste, focus group, verbali e canali anonimi, per garantire che il Top Management sia consapevole di comunicazioni inefficaci, incomprensioni o aree che necessitano miglioramenti. Il Top Management dimostra che i contributi dei dipendenti sono apprezzati rispondendo attivamente ai feedback e agendo di conseguenza. Se ciò non avviene, i dipendenti possono diventare meno inclini a fornire feedback, percependo che le cose non cambieranno.

- Integrazione dei feedback sulla performance del Top Management nelle loro performance review, per monitorare in modo continuativo il recepimento delle direttive della leadership. Ciò rafforza l'importanza dei messaggi della leadership e garantisce che si riflettano nelle operazioni quotidiane.

c. L'escalation all'interno dell'organizzazione viene incoraggiata per favorire l'identificazione e mitigazione tempestiva dei rischi , nonché per creare un ambiente psicologicamente sicuro, in cui i dipendenti si sentano liberi di segnalare problematiche senza timore di ritorsioni. Gli Internal Auditor possono esaminare controlli chiave per rafforzare un efficace risk management, quali:

   - Meccanismi di feedback di facile utilizzo, tra cui segnalazioni dirette e possibilità di anonimato , hotline interne ed esterne per frodi o whistleblowing, sondaggi, cassette per suggerimenti e piattaforme digitali per consentire segnalazioni confidenziali e cogliere problematiche che gli individui potrebbero esitare a segnalare apertamente.
   - Processi ben definiti e di facile comprensione per la segnalazione delle problematiche con molteplici canali diretti e anonimi, interni ed esterni, e iniziative volte a sensibilizzare i dipendenti. Le caratteristiche dei canali di segnalazione dovrebbero includere:
     - Garanzie di riservatezza, per proteggere l'identità di chi segnala le problematiche.
     - Policy rigorose di non ritorsione, comunicate chiaramente e sostenute in modo coerente, per tutelare chi segnala le problematiche.
     - Comunicazione di riscontro a coloro che segnalano in forma non anonima, indipendentemente dal motivo o dall'esito.
     - Sintesi periodiche a livello organizzativo delle problematiche segnalate e dei relativi esiti, per dimostrare che le criticità vengono comunicate e affrontate e per garantire trasparenza sulle azioni intraprese in risposta ai feedback.
   - Comunicazioni regolari da parte del management che sottolineano l'importanza della comunicazione aperta e della segnalazione delle problematiche, e che dimostrano come lo stesso management dia l'esempio di tali comportamenti.
   - Sessioni di formazione periodiche che sottolineano l'importanza della sicurezza psicologica, incoraggiano le persone a segnalare i problemi e forniscono indicazioni su come gestire correttamente l'escalation delle segnalazioni. La formazione dovrebbe essere ripetuta a intervalli regolari per rafforzare nel tempo i comportamenti desiderati.
   - Riconoscimenti informali, come apprezzamenti verbali o scritti, e riconoscimenti pubblici per le persone che segnalano le problematiche.
   - Revisioni periodiche del processo di escalation per garantirne l'efficacia e l'efficienza, anche sollecitando feedback dai dipendenti per identificare e affrontare tempestivamente gli ostacoli alla segnalazione.
   - Comunicazioni relative alla risoluzione dei feedback.

D. I programmi di incentivazione e disincentivazione sono allineati ai comportamenti desiderati e agli obiettivi dell'organizzazione e vengono comunicati. Gli Internal Auditor possono esaminare controlli quali:

- Gli incentivi, sia monetari (ad esempio bonus e promozioni) sia non monetari (ad esempio riconoscimenti e opportunità di sviluppo) sono allineati agli obiettivi dell'organizzazione e collegati alla dimostrazione dei comportamenti desiderati.
- Criteri equilibrati di performance review integrano il modo in cui gli obiettivi sono raggiunti (ad esempio collaborazione, integrità, orientamento al cliente), oltre agli indicatori di risultato più tradizionali (ad esempio, obiettivi finanziari).
- I criteri di incentivazione e le soglie di disincentivazione sono chiaramente definiti, applicati in modo coerente e soggetti a revisione da parte del management o delle risorse umane, per evitare bias e risultati non intenzionali.
- Gruppi interfunzionali convalidano la coerenza e l'equità delle decisioni in merito agli incentivi tra le diverse business unit.
- Le conseguenze per comportamenti scorretti e violazioni culturali includono disincentivi chiari e proporzionati (ad esempio riduzioni dei bonus o blocchi delle promozioni), con azioni spiegate e documentate per garantire trasparenza.
- I programmi di riconoscimento non economico valorizzano i dipendenti che incarnano i valori culturali, ad esempio tramite decisioni etiche e promozione della sicurezza psicologica.
- L'impatto dei programmi di incentivazione è valutato regolarmente tramite feedback dei dipendenti e metriche comportamentali al fine di perfezionare o riequilibrare i meccanismi di ricompensa. I programmi di incentivazione dovrebbero essere valutati e adattati per garantire che:
  - Gli obiettivi non siano troppo stringenti né troppo generici.
  - Gli obiettivi siano raggiungibili.
  - Gli obiettivi a breve termine non compromettano i risultati di lungo periodo.
  - I livelli accettabili di assunzione di rischio siano esplicitati.
  - Siano implementate misure di salvaguardia per garantire comportamenti etici nel raggiungimento degli obiettivi (ad esempio, leader come modelli di comportamento etico, rendere il costo dell'illecito molto superiore al beneficio e una rigorosa supervisione).
  - Gli obiettivi siano adattati alle capacità e alle circostanze individuali, pur mantenendo l'equità.
  - Gli obiettivi di squadra non siano in contrasto con quelli individuali.
  - La motivazione intrinseca sia valutata e il management riconosca che alcuni obiettivi possono limitarla.

- Gli obiettivi finali dell'organizzazione siano considerati e sia valutata l'adeguatezza del tipo di obiettivo (ad esempio di performance o di apprendimento).

- L'organizzazione integra rinforzi positivi e azioni correttive per coltivare un comportamento organizzativo proattivo allineato ai propri obiettivi e ai requisiti normativi. I controlli chiave dovrebbero includere:
  - Valutazioni periodiche dell'efficacia dei programmi di comunicazione e formazione, per garantire che i dipendenti comprendano l'importanza della segnalazione delle problematiche e delle conseguenze della non conformità e si sentano incoraggiati a segnalare.
  - Sistemi di monitoraggio e reporting che tracciano la compliance e identificano i potenziali problemi di mancato reporting.
  - Le azioni disciplinari sono applicate in modo coerente ed equo e non sono né così severe da scoraggiare le segnalazioni né così indulgenti da non scoraggiare i comportamenti non etici.
  - I meccanismi di feedback che consentono ai dipendenti di segnalare problematiche in forma anonima vengono regolarmente rivisti per garantirne l'efficacia e incoraggiare segnalazioni sincere.

E. Il processo di gestione delle problematiche identifica i comportamenti non allineati agli obiettivi dell'organizzazione e li segnala ai livelli superiori quando necessario per creare un piano di azione gestionale volto a mitigare il rischio di risultati negativi. Gli Internal Auditor possono esaminare controlli chiave per interventi efficaci di cambiamento comportamentale, quali:

- Approcci basati su evidenze: Il piano d'azione integra approcci basati sull'evidenza scientifica per la modifica del comportamento, che affondano le proprie radici nelle scienze comportamentali, nei modelli comportamentali e nel change management.. Se l'approccio non è esplicitamente basato su uno specifico modello di cambiamento comportamentale, dovrebbe combinare strategie di intervento relative a:
  - Comunicazione: dipendenti e management siano costantemente sensibilizzati sulla necessità di un cambiamento comportamentale e si favorisca l'adozione e il supporto della trasformazione.
  - Formazione e sviluppo dei dipendenti: si investa in programmi di formazione adeguati ai diversi ruoli e si dotino i dipendenti delle competenze e dei comportamenti necessari tramite workshop, e-learning e opportunità di sviluppo continuo. Ciò include l'apprendimento e la capacità di implementare efficacemente nuove competenze e comportamenti necessari per realizzare i cambiamenti desiderati dall'organizzazione.
  - Sviluppo manageriale: i manager a tutti i livelli valutino come facilitare e dimostrare i cambiamenti comportamentali nelle situazioni quotidiane. Ciò può includere l'adeguamento del proprio comportamento al fine di aiutare il

personale a sentirsi maggiormente a proprio agio nell'adottare i nuovi comportamenti, la richiesta diretta ai dipendenti di adottarli, l'incoraggiamento dell'apprendimento e la richiesta di formazione sulle competenze e sui comportamenti non ancora acquisiti. Programmi di leadership e coaching possono affinare competenze e fiducia.

- Rinforzi costanti nelle situazioni quotidiane: le persone hanno bisogno di sostegno, incoraggiamento e promemoria regolari per sviluppare nuovi comportamenti e integrarli nella propria routine di lavoro quotidiana.
- Rinforzo congruente: un piano di intervento dovrebbe essere allineato ai messaggi della leadership, ai processi, ai sistemi, al coaching e ai meccanismi di feedback informali per rafforzare il cambiamento desiderato. Tale allineamento elimina l'incertezza e la confusione, garantendo che i dipendenti comprendano i cambiamenti comportamentali desiderati, le modalità di adozione e la loro importanza.
- Intervento sui driver dei comportamenti: un cambiamento comportamentale sostenibile richiede che si affrontino i driver sottostanti (cfr. Risk Management, C) dei comportamenti, e non solo i comportamenti stessi.
- Misurazione: la misurazione dei progressi e dell'efficacia degli interventi consente di determinare se stanno producendo l'impatto desiderato e se sono necessari aggiustamenti. Aggiornamenti regolari fungono da rinforzo positivo e forniscono agli stakeholder informazioni sui progressi compiuti. Un approccio di misurazione efficace combina metodi qualitativi e quantitativi, come sondaggi e interviste, e fornisce una comprensione completa dei progressi.

F. I programmi di formazione destinati a influenzare i comportamenti sono esplicitamente collegati ad aspettative comportamentali definite o a dichiarazioni di risk appetite. Esempi di argomenti di formazione sono l'etica, la compliance, la leadership, l'inclusione, la consapevolezza del rischio e il processo decisionale. Gli Internal Auditor possono verificare che i programmi di formazione siano:

- Rappresentativi della condotta e degli atteggiamenti desiderati e includano obiettivi di apprendimento chiari e documentati.
- Basati su evidenze comportamentali o sull'apprendimento dagli incidenti (ad esempio rilievi di Audit, analisi delle root cause e meccanismi di feedback).
- Erogati a tutti i gruppi di ruoli rilevanti, con moduli specifici per Top Management, manager di linea e personale.
- Obbligatori ove pertinente (ad esempio processi ad alto rischio, responsabilità regolamentate e ruoli di controllo).
- Aggiornati regolarmente, con una revisione dei contenuti almeno annuale per garantirne la rilevanza e l'efficacia.
- Progettati in modo tale da:

- Integrare scenari o case study reali per rendere concrete le aspettative comportamentali.
- Utilizzare tecniche che coinvolgono i partecipanti (ad esempio storytelling e domande che stimolano la riflessione).
- Coinvolgere attivamente il Top Management per indicare il *tone at the top* e incoraggiare i dipendenti ad adottare cambiamenti comportamentali.

- Comprensivi di controlli di impatto e di assurance che:
  - Tracciano il completamento della formazione obbligatoria e riportano le eccezioni.
  - Misurano l'impatto sui comportamenti e la ritenzione dell'apprendimento attraverso sondaggi informali, test semplici o valutazioni basate sull'osservazione.
  - Rilevano le percezioni dei partecipanti e acquisiscono informazioni sull'efficacia della formazione tramite processi strutturati di feedback.
  - Assicurano che i contenuti formativi siano allineati ai framework di rischio e ai requisiti di controllo e includano processi formali di revisione e approvazione.

G. I processi di assunzione sono allineati alle aspettative comportamentali dell'organizzazione e integrano competenze comportamentali. Gli Internal Auditor possono esaminare caratteristiche di controllo quali:

- Strumenti che consentono di valutare l'allineamento dei candidati ai valori dell'organizzazione, tra cui guide strutturate per i colloqui e domande basate su scenari.
- Colloqui comportamentali e feedback dei pari sono utilizzati per valutare tratti quali empatia, giudizio etico e senso di responsabilità.
- Gli annunci di recruitment ed employer branding riflettono le aspirazioni culturali dell'organizzazione per attrarre candidati culturalmente allineati.
- I meccanismi di feedback consentono di valutare l'integrazione culturale dei neoassunti, così da affrontare tempestivamente eventuali disallineamenti.
- La documentazione (ad esempio griglie di valutazione e verbali dei colloqui) dimostra l'applicazione coerente dei criteri decisionali di assunzione.
- Le risorse umane e il Top Management esaminano i modelli di assunzione per individuare eventuali rischi, quali favoritismi, bias o mancato rispetto degli standard comportamentali.
- Le politiche di assunzione e promozione vengono regolarmente riviste per verificarne la coerenza con i valori dell'organizzazione e l'efficacia nella pratica.

Appendice A. Esempi di applicazione pratica

Gli esempi che seguono illustrano scenari in cui il Requisito Tematico sul Comportamento Organizzativo potrebbe essere applicato.

Esempio 1: Revisione autonoma del framework comportamentale di un'organizzazione

La funzione di Internal Audit ha avviato una revisione autonoma del framework complessivo dell'organizzazione per valutarne la struttura e l'efficacia operativa nella gestione del rischio comportamentale. L'ambito di questo incarico ha riguardato le strutture di governance, le attività di risk management e i controlli comportamentali che supportano l'allineamento all'interno dell'organizzazione.

Gli Internal Auditor hanno valutato se le responsabilità relative alla supervisione dei comportamenti fossero chiaramente definite e prive di conflitti di interesse. Il team ha esaminato i termini di riferimento del Board e ha verificato che il Board avesse ricevuto regolarmente reporting sugli indicatori di rischio comportamentale, quali i risultati dei sondaggi e le tendenze nelle segnalazioni. È stato inoltre verificato se le policy legate alla cultura, come quelle sul whistleblowing e sulla condotta etica, venissero regolarmente aggiornate e applicate.

Gli Internal Auditor hanno inoltre valutato gli elementi di risk management, a partire dal framework di gestione del rischio comportamentale gestito dalla seconda linea, concentrandosi sulla sua capacità di identificare i principali fattori di rischio comportamentale (quali scarsa sicurezza psicologica o obiettivi di performance non allineati). La valutazione si è focalizzata sulle modalità con cui l'organizzazione ha monitorato e affrontato le discrepanze tra comportamenti attesi e comportamenti osservati, verificando se le anomalie comportamentali fossero oggetto di escalation e gestite in modo sistematico.

È stato esaminato l'ambiente di controllo per determinare se i processi formali supportassero le aspettative comportamentali. Gli Auditor hanno verificato se i protocolli di assunzione fossero in grado di valutare l'allineamento ai valori, se i contenuti del processo di onboarding fossero coerenti con le norme della cultura organizzativa e in quale misura gli incentivi (monetari e non) venissero riesaminati per identificare possibili conseguenze non intenzionali. Sono stati inoltre testati i programmi di formazione, i canali di segnalazione, i messaggi della leadership e le analisi dei dati utilizzate per rilevare problematiche comportamentali.

Questo incarico ha fornito una visione completa di come il rischio comportamentale sia gestito a livello organizzativo e ha costituito la base per raccomandare miglioramenti all'infrastruttura comportamentale dell'organizzazione.

Esempio 2: Audit tematico delle pratiche di incentivazione

Questo incarico di Audit ha valutato principalmente come i framework di incentivazione dell'organizzazione influenzino i comportamenti e se tali framework siano in linea con lo scopo, i valori e le aspettative normative dell'organizzazione. La funzione di Internal Audit ha scelto questo tema a causa di crescenti preoccupazioni legate al rischio di comportamenti scorretti e di evidenze emergenti di comportamenti influenzati da pressioni nelle business unit.

La revisione è iniziata valutando gli assetti di governance per la progettazione e l'approvazione delle strutture di incentivazione. La funzione di Audit ha valutato se i soggetti responsabili dell'attuazione delle decisioni di governance, come le risorse umane o i comitati per la remunerazione, avessero una supervisione formale sulla progettazione degli incentivi e se il loro operato fosse oggetto di revisione indipendente da parte delle funzioni risk management, compliance o Audit.

È stata adottata una prospettiva di risk management per comprendere se lo sviluppo delle strutture di incentivazione includesse una considerazione delle loro implicazioni comportamentali. Gli Auditor hanno verificato se l'organizzazione avesse testato scenari o analizzato i rischi comportamentali in relazione alle proprie strutture di ricompensa. Hanno inoltre verificato se i key performance indicator comportamentali, come i punteggi di collaborazione, fossero monitorati e utilizzati per valutare i risultati.

Il testing dei controlli ha riguardato una serie di meccanismi progettati per orientare i comportamenti legati alle ricompense. Tra questi figuravano le balanced scorecard, che incorporano criteri di performance volti a misurare i risultati e le modalità con cui sono stati conseguiti, l'applicazione di clausole di malus (penalità o riduzione della retribuzione) e/o di clawback, nonché l'esistenza di processi di feedback a 360 gradi. Gli Auditor hanno inoltre esaminato la formazione fornita ai manager di linea riguardo alla comunicazione di feedback comportamentali ed esplorato i programmi di riconoscimento non monetario che premiano condotte coerenti con i valori.

Nel corso dell'incarico, gli Internal Auditor hanno tentato di capire se le pratiche di incentivazione potessero involontariamente indurre comportamenti indesiderati, come l'assunzione di rischi eccessivi, l'adozione di scorciatoie o la riluttanza a effettuare l'escalation delle problematiche. Sono state formulate raccomandazioni per migliorare la trasparenza, integrare in modo più coerente obiettivi basati sui valori e rafforzare le revisioni indipendenti da parte della seconda linea durante il processo di progettazione dei sistemi di ricompensa.

Esempio 3: Integrazione in un Audit tradizionale: gestione del rischio informatico

In questo esempio, la funzione di Internal Audit ha integrato considerazioni sul rischio comportamentale in un incarico tradizionale volto a valutare la gestione del rischio informatico. Riconoscendo che molti incidenti di sicurezza in ambito informatico derivano non solo da problemi tecnici, ma anche da comportamenti umani, gli Auditor hanno inserito verifiche sui comportamenti in tutte le fasi dell'incarico.

L'incarico è iniziato valutando in che misura il rischio comportamentale fosse riconosciuto all'interno della governance della cyber resilience. Gli Auditor hanno esaminato la supervisione esercitata da parte del Board e del Top Management sulla strategia di cybersecurity, cercando

evidenze che tali organi monitorassero e discutessero l'allineamento dei comportamenti agli obiettivi dell'organizzazione, come ad esempio il rispetto delle pratiche di sicurezza o l'esempio dato dalla leadership in materia di comportamenti sicuri.

In termini di risk management, il team ha considerato se le valutazioni del rischio informatico dell'organizzazione tenessero conto dei fattori umani. In particolare, è stato verificato se i dati comportamentali (ad esempio la frequenza di fallimenti nei test di phishing, violazioni di accesso ai sistemi o bassi tassi di completamento della formazione) fossero utilizzati per monitorare il rischio e segnalarlo ai livelli superiori. L'incarico ha inoltre indagato se fosse stata individuata la root cause dei precedenti incidenti di sicurezza per identificare potenziali driver comportamentali, come responsabilità poco chiare o un atteggiamento inadeguatodel management.

Il testing dei controlli si è concentrato sulla progettazione comportamentale e sulla sicurezza operativa. Gli Auditor hanno verificato se nei processi di assunzione per ruoli con accesso privilegiato fosse incluso lo screening comportamentale. Le strutture di incentivazione sono state valutate per verificare se incoraggiassero pratiche online sicure o se involontariamente favorissero comportamenti rischiosi a scapito della sicurezza. Anche la formazione in materia di cybersecurity è stata valutata per stabilire se fosse coinvolgente, aggiornata regolarmente e comprendesse simulazioni volte a testare le risposte comportamentali a phishing e social engineering.

Infine, l'incarico ha esaminato come il management ha rafforzato i comportamenti sicuri attraverso la comunicazione e se i dipendenti si sono sentiti tranquilli nel segnalare comportamenti informatici non sicuri. Una cultura organizzativa che incoraggia i dipendenti a segnalare i problemi è stata considerata un fattore abilitante fondamentale per la resilienza.

L'inclusione degli aspetti comportamentali all'interno di questo Audit informatico ha portato a insight più approfonditi e a raccomandazioni utili, rafforzando la capacità dell'organizzazione di gestire il rischio in uno dei suoi ambiti più critici.

Appendice B. Casi di studio di Audit specifici

Case Study 1: Dipartimento dell'edilizia abitativa (settore pubblico)

Gli esempi contenuti in questo case study illustrano come la funzione di Internal Audit di un'agenzia governativa potrebbe applicare il Requisito Tematico sul Comportamento Organizzativo al fine di valutare come l'agenzia adempia al proprio obiettivo di fornire servizi abitativi equi alla collettività. Gli Internal Auditor dovrebbero riconoscere che le priorità dei funzionari pubblici, le sensibilità politiche, gli stanziamenti di bilancio e alcune scelte politiche esulano dal loro ambito. Tuttavia, rientra pienamente nel loro ambito di valutazione il modo in cui gli alti funzionari e i dirigenti interpretano e applicano tali politiche, nonché la cultura interna del dipartimento.

Governance

A. Ruoli e responsabilità: il dipartimento dispone di una chiara struttura organizzativa, con separazione delle responsabilità tra la definizione delle policy (alti funzionari) e l'erogazione dei servizi abitativi. Parte dell'obiettivo dell'incarico per la funzione di Internal Audit è determinare se siano evitati i conflitti di interesse strutturali: ad esempio, la responsabilità dellla conformità alle policy è distinta dalla supervisione degli appaltatori?
B. Accountability: al vertice dell'organizzazione e al Top Management sono attribuite responsabilità per gli obiettivi organizzativi legati a risultati culturali, quali l'equità nell'assegnazione degli alloggi e il benessere del personale. La funzione di Internal Audit valuta se l'accountability è visibile e accettata.
C. Supervisione e monitoraggio: un "comitato per la cultura organizzativa" presieduto da un top manager esamina trimestralmente i sondaggi del personale, i dati sul whistleblowing e i reclami degli stakeholder. Gli Auditor valutano se tali processi consentano di rilevare tempestivamente comportamenti non conformi.
D. Policy e procedure: esistono codici di condotta debitamente autorizzati, linee guida per l'assegnazione degli alloggi e registri dei conflitti di interesse che vengono revisionati periodicamente (ad esempio con cadenza almeno semestrale). La funzione di Internal Audit valuta se gli aggiornamenti riflettono gli insegnamenti tratti da scandali nel settore dell'edilizia abitativa e dai report di Audit resi pubblici.

Risk Management

A. Framework del rischio comportamentale: il dipartimento identifica i rischi culturali che possono incidere sull'erogazione dei programmi di servizio pubblico, come favoritismi nell'assegnazione degli alloggi, eccessiva burocrazia o la ritrosia dei dipendenti a contestare le direttive dei funzionari pubblici. La funzione di Internal Audit assicura che tali rischi siano formalmente registrati nel risk register, presi in considerazione dal management e affrontati quando necessario.

B. Indicatori e analisi dei dati: le dashboard monitorano dati comportamentali quali turnover del personale, lamentele, numero di reclami informali da parte degli inquilini e dei cittadini, nonché tempi di risposta a richieste di accesso agli atti pubblici Gli Auditor valutano se gli indicatori e le analisi sono affidabili e discussi all'interno dell'ente.

C. Gestione degli scostamenti: quando emergono scostamenti (ad esempio casi di whistleblowing che mostrano deviazioni dai principi di equità), questi vengono segnalati alla dirigenza. Gli Auditor verificano se l'analisi degli scostamenti conduce ad azioni correttive.

D. Contributo degli stakeholder alla risoluzione delle criticità: autorità competenti, associazioni per l'edilizia residenziale pubblica, sindacati e panel di cittadini vengono consultati in caso di individuazione di problemi culturali (come scortesia del personale di front line o bias nelle assegnazioni). Gli Auditor verificano che i piani di risoluzione tengano in considerazione i feedback provenienti dalla consultazione. .

Controlli

A. Revisioni del rischio comportamentale: vengono condotte analisi retrospettive in seguito a insuccesi nei progetti abitativi (ad esempio ritardi nella costruzione di alloggi sociali). Gli Auditor verificano se sono state valutate le root cause di natura comportamentale (come scarsa collaborazione o cultura della colpa).

B. Impostazione della linea di condotta: i dirigenti comunicano le aspettative in materia di equità, imparzialità e qualità del servizio attraverso riunioni plenarie con il personale e video pubblicati sulla intranet. Gli Internal Auditor verificano se tali aspettative sono recepite e messe in pratica.

C. Meccanismi di escalation: il dipartimento mantiene un canale di whistleblowing accessibile al pubblico e un processo di gestione dei reclami per inquilini, personale e cittadini. Gli Auditor esaminano la tempestività, la riservatezza e l'assenza di ritorsioni nei confronti di chi effettua le segnalazioni..

D. Incentivi: le valutazioni delle performance sottolineano la collaborazione del personale, il coinvolgimento degli stakeholder e l'equità nelle interazioni con gli inquilini. Gli Auditor valutano se promozioni e riconoscimenti rafforzano tali comportamenti.

E. Monitoraggio dei comportamenti: i manager di linea valutano il personale in base agli standard comportamentali (integrità, empatia verso gli inquilini vulnerabili) durante le revisioni annuali. Gli Auditor verificano se i risultati sono coerenti e se gli schemi comportamentali inadeguati vengono affrontati.

F. Formazione: i programmi obbligatori riguardano i pregiudizi inconsci, la risoluzione dei conflitti e il processo decisionale etico nell'assegnazione degli alloggi. Gli Auditor verificano se i tassi di completamento sono elevati e valutano i risultati dei sondaggi post-formazione.

G. Processi di remediation: quando vengono individuate violazioni culturali (come la manipolazione delle liste di attesa per gli alloggi), vengono condotte analisi delle root cause e monitorati i piani d'azione. Gli Auditor verificano se le misure correttive sono efficaci e durature.

Insight chiave

Sebbene l'indirizzo impartito dai funzionari pubblici e la definizione delle politiche di alto livello esulino dall'ambito e dal controllo della funzione di Internal Audit, le strutture di governance, risk management e controllo del dipartimento relative ai comportamenti possono essere oggetto di Audit. L'applicazione di tutti i 15 requisiti previsti dal Requisito Tematico sul Comportamento Organizzativo garantisce che gli Internal Auditor possano valutare se il comportamento organizzativo influisca sule modalità di erogazione dei servizi abitativi, se ad esempio sono eque, trasparenti e coerenti con i valori, nonostante il contesto politico.

Case Study 2: Piccola impresa di costruzioni (Funzione di Internal Audit di piccole dimensioni)

La funzione di Internal Audit di una ipotetica impresa di costruzioni con 50 dipendenti teme che il Requisito Tematico sul Comportamento Organizzativo sia pensato per organizzazioni grandi e complesse. Tuttavia si applicano i medesimi principi, adattandoli alla scala dell'azienda. Anche in assenza di un sottocomitato del Board o di dashboard sofisticate, la società può comunque dimostrare l'allineamento a tutti i 15 requisiti previsti dal Requisito Tematico.

Governance

A. Ruoli e responsabilità: il responsabile aziendale delega formalmente la responsabilità delle risorse umane al responsabile dell'ufficio e la supervisione dei progetti ai responsabili di cantiere. Gli Internal Auditor valutano se i ruoli sono chiari e se sono evitati i conflitti (ad esempio se le medesime figure approvano e monitorano le spese degli appaltatori).

B. Accountability: ogni manager sottoscrive trimestralmente dichiarazioni con cui attesta la propria responsabilità per il comportamento del team, nonché per l'osservanza delle norme di sicurezza e il trattamento dei subappaltatori. Gli Auditor valutano se tali dichiarazioni sono ragionevoli e monitorate.

C. Supervisione e monitoraggio: il management si riunisce mensilmente per esaminare il turnover del personale, i reclami dei clienti e i report sulla sicurezza dei progetti. Gli Auditor verificano se le criticità legate alla cultura organizzativa vengono sollevate e monitorate.

D. Policy e procedure: gli Auditor verificano che i codici di condotta scritti, i protocolli di sicurezza e le linee guida contro il bullismo siano revisionati annualmente e comunicati al personale.

Risk Management

A. Framework del rischio comportamentale: l'azienda identifica rischi quali fretta o mancata osservanza di tutte le procedure di sicurezza richieste per rispettare le scadenze, favoritismi nell'assegnazione degli straordinari e molestie nei cantieri. Gli Auditor verificano che tali rischi siano inclusi nel registro dei rischi.

B. Indicatori e analisi dei dati: l'azienda non utilizza dashboard ma semplici fogli di calcolo per monitorare assenze, reclami e incidenti di sicurezza. Gli Auditor valutano se tali strumenti evidenziano aree che necessitano di revisione.

C. Gestione degli scostamenti: se i sondaggi tra il personale rilevano un divario tra il "rispetto atteso" e il "rispetto effettivamente percepito", i manager devono presentare azioni correttive alla riunione successiva. Gli Auditor determinano se le azioni sono state implementate e chiuse.

D. Contributo degli stakeholder alla risoluzione dei problemi: le autorità competenti, i rappresentanti dei dipendenti e talvolta i clienti chiave vengono invitati a fornire osservazioni quando emergono problemi culturali. Gli Auditor determinano se la risposta tiene conto del feedback ricevuto.

Controlli

A. Revisioni del rischio comportamentale: dopo ogni insuccesso progettuale (ad esempio superamento dei costi dovuto a scarsa collaborazione), il responsabile aziendale conduce una sessione di "*lessons learned*". Gli Auditor verificano se le cause culturali (colpe, scarsa comunicazione) vengono registrate e se vengono implementati controlli per correggere le azioni future.

B. Impostazione del tono: il responsabile aziendale organizza briefing trimestrali con il personale per rafforzare i valori di equità, qualità e rispetto. Gli Internal Auditor raccolgono feedback dal personale per verificare se il messaggio viene recepito correttamente.

C. Meccanismi di escalation: in assenza di una hotline formale, i canali di segnalazione sono costituiti da una cassetta dei suggerimenti chiusa a chiave e dall'accesso diretto al responsabile aziendale. Gli Auditor verificano se il personale li utilizza e se esistono policy contro le ritorsioni.

D. Incentivi: i bonus sono modesti ma legati al lavoro di squadra e al feedback dei clienti e non solo al rispetto delle scadenze di progetto. Gli Auditor verificano se l'assegnazione dei premi è coerente e ragionevole.

E. Monitoraggio dei comportamenti: i supervisori forniscono feedback informali sul comportamento del personale durante le valutazioni delle performance. Gli Auditor valutano se il feedback viene applicato in modo coerente nei vari team.

F. Formazione: ogni anno vengono organizzati brevi workshop sul rispetto al lavoro e sulla sicurezza in cantiere. Gli Auditor verificano la partecipazione e l'efficacia attraverso interviste a campione.

G. Processi di remediation: se si verificano episodi di bullismo o cattiva condotta, il responsabile aziendale (o un'autorità superiore se necessario) conduce un'indagine, documenta il caso e applica le misure conseguenti. Gli Auditor verificano se le sanzioni o le azioni correttive sono tempestive e proporzionate.

Insight chiave

Anche in assenza di una seconda linea o di un comitato endoconsiliare, un'azienda di piccole dimensioni può applicare tutti i 15 requisiti previsti dal Requisito Tematico sul Comportamento Organizzativo attraverso meccanismi semplificati: semplici registri, supervisione diretta del responsabile aziendale, revisioni informali e formazione adeguata. Ciò dimostra che il Requisito Tematico è pratico e rilevante per tutte le organizzazioni, indipendentemente dalle dimensioni.

Appendice C. Tool di documentazione opzionale

Gli Internal Auditor devono esercitare il giudizio professionale per determinare l'applicabilità dei requisiti sulla base del risk assessment e documentare in modo appropriato l'esclusione di determinati requisiti. Il Requisito Tematico può essere documentato nel Piano di Audit o nelle carte di lavoro dell'incarico, a giudizio dell'Internal Auditor. I requisiti possono essere coperti da uno o più incarichi di Internal Audit. Inoltre, i requisiti potrebbero non essere tutti applicabili. La tabella riportata di seguito offre un'opzione per documentare la conformità al Requisito Tematico sul Comportamento Organizzativo, ma il suo utilizzo non è obbligatorio.

Governance del Comportamento Organizzativo

Requisito	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
A. Il Board esercita la supervisione e il Top Management struttura ruoli e responsabilità per evitare conseguenze non intenzionali derivanti da un comportamento organizzativo non allineato. Le conseguenze non intenzionali includono conflitti di interesse o processi decisionali poco chiari.		
B. Il Board esercita la supervisione e il Top Management attribuisce e mantiene la responsabilità individuale e di gruppo rispetto alle aspettative comportamentali, garantendo che ruoli e responsabilità siano assunti, compresi e costantemente allineati agli obiettivi dell'organizzazione.		

Requisito	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
C. Sono in atto processi di governance per assicurare il monitoraggio, la valutazione e la messa in discussione regolari dell'allineamento tra le comportamenti osservati e gli obiettivi dell'organizzazione, nonché l'adozione di azioni in caso di disallineamenti.		
D. Le policy e le procedure che affrontano i protocolli di rischio comportamentale sono stabilite e periodicamente riviste per verificarne la pertinenza e l'accuratezza. Tali policy e procedure sono comunicate in modo efficace e integrate nelle operazioni e nei processi decisionali dell'organizzazione.		

Risk management del Comportamento Organizzativo

Requisito	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
A. L'organizzazione ha definito in modo appropriato un approccio alla gestione dei rischi comportamentali, includendo le caratteristiche comportamentali critiche per il raggiungimento degli obiettivi organizzativi.		
B. Il monitoraggio del comportamento organizzativo è adeguato e tempestivo, con risultati comunicati agli stakeholder.		
C. Gli scostamenti tra le aspettative comportamentali e i comportamenti effettivi, unitamente alle relative analisi delle root cause, sono comunicati in modo efficace e coerente agli stakeholder.		

Requisito	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
D. Gli scostamenti tra le aspettative comportamentali e le prassi correnti vengono risolti con il contributo degli stakeholder. Le azioni di risoluzione sono monitorate fino al completamento e misurate in modo efficace per garantire che siano intraprese azioni adeguate.		

Controlli sul Comportamento Organizzativo

Requisito	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
A. L'organizzazione ha elaborato un approccio per identificare e mitigare gli schemi comportamentali che possono rappresentare rischi per il raggiungimento degli obiettivi organizzativi. Tra gli esempi vi sono le valutazioni delle performance e le review del rischio operativo.		
B. L'organizzazione definisce un tono chiaro e coerente riguardo ai comportamenti attesi e comunica tali aspettative attraverso canali affidabili e accessibili. Viene mantenuto un meccanismo strutturato di feedback per valutare la comprensione da parte dei dipendenti, il loro livello di adesione e per consentire le modifiche necessarie.		
C. Sono implementati processi che incoraggiano la segnalazione di comportamenti organizzativi in conflitto con il raggiungimento degli obiettivi dell'organizzazione. Tali processi includono protocolli di protezione e di risoluzione.		
D. Sono in essere programmi di incentivazione, comprendenti remunerazione e premi non monetari, adeguatamente comunicati e allineati agli obiettivi dell'organizzazione e ai requisiti normativi. Sono inoltre previsti disincentivi e conseguenze per comportamenti organizzativi impropri.		
E. È implementato un processo per la gestione delle criticità, che comprende l'identificazione e la correzione di schemi comportamentali non allineati con gli obiettivi dell'organizzazione e l'escalation delle problematiche quando necessario.		

Requisito	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
F. Programmi di formazione e sensibilizzazione, progettati per garantire l'allineamento tra comportamento organizzativo e obiettivi dell'organizzazione vengono erogati periodicamente e in modo efficace.		
G. I processi di acquisizione dei talenti e di onboarding sono allineati alle aspettative dell'organizzazione in merito ai comportamenti e includono le competenze comportamentali.		

Appendice D. Corrispondenza con il COSO Framework

La tabella che segue mette in corrispondenza i requisiti relativi alla governance, al risk management e ai processi di controllo previsti dal Requisito Tematico sul Comportamento Organizzativo con il *COSO Internal Control – Integrated Framework* (2013) e il *COSO Enterprise Risk Management Framework* (2017). Questo riferimento-incrociato consente agli Internal Auditor di riconciliare i test basati sul-COSO con la copertura prevista dal Requisito Tematico sul Comportamento Organizzativo.

Requisiti di governance

Requisito	Riferimento al COSO Internal Control (2013)	Riferimento al COSO ERM (2017)
A. Il Board esercita la supervisione e il Top Management struttura ruoli e responsabilità per evitare conseguenze non intenzionali derivanti da un comportamento organizzativo non allineato. Le conseguenze non intenzionali includono conflitti di interesse o processi decisionali poco chiari.	Ambiente di controllo: Principio 2 (indipendenza del Board e supervisione dei canali di escalation), Principio 3 (struttura, autorità e responsabilità).	Governance e cultura: Principio 1 (esercita la supervisione del rischio da parte del Board), Principio 2 (stabilisce le strutture operative).
B. Il Board esercita la supervisione e il Top Management attribuisce e mantiene la responsabilità individuale e di gruppo rispetto alle aspettative comportamentali, garantendo che ruoli e responsabilità siano assunti, compresi e costantemente allineati agli obiettivi dell'organizzazione.	Ambiente di controllo: Principio 1 (integrità e valori etici), Principio 5 (responsabilità e misure di performance).	Governance e cultura: Principi 4-5 (dimostra impegno verso i valori fondamentali; attrae, sviluppa e trattiene persone capaci).

Requisito	Riferimento al COSO Internal Control (2013)	Riferimento al COSO ERM (2017)
C. Sono in atto processi di governance per assicurare il monitoraggio, la valutazione e la messa in discussione regolari dell'allineamento tra le evidenze comportamentali e gli obiettivi dell'organizzazione, nonché l'adozione di azioni in caso di disallineamenti.	Monitoraggio: Principio 16 (valutazioni continue/separate), Principio 17 (valuta e comunica le carenze); Informazione e comunicazione: Principio 13 (utilizza informazioni rilevanti), Principio 14 (comunica internamente), Principio 15 (comunica all'esterno, se pertinente).	Governance e cultura: Principio 1 (esercita la supervisione del rischio da parte del Board); Performance: Principi 10-14 (identifica i rischi, valuta la gravità, prioritizza i rischi, implementa le risposte ai rischi); Informazione, comunicazione e reporting: Principi 18-20 (reporting su formazione e sensibilizzazione).
D. Le policy e le procedure che affrontano i protocolli di rischio comportamentale sono stabilite e periodicamente riviste per verificarne la pertinenza e l'accuratezza. Tali policy e procedure sono comunicate in modo efficace e integrate nelle operazioni aziendali e nei processi decisionali.	Attività di controllo: Principio 10 (seleziona e sviluppa attività di controllo), Principio 12 (implementa tramite policy e procedure).	Riesame e revisione: Principi 15-17 (valuta i cambiamenti; riesamina le performance; persegue il miglioramento).

Requisiti di risk management

Requisito	Riferimento al COSO Internal Control (2013)	Riferimento al COSO ERM (2017)
A. L'organizzazione ha definito in modo appropriato un approccio alla gestione dei rischi comportamentali, includendo le caratteristiche comportamentali critiche per il raggiungimento degli obiettivi organizzativi.	Risk assessment: Principio 6 (definisce obiettivi adeguati), Principio 7 (identifica e analizza il rischio), Principio 8 (valuta il rischio di frode), Principio 9 (identifica e analizza i cambiamenti significativi).	Governance e cultura: Principi 4-5 (dimostra impegno verso i valori fondamentali; attrae, sviluppa e trattiene persone capaci); Definizione della strategia e degli-obiettivi: Principi 6-9 (definisce il risk appetite, valuta strategie alternative, considera il rischio nella definizione degli obiettivi).

Requisito	Riferimento al COSO Internal Control (2013)	Riferimento al COSO ERM (2017)
B. Il monitoraggio del comportamento organizzativo è adeguato e tempestivo, con risultati comunicati agli stakeholder.	Informazione e comunicazione: Principio 13 (utilizza informazioni rilevanti), Principio 14 (comunica internamente); Monitoraggio: Principio 16 (valutazioni continue/separate), Principio 17 (valuta e comunica le carenze).	Performance: Principi 10-14 (identifica i rischi, valuta la gravità, prioritizza i rischi, implementa le risposte al rischi); Informazione, comunicazione e reporting: Principi 18-20 (reporting su formazione e sensibilizzazione).
C. Gli scostamenti tra le aspettative comportamentali e i comportamenti effettivi, unitamente alle relative analisi delle root cause, sono comunicati in modo efficace e coerente agli stakeholder.	Informazione e comunicazione: Principio 14 (comunica internamente), Principio 15 (comunica all'esterno, se pertinente).	Informazione, comunicazione e reporting: Principi 19-20 (comunica le informazioni sui rischi; riferisce su rischio, cultura e performance).
D. Gli scostamenti tra le aspettative comportamentali e le prassi correnti vengono risolti con il contributo degli stakeholder. Le azioni di risoluzione sono monitorate fino al completamento e misurate in modo efficace per garantire che siano intraprese azioni adeguate.	Attività di controllo: Principio 10 (seleziona e sviluppa attività di controllo), Principio 12 (implementa tramite policy e procedure); Monitoraggio: Principio 16 (valutazioni continue/separate), Principio 17 (valuta e comunica le carenze).	Riesame e revisione: Principi 15-17 (valuta i cambiamenti; riesamina le performance; persegue il miglioramento).

Requisiti di controllo

Requisito	Riferimento al COSO Internal Control (2013)	Documentazione di riferimento
A. L'organizzazione ha elaborato un approccio per identificare e mitigare gli schemi comportamentali che possono rappresentare rischi per il raggiungimento degli obiettivi organizzativi. Tra gli esempi vi sono le performance review e le review del rischio operativo.	Risk assessment: Principio 7 (identifica e analizza il rischio), Principio 8 (valuta il rischio di frode), Principio 9 (identifica e analizza i cambiamenti significativi); Monitoraggio: Principio 16 (valutazioni continue/separate), Principio 17 (valuta e comunica le carenze).	Performance: Principi 10-14 (identifica i rischi, valuta la gravità, prioritizza i rischi, implementa le risposte al rischi); Riesame e revisione: Principi 15-17 (valuta i cambiamenti; riesamina le performance; persegue il miglioramento).

Requisito	Riferimento al COSO Internal Control (2013)	Documentazione di riferimento
B. L'organizzazione definisce un tono chiaro e coerente riguardo ai comportamenti attesi e comunica tali aspettative attraverso canali affidabili e accessibili. Viene mantenuto un meccanismo strutturato di feedback per valutare la comprensione da parte dei dipendenti, il loro livello di adesione e per consentire le modifiche necessarie.	Ambiente di controllo: Principio 1 (integrità e valori etici), Principio 5 (responsabilità e misure di performance); Informazione e comunicazione: Principio 13 (utilizza informazioni rilevanti), Principio 14 (comunica internamente), Principio 15 (comunica all'esterno, se pertinente).	Governance e cultura: Principio 1 (esercita la supervisione del rischio da parte del Board), Principio 4 (dimostra impegno verso i valori fondamentali), Principio 5 (attrae, sviluppa e trattiene persone capaci); Informazione, comunicazione e reporting: Principi 18-20 (reporting su formazione e sensibilizzazione).
C. Sono implementati processi che incoraggiano la segnalazione di comportamenti organizzativi in conflitto con il raggiungimento degli obiettivi dell'organizzazione. Tali processi includono protocolli di protezione e di risoluzione.	Informazione e comunicazione: Principio 14 (canali di comunicazione interna); Ambiente di controllo: Principio 2 (indipendenza del Board e supervisione dei canali di escalation).	Governance e cultura: Principio 1 (esercita la supervisione del rischio da parte del Board), Principio 4 (dimostra impegno verso i valori fondamentali), Principio 5 (attrae, sviluppa e trattiene persone capaci); Informazione, comunicazione e reporting: Principi 19-20 (comunica le informazioni sui rischi; riferisce su rischio, cultura e performance).
D. Sono in essere programmi di incentivazione, comprendenti remunerazione e premi non monetari, adeguatamente comunicati e allineati agli obiettivi dell'organizzazione e ai requisiti normativi. Sono inoltre previsti disincentivi e conseguenze per comportamenti organizzativi impropri.	Ambiente di controllo: Principio 1 (integrità e valori etici), Principio 5 (responsabilità e misure di performance).	Governance e cultura: Principio 4 (dimostra impegno verso i valori fondamentali), Principio 5 (attrae, sviluppa e trattiene persone capaci); Performance: Principi 10-14 (identifica i rischi, valuta la gravità, prioritizza i rischi, implementa le risposte ai rischi).
E. È implementato un processo per la gestione delle criticità, che comprende l'identificazione e la correzione di schemi comportamentali non allineati con gli obiettivi dell'organizzazione e l'escalation delle problematiche quando necessario.	Monitoraggio: Principio 16 (valutazioni continue/separate), Principio 17 (valuta e comunica le carenze); Informazione e comunicazione: Principio 13 (utilizza informazioni rilevanti).	Riesame e revisione: Principi 15-17 (valuta i cambiamenti; riesamina le performance; persegue il miglioramento); Performance: Principi 10-14 (identifica i rischi, valuta la gravità, prioritizza i rischi, implementa le risposte al rischi).

Requisito	Riferimento al COSO Internal Control (2013)	Documentazione di riferimento
F. Programmi di formazione e sensibilizzazione, progettati per garantire l'allineamento tra comportamento organizzativo e obiettivi dell'organizzazione vengono erogati periodicamente e in modo efficace.	Ambiente di controllo: Principio 4 (impegno per la competenza); Informazione e comunicazione: Principio 13 (utilizza informazioni rilevanti).	Governance e cultura: Principio 5 (attrae, sviluppa e trattiene persone capaci); Informazione, comunicazione e reporting: Principi 18-20 (reporting su formazione e sensibilizzazione).
G. I processi di acquisizione dei talenti e di onboarding sono allineati alle aspettative dell'organizzazione in merito al comportamento e includono le competenze comportamentali.	Ambiente di controllo: Principio 1 (integrità e valori etici), Principio 4 (impegno per la competenza).	Governance e cultura: Principio 5 (attrae, sviluppa e trattiene persone capaci).

Appendice E. Attività di Audit e assurance che riguardano i comportamenti

Gli auditor potrebbero scoprire che le attività che già svolgono possono fornire una base utile per la loro applicazione del Requisito Tematico sul Comportamento Organizzativo. La tabella che segue riporta alcuni esempi di Audit mirati e di elementi comuni di Audit che possono essere messi in corrispondenza con i requisiti e utilizzati, ove applicabile, per dimostrare la conformità. Questi esempi non dovrebbero essere considerati come Audit obbligatori; sono forniti per mostrare come attività di Audit comunemente condotte possano fornire una potenziale copertura dei Requisiti Tematici.

Esempi di attività di Audit e assurance che possono riguardare direttamente o indirettamente i comportamenti includono:

Area	Audit mirati	Elementi di verifica comuni negli Audit
Governance	• Cultura del rischio • Corporate governance • Revisione dell'efficacia del Board e della leadership • Risposta regolatoria • Retribuzione basata su incentivi • Misurazioni delle performance • Strategia e pianificazione aziendale • Pianificazione della trasformazione • Fusioni e acquisizioni	• Policy e procedure aziendali • Controlli a livello di entità/di revisione manageriale • Azioni correttive su questioni regolatorie a livello organizzativo (ad esempio piano di miglioramento aziendale) • Delega di autorità
Risk Management	• Funzione legale e compliance • Framework di gestione del rischio • Programma di etica e compliance • ESG • Revisione frodi/linea diretta whistleblowing	• Mantenimento dei registri dei rischi e dei controlli • Autovalutazioni da parte del management • Risposta a carenze di controllo e a rilievi di Audit/altre verifiche

Area	Audit mirati	Elementi di verifica comuni negli Audit
Controlli	• Risorse umane (inclusi reclutamento e retention) • Processi di vendita (ad esempio condotta commerciale e compliance) • Approvvigionamento (ad esempio indipendenza dei fornitori, spese di rappresentanza) • Filiale/entità (ad esempio gestione e revisione) • Linea diretta frodi/whistleblowing	• Segregation of duties • Controlli di revisione e monitoraggio da parte del management • Rischi di frode individuali • Competenze e consapevolezza del rischio • Azioni correttive su processi e controlli

Informazioni sull'Institute of Internal Auditors

L'Institute of Internal Auditors (IIA) è un'associazione professionale internazionale che conta più di 265.000 membri a livello globale e ha rilasciato più di 200.000 certificazioni di Certified Internal Auditor® (CIA®) in tutto il mondo. Fondata nel 1941, l'IIA è riconosciuta in tutto il mondo come leader nella professione dell'Internal Audit per quanto riguarda gli standard, le certificazioni, la formazione, la ricerca e la guida tecnica. Per ulteriori informazioni, visitare theiia.org.

Esclusione di responsabilità

Copyright

Dicembre 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101