Third-Party

Topical Requirement

Requisito Tematico

The Institute of Internal Auditors

Tradotto da:

Associazione Italiana Internal Auditors

Requisito Tematico sulle Terze Parti

L'International Professional Practices Framework® comprende i Global Internal Audit Standards™, i Requisiti Tematici e le Global Guidance. I Requisiti Tematici sono una componente obbligatoria e devono essere utilizzati insieme agli Standards, che costituiscono la base autorevole delle pratiche di audit richieste.

I Requisiti Tematici forniscono chiare indicazioni per gli Internal Auditor, stabilendo un livello minimo di riferimento per gli incarichi di audit su specifiche aree di rischio. Il profilo di rischio specifico dell'organizzazione potrebbe richiedere agli Internal Auditor di considerare ulteriori aspetti dell'argomento in questione.

La conformità ai Requisiti Tematici aumenterà la coerenza con cui vengono svolti i servizi di Internal Auditing e migliorerà la qualità e l'affidabilità degli incarichi di audit e dei risultati. In definitiva, i Requisiti Tematici elevano la professione dell'Internal Audit.

Gli Internal Auditor devono applicare i Requisiti Tematici in conformità ai Global Internal Audit Standards. La conformità ai Requisiti Tematici è obbligatoria per i servizi di assurance e raccomandata per i servizi di advisory. Il Requisito Tematico si applica quando l'argomento è:

1. Oggetto di un incarico incluso nel Piano di Audit.
2. Identificato durante l'esecuzione di un incarico.
3. Oggetto di una richiesta di incarico non prevista nel piano di Audit originale.

Deve essere documentata e conservata evidenza della valutazione di applicabilità di ciascun requisito previsto dal Requisito Tematico. È possibile che non tutti i singoli requisiti siano applicabili in ogni incarico; qualora alcuni requisiti vengano esclusi, la motivazione deve essere documentata e conservata. La conformità al Requisito Tematico è obbligatoria e sarà oggetto di valutazione durante le attività di quality assessment.

Terze parti

Una terza parte è un soggetto esterno — persona fisica, gruppo o entità — con cui un'organizzazione ("l'organizzazione principale") instaura un rapporto commerciale al fine di ottenere prodotti o servizi. Il rapporto può essere formalizzato tramite un contratto, un accordo o altri mezzi. Questo Requisito Tematico utilizza il termine "terza parte" per riferirsi a fornitori, appaltatori, subappaltatori, fornitori di servizi esternalizzati, altre agenzie e consulenti. Il termine include gli accordi tra una terza parte e i suoi subfornitori, spesso indicati come "N" parti.

Il Requisito Tematico si applica quando la funzione di Internal Audit svolge incarichi di assurance su terze parti e/o su qualsiasi rapporto subappaltato, inclusi quelli di quarto livello o di livello ulteriore, consentiti dal contratto o dall'accordo tra la terza parte e l'organizzazione principale. Gli Internal Auditor dovrebbero prioritizzare tutte le parti incluse nella filiera con un approccio basato sul rischio, come

illustrato più avanti nella sezione sul risk management. Gli Internal Auditor devono applicare tutti i requisiti indicati dai risultati del risk assessment, e le esclusioni devono essere documentate.

Questo Requisito Tematico non è destinato a trattare relazioni, interessi o coinvolgimenti tra l'organizzazione principale e regulator, agenti, fiduciari o membri del Board, né relazioni interne, quali quelle con i dipendenti.

Il termine "terza parte" può essere definito e utilizzato in modo diverso a seconda del settore o di altri contesti. Agli Internal Auditor è concessa flessibilità e dovrebbero affidarsi al proprio giudizio professionale per adattare il Requisito Tematico alla definizione di terza parte adottata dall'organizzazione principale.

L'organizzazione principale (l'organizzazione che stipula un accordo con una terza parte) mantiene la responsabilità per i rischi associati al conseguimento dei propri obiettivi, anche quando per raggiungere uno o più obiettivi si avvale di una terza parte. La collaborazione con terze parti comporta rischi che devono essere identificati, valutati e gestiti attraverso adeguati processi di governance, risk management e controllo, come indicato nel presente Requisito Tematico. Se una terza parte non adempie al contratto, partecipa a pratiche non etiche o subisce un'interruzione dell'attività, l'organizzazione principale può subirne ripercussioni. Le categorie e gli esempi di rischi legati a terze parti includono:

- Rischi strategici, come la capacità di realizzare la mission dell'organizzazione principale e/o i suoi obiettivi di alto livello, o di gestire gli impatti di fusioni e acquisizioni.
- Rischi reputazionali, come i danni causati all'ambiente o al rapporto e alla fiducia tra l'organizzazione principale e i clienti, i consumatori e gli stakeholder.
- Rischi etici, come carenze di integrità, conflitti di interesse, tangenti e corruzione.
- Rischi operativi, come la sicurezza fisica e delle informazioni, insider risk, le interruzioni dei servizi e il mancato raggiungimento degli obiettivi.
- Rischi finanziari, come l'insolvenza e le frodi da terze parti.
- Rischi di conformità, relativi al rispetto delle normative vigenti a livello locale, nazionale e internazionale.
- Rischi di cybersecurity e altre forme di protezione dei dati, come la compromissione e la perdita di dati sensibili.
- Rischi di information technology, come la carenza di servizi a supporto dei processi operativi critici.
- Rischi legali, quali conflitti di interesse, controversie e contenziosi per violazioni contrattuali.
- Rischi di sostenibilità, riguardanti aspetti ambientali, sociali e di governance. Ad esempio, i rischi legati all'impatto dell'organizzazione sull'ambiente naturale e i rischi connessi alle sue interazioni con le comunità.
- Rischi geopolitici, come controversie commerciali/sanzioni e instabilità politica.

Il ciclo di vita delle terze parti comprende la selezione, la contrattualizzazione, l'onboarding, il monitoraggio e l'offboarding. Gli Internal Auditor, nel valutare i processi di governance, risk management e controllo, dovrebbero tener conto di queste fasi.

Verifica e valutazione dei processi di Governance, Risk Management e Controllo relativi alle terze parti

Questo Requisito Tematico fornisce un approccio coerente e completo per valutare la progettazione e l'implementazione dei processi di governance, risk management e controllo relativi alle terze parti. I requisiti rappresentano una base di riferimento per la valutazione.

GOVERNANCE

Requisiti:

Gli Internal Auditor devono valutare i seguenti aspetti della governance esercitata dall'organizzazione principale sulle terze parti, inclusa la supervisione del Board:

A. Viene stabilito, implementato e periodicamente rivisto un approccio formale per determinare se stipulare un contratto con una terza parte. L'approccio include specifici criteri per definire e valutare le risorse necessarie e disponibili per raggiungere gli obiettivi mediante la fornitura di un prodotto o servizio.

B. Vengono stabilite policy e procedure per definire, valutare e gestire i rapporti e i rischi con le terze parti lungo tutto il ciclo di vita delle stesse. Le policy e le procedure sono conformi ai requisiti normativi applicabili e vengono periodicamente riviste e aggiornate per rafforzare l'ambiente di controllo.

C. Vengono definiti ruoli e responsabilità per la gestione delle terze parti all'interno dell'organizzazione, specificando chi seleziona, gestisce le terze parti, comunica con esse e ne esegue il monitoraggio, e chi deve essere informato in merito alle attività delle terze parti. Esiste un processo per garantire che le persone aventi ruoli e responsabilità relativi alle terze parti possiedano competenze adeguate.

D. Vengono definiti protocolli di comunicazione con gli stakeholder rilevanti, che includono la tempestiva rendicontazione delle performance, dei rischi e della compliance (in particolare le violazioni di leggi e normative) delle terze parti rilevanti. Le terze parti sono prioritizzate secondo un approccio basato sul rischio. Tra gli stakeholder rilevanti si possono includere il Board, il Top Management, le funzioni Procurement, Operations, Risk management, Compliance, Legale, Information technology, Information security, Risorse umane e altre.

RISK MANAGEMENT

Requisiti:

Gli Internal Auditor devono valutare i seguenti aspetti della gestione del rischio terze parti dell'organizzazione.

A. I processi per la gestione del rischio terze parti sono standardizzati e completi, includono ruoli e responsabilità e indirizzano adeguatamente i rischi chiave dell'organizzazione (quali quelli strategici, reputazionali, etici, operativi, finanziari, compliance, cybersecurity, information technology, legali, sostenibilità e geopolitici). Il rispetto dei processi viene monitorato e vengono implementate azioni correttive in caso di deviazioni.

B. I rischi connessi alle terze parti vengono identificati e valutati regolarmente lungo l'intero ciclo di vita. Tutte le terze parti incluse nella filiera sono prioritizzate secondo la valutazione dei rispettivi rischi (risk assessment). Anche le risposte al rischio vengono classificate e prioritizzate. Il risk assessment viene periodicamente rivisto e aggiornato.

C. Le risposte al rischio sono adeguate, accurate e commisurate al livello di priorità. Le risposte al rischio vengono implementate, riesaminate, approvate, monitorate, valutate e adattate secondo necessità.

D. Esistono processi per la gestione e, se necessario, per l'escalation delle problematiche derivanti da terze parti, garantendo la responsabilità per i risultati e aumentando la probabilità di rispettare i termini dei contratti o di altri accordi. Se una terza parte non risponde alle problematiche oggetto di escalation, sono previsti processi che consentono al management di valutare i rischi derivanti dal rapporto commerciale in essere e di intraprendere, se necessario, ulteriori azioni, attività di remediation o la cessazione del rapporto.

CONTROLLI

Requisiti:

Gli Internal Auditor devono valutare i seguenti controlli relativi alle terze parti prioritizzate in base al rischio. La valutazione deve includere i processi adottati dal management per l'analisi e il monitoraggio continuo delle terze parti dell'organizzazione.

A. È implementato un solido processo di due diligence per l'individuazione e la selezione delle terze parti, supportato da un business case documentato e approvato, o da altra documentazione pertinente, che descriva e giustifichi la necessità e la natura del rapporto con la terza parte.

B. La contrattualizzazione e l'approvazione vengono effettuate in conformità alle policy e alle procedure di gestione del rischio terze parti dell'organizzazione e prevedono la collaborazione tra specifiche funzioni dell'organizzazione.

C. I contratti o gli accordi definitivi vengono rivisti e approvati da tutti gli stakeholder rilevanti, incluse le funzioni Legale e Compliance, vengono firmati dalle persone autorizzate da entrambe le parti e archiviati in modo sicuro. Ciascun contratto viene affidato alla responsabilità di un contract manager.

D. Viene mantenuto un elenco accurato, completo e aggiornato di tutti i rapporti con terze parti, ad esempio all'interno di un sistema centralizzato di gestione dei contratti.

E. Vengono stabiliti, seguiti e documentati processi di onboarding per creare le condizioni affinché le terze parti rispettino i termini del contratto o dell'accordo.

F. Esistono processi di monitoraggio continuo per valutare se le terze parti operano in conformità ai termini del contratto o dell'accordo durante l'intero ciclo di vita e se rispettano gli obblighi contrattuali. I processi includono la verifica dell'affidabilità delle informazioni fornite e la rivalutazione periodica delle performance e ad ogni modifica dell'accordo.

G. Vengono definiti protocolli per avviare azioni correttive nel caso in cui una terza parte non soddisfi le aspettative o comporti un rischio maggiore o imprevisto. I protocolli includono l'escalation degli incidenti in base alla gravità, la conduzione di verifiche post-incidente e l'analisi delle cause profonde degli incidenti.

H. Le date di scadenza e di rinnovo dei contratti vengono monitorate e, se necessario, vengono intraprese azioni per il rinnovo.

I. Viene implementato, seguito e documentato un piano di offboarding per garantire che i requisiti contrattuali relativi a tempistiche e aspettative siano rispettati. I processi includono le modalità per:

- Interrompere il rapporto con la terza parte.
- Sostituire, se necessario, la terza parte.
- Riassegnare la custodia, restituire o distruggere i dati sensibili dell'organizzazione conservati presso la terza parte.
- Revocare l'accesso della terza parte a sistemi, tool e strutture.

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 maggiori informazioni, visitare theiia.org.

Copyright

Settembre 2025

The Institute of Internal Auditors

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