# Third-Party

## Topical Requirement

## Requisito Tematico

## 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. 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, 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 la pianificazione delle attività 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 gliincarichi 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).

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 elevato rischio potrebbero dover analizzare ulteriori aspetti.

Se la funzione di Internal Audit non possiede le competenze necessarie per svolgere incarichi su un argomento oggetto di un Requisito Tematico, il CAE deve stabilire come ottenere le risorse e comunicare tempestivamente al Board e al Top Management l'impatto delle limitazioni e come saranno affrontate eventuali carenze di risorse. Il CAE è responsabile di garantire la conformità della funzione di Internal Audit ai Requisiti Tematici, indipendentemente da come vengono ottenute le risorse (Standard 3.1 Competenza, 7.2 Qualifiche del Chief Audit Executive, 8.2 Risorse, 10.2 Risorse Umane).

## 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. Leggi locali, normative, aspettative degli organi di supervisione e altri framework riconosciuti a livello professionale possono imporre requisiti aggiuntivi o più specifici. Gli Internal Auditor devono comprendere e rispettare le leggi e/o le normative specifiche del settore e dell'area in cui opera l'organizzazione, incluse quelle relative alla divulgazione delle informazioni se richiesto, conformemente allo Standard 1.3 Comportamento legale ed etico. Gli Internal Auditor potrebbero aver già integrato tali requisiti aggiuntivi nei programmi di audit e nelle procedure di testing e dovrebbero confrontarli con il Requisito Tematico per garantire una copertura adeguata.

La copertura del Requisito Tematico può essere documentata nel Piano di Audit o nelle carte 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, implementi 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 sarà valutata nei quality assessment.

## Terza parte

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 per fornire all'organizzazione prodotti, servizi, manodopera, attività di produzione o soluzioni informatiche, quali l'archiviazione, l'elaborazione e la manutenzione dei dati.

> 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 termine "terza parte" può essere utilizzato in modo diverso a seconda del settore o di altri contesti. Ogni funzione di Internal Audit ha la flessibilità di applicare il Requisito Tematico secondo il proprio giudizio, in funzione della definizione di terza parte adottata dall'organizzazione principale (l'organizzazione che stipula un accordo con la terza parte). Nel Requisito Tematico sulle Terze Parti e nella relativa User Guide, il termine "terza parte" si riferisce a fornitori, appaltatori, subappaltatori, fornitori di servizi esternalizzati, altre agenzie e consulenti. Il termine "terza parte" include tutte queste tipologie di accordi, compresi quelli tra una terza parte e i suoi subfornitori, spesso indicati come "subappaltatori a valle", "quarte parti", "quinte parti" o "n-esime parti".

Questo Requisito Tematico non è destinato a trattare relazioni, interessi o coinvolgimenti tra l'organizzazione principale e i regolatori, agenti, broker, investitori, fiduciari/membri del Board, servizi pubblici e privati cittadini, né relazioni interne, quali quelle con i dipendenti o i fornitori di servizi intragruppo.

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'efficacia dei processi di gestione dei rapporti con le terze parti può essere valutata nell'ambito dell'organizzazione e/o a livello di uno o più singoli contratti, accordi o rapporti. Gli Internal Auditor dovrebbero adottare un approccio top-down per comprendere policy, procedure, processi, framework e ciclo di vita che l'organizzazione adotta per gestire i rapporti con le terze parti. Gli Internal Auditor dovrebbero usare il proprio giudizio per comprendere le sfumature dei rischi legati alle terze parti in funzione dei settori, delle organizzazioni e degli argomenti specifici dell'incarico. In linea con lo Standard 5.1 Utilizzo delle informazioni, gli Internal Auditor dovrebbero conoscere e rispettare tutte le policy e le procedure relative alle informazioni di terze parti a cui possono accedere.

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.

Il Requisito Tematico sulle Terze Parti e la relativa User Guide fanno riferimento alle fasi del rapporto tra l'organizzazione e le sue terze parti, note anche come fasi del ciclo di vita: selezione, contrattualizzazione, onboarding, monitoraggio e offboarding. Queste fasi saranno utilizzate ai fini del Requisito Tematico sulle Terze Parti e della relativa User Guide, anche se alcuni settori hanno versioni proprie del ciclo di vita. Le fasi sono:

- Selezione: include i processi volti a determinare la necessità di una terza parte, il piano per il suo utilizzo e la due diligence per la selezione. Inoltre, la selezione dovrebbe includere la valutazione dei rischi associati alle terze parti potenziali e a quelle già utilizzate.
- Contrattualizzazione: include i processi di due diligence per la redazione, la negoziazione, l'approvazione e l'implementazione di un accordo legale con la terza parte.
- Onboarding: inizia con la firma del contratto per avviare il rapporto e stabilisce le basi affinché le terze parti soddisfino i termini del contratto o dell'accordo.
- Monitoraggio: include i processi di gestione e di monitoraggio continuo della terza parte, dopo che il contratto è stato stipulato e approvato. L'approccio è solitamente sistematico e basato sul rischio e dovrebbe prevedere il miglioramento continuo. Il monitoraggio, se necessario, include anche il rinnovo dei contratti o degli accordi in corso con le terze parti.
- Offboarding: include i processi per terminare contratti e accordi, il mantenimento di exit strategy per le terze parti prioritizzate in base al rischio, e la cessazione dei rapporti quando necessario. I processi utilizzano in genere un approccio basato sul rischio e possono prevedere un exit plan formale.

L'organizzazione principale 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. Il coinvolgimento di terze parti può ridurre alcuni dei costi sostenuti dall'organizzazione per l'esecuzione dei processi. Tuttavia, può introdurre rischi operativi, poiché l'organizzazione principale ha meno visibilità e autorità sui processi di controllo della terza. 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.

L'organizzazione principale deve identificare, valutare e gestire i rischi attraverso adeguati processi di governance, risk management e controllo. Le categorie e gli esempi di rischi legati a terze parti includono:

- Rischi strategici, come la capacità di realizzare la missione dell'organizzazione 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 clienti, consumatori e 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 o 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.

Gli Internal Auditor dovrebbero tener conto di ogni fase del ciclo di vita delle terze parti quando valutano i requisiti per i processi di governance, risk management e controllo.

I requisiti del Requisito Tematico sulle Terze Parti sono suddivisi in tre sezioni conformemente allo Standard 9.1 Comprensione dei processi di governance, risk management e controllo:

- Governance – chiara definizione di obiettivi e strategie per l'utilizzo delle terze parti a supporto degli obiettivi, delle policy e delle procedure dell'organizzazione.
- Risk Management - processi per identificare, analizzare, gestire e monitorare i rischi derivanti dall'utilizzo di terze parti, 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 connessi all'utilizzo di terze parti.

In aggiunta al Requisito Tematico e alla presente User Guide, gli Internal Auditor possono fare riferimento a ulteriori linee guida professionali in materia di terze parti, come le Global Guidance dell'IPPF e risorse specifiche di settore.

# Aspetti da valutare

Per applicare i requisiti contenuti nel Requisito Tematico sulle Terze Parti gli Internal Auditor possono tenere in considerazione i seguenti aspetti. Le dichiarazioni contrassegnate da lettere in ciascuna delle sezioni che seguono ribadiscono o parafrasano i requisiti corrispondenti del Requisito Tematico. Queste considerazioni non vincolanti sono fornite a scopo esemplificativo per illustrare possibili modalità di valutazione dei requisiti. Gli Internal Auditor dovrebbero applicare il proprio giudizio professionale nel determinare cosa includere nelle loro valutazioni.

## Aspetti da valutare sulla Governance

Per valutare come i processi di governance, inclusa la supervisione del Board, sono applicati agli obiettivi relativi alle terze parti, gli Internal Auditor possono esaminare evidenze quali:

**A.** La formalizzazione di un approccio o una strategia di valutazione basata sul rischio, per determinare se ricorrere o meno a una terza parte. L'approccio è sottoposto a revisione periodica e comprende:

- Un processo di implementazione dell'approccio chiaro, standardizzato e approvato dall'organizzazione.
- Allocazione di risorse (budget) sulla base di un'analisi costi-benefici per giustificare il ricorso a una terza parte, garantendo allineamento strategico ed efficientamento delle risorse.
- La valutazione da parte del management dei rischi e dei controlli, inclusi quelli relativi a problematiche con le terze parti.
- Risorse adeguate a contrattualizzare, gestire e monitorare la performance delle terze parti.
- L'integrazione del feedback degli stakeholder nell'approccio o nella strategia.

**B.** Policy, procedure e altra documentazione rilevante utilizzate per definire, valutare e gestire i rapporti con le terze parti lungo l'intero ciclo di vita. Le policy e le procedure possono includere:

- Strumenti e template standardizzati per facilitare i principali processi di governance, risk management e controllo.
- Processi per valutare periodicamente le policy e le procedure, determinarne l'adeguatezza e aggiornarle quando necessario.
- Criteri definiti per la selezione, la contrattualizzazione, l'onboarding, il monitoraggio e l'offboarding delle terze parti.
- L'individuazione e la revisione periodica dei requisiti normativi applicabili, al fine di garantirne l'allineamento con le policy e le procedure.
- Esercizi di benchmarking condotti per individuare e confrontare le best practice di gestione delle terze parti.

C. Ruoli e responsabilità definiti che supportano il conseguimento degli obiettivi relativi alle terze parti. Ulteriori evidenze possono includere:

- Processi per valutare se i valori, l'etica e la responsabilità sociale d'impresa della terza parte sono allineati ai principi dell'organizzazione principale. Il processo dovrebbe includere le modalità per affrontare tempestivamente potenziali conflitti di interesse o pratiche non etiche.
- Formazione periodica del personale che ricopre ruoli di gestione delle terze parti e valutazione periodica delle relative competenze.
- Un processo per valutare se il programma formativo è stato implementato al fine di diffondere la consapevolezza in merito alle terze parti nell'organizzazione.
- Ruoli e responsabilità allineati al Three Lines Model.

D. Comunicazione tempestiva e coinvolgimento degli stakeholder rilevanti lungo l'intero ciclo di vita delle terze parti (ad esempio il Board, il Top Management, la funzione procurement, le operations, il risk management, la compliance, la funzione legale, l'information technology, l'information security, le risorse umane e altri), tali attività comprendono:

- Informazioni sui rischi connessi alle terze parti e sulle potenziali vulnerabilità conosciute, riportate nei verbali delle riunioni, nei report o nelle email.
- Uno scambio di informazioni sulla gestione delle terze parti e la promozione della collaborazione (ad esempio, attraverso riunioni periodiche interfunzionali).

## Aspetti da valutare nel Risk Management

Per valutare come i processi di risk management sono applicati agli obiettivi relativi alle terze parti, gli Internal Auditor possono esaminare evidenze quali:

A. Processi di risk management standardizzati e completi per l'utilizzo di servizi di terze parti, che includono ruoli e responsabilità definiti e indirizzano in modo adeguato i rischi rilevanti per l'organizzazione:

- Processi di valutazione e gestione dei rischi connessi alle terze parti che includono le modalità attraverso cui i principali rischi vengono:
  - Inizialmente identificati e segnalati.
  - Analizzati per valutarne l'impatto sulla capacità di conseguire gli obiettivi dell'organizzazione.
  - Mitigati, prevedendo piani d'azione per ridurre il rischio a un livello accettabile.
  - Monitorati, prevedendo la rilevazione e la risposta ai primi alert e il reporting continuo fino alla completa risoluzione delle minacce.
- Viene effettuato un monitoraggio per garantire l'aderenza ai processi e l'attuazione di azioni correttive in caso di deviazioni, al fine di non compromettere gli obiettivi o la strategia di lungo termine dell'organizzazione.

- Un comitato di risk management o un altro gruppo fornisce una supervisione diretta sulle terze parti e riporta al Board. Il comitato ha uno scopo definito e si riunisce regolarmente. Le evidenze possono includere i verbali delle riunioni.

**B.** I rischi connessi alle terze parti vengono identificati e valutati regolarmente lungo l'intero ciclo di vita. Il risk assessment classifica e prioritizza le terze parti. Le risposte al rischio sono classificate e prioritizzate.

- Nel valutare i rischi legati alle terze parti l'organizzazione principale considera fattori quali la propria dimensione, il livello di maturità e il numero di terze parti coinvolte.
- Il risk assessment è documentato e identifica rischi inerenti e residui.
- L'organizzazione segue un processo di due diligence per rivedere e aggiornare il risk assessment.
- Vengono stabiliti criteri per classificare e prioritizzare le terze parti in base ai rischi. Esempi di tali criteri includono:
  - I servizi forniti sono fondamentali per l'operatività dell'organizzazione.
  - Il valore finanziario dell'accordo è rilevante.
  - Il rapporto è nuovo, è stato instaurato rapidamente e/o ha una durata prolungata.
  - Sono coinvolte più parti esterne.
  - La terza parte prevede di subappaltare parte o la totalità del lavoro.
- L'organizzazione adotta pratiche di risk assessment diffuse, che prevedono che il risk assessment sia effettuato il prima, solitamente durante l'analisi della proposta nella fase di selezione e prima dell'onboarding.
- I fornitori compilano un questionario per determinarne il loro livello di rischio e la relativa priorità, sulla base dei rischi inerenti. L'organizzazione garantisce che i questionari siano compilati da personale competente e siano sottoposti a revisione per assicurarne l'accuratezza.
- L'organizzazione ottiene aggiornamenti periodici sulla gestione del rischio terze parti dalle funzioni aziendali, quali l'information technology, la funzione procurement, il risk management, le risorse umane, la funzione legale, la compliance, le operations, la contabilità e la finanza.

**C.** Le risposte al rischio, come la mitigazione, l'accettazione, l'eliminazione e la condivisione, sono identificate e commisurate al livello di rischio.

- Le risposte al rischio sono documentate e tengono conto dell'ambiente di controllo della terza parte.
- È documentata la revisione dell'adeguatezza delle risposte ai rischi che superano la risk tolerance dell'organizzazione principale, in particolare quando tali rischi vengono accettati. Le risposte includono quelle per indirizzare i potenziali conflitti di interesse con terze parti.

D. I processi per la gestione e l'escalation dei rischi legati a terze parti, incluse le modalità di valutazione, assegnazione e prioritizzazione del livello di minaccia o di rischio. L'analisi può includere l'identificazione di:

- Definizioni e spiegazioni dei livelli di rischio dell'organizzazione, quali elevato, moderato e basso, e procedure di escalation per ciascuna categoria di rischio.
- Elenco delle terze parti prioritizzate in base ai rischi identificati e le modalità di gestione di ogni evento di rischio.
- Requisiti legali, normativi e di compliance applicabili.
- Impatto finanziario e non finanziario (ad esempio reputazionale) dei rischi.
- Processi per la comunicazione al management e ai dipendenti dei rischi legati a terze parti, incluso il regolare reporting del profilo di rischio al Board (o ad altro organo competente). Le comunicazioni dovrebbero includere aggiornamenti sulla risoluzione di eventuali problematiche riscontrate con le terze parti rilevanti.
- Processi per rivalutare la classificazione e la prioritizzazione quando cambiano i livelli di risk appetite e risk tolerance dell'organizzazione principale.

## Aspetti di Controllo da valutare

Per valutare l'applicazione dei processi di controllo ai rapporti con terze parti, gli Internal Auditor possono esaminare evidenze quali:

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.

- Il business case può inoltre:
  - Affrontare i rischi legati alla capacità della terza parte di soddisfare le aspettative e i potenziali impatti sull'organizzazione.
  - Include un'analisi dettagliata dei costi e dei benefici.
- Vengono seguiti processi di approvvigionamento consolidati, come gare d'appalto, richieste di offerta e sole sourcing. I processi includono:
  - Criteri per aspetti rilevanti come la revisione dei protocolli di cybersecurity, la verifica dei dati bancari, i controlli sul background finanziario e l'analisi della struttura organizzativa, dei precedenti penali e giudiziari, dei precedenti di guida, delle attività politiche e degli eventuali legami con attività criminali della terza parte.
  - Criteri di selezione ben definiti, inclusi quelli per valutare le performance pregresse, le referenze, la reputazione e i costi contrattuali.
  - Attività di due diligence per garantire una selezione appropriata dei fornitori, come la costituzione di team interfunzionali per esaminare le proposte. Al fine di mitigare il rischio di bias, i controlli su tali team di revisione includono procedure per la loro costituzione e disposizioni per la dichiarazione di potenziali conflitti di interesse.

- Due diligence nella valutazione dell'ambiente di controllo della terza parte; ad esempio, effettuando una visita in loco o verificando i seguenti aspetti relativi alla terza parte:
  - I report SOC (System and Organization Control).
  - La stabilità finanziaria.
  - L'atto costitutivo o il certificato di vigenza.
  - La trasparenza nei processi decisionali dei vertici aziendali e degli stakeholder.
  - La struttura organizzativa.
  - La stabilità operativa.
  - I protocolli di cybersecurity.
  - La conformità a leggi, normative e standard pertinenti.
  - L'etica.
  - I precedenti con l'organizzazione principale.
  - La reputazione.
- Evidenze attestanti che i potenziali fornitori o appaltatori avanzano alla fase di contrattualizzazione solo dopo che è stata completata la due diligence e che i risultati sono stati analizzati.

**B.** Le policy e le procedure di contrattualizzazione vengono stabilite e seguite.

- I contratti sono redatti in termini non ambigui.
- I rischi chiave vengono presi in considerazione nella fase di redazione del contratto e vengono inserite clausole pertinenti. Le problematiche da risolvere vengono comunicate alla terza parte durante questa fase.
- Gli elementi essenziali dei contratti vengono determinati in base alle policy e alle procedure di contrattualizzazione dell'organizzazione e al livello di priorità attribuito alla terza parte. Gli elementi possono includere:
  - Accordi di riservatezza (privacy).
  - Clausole di risoluzione e parametri specifici per l'accesso ai dati.
  - Requisiti di cybersecurity, inclusi quelli relativi all'accesso e alla condivisione di tutti i dati, nonché alla segnalazione di incidenti o violazioni entro un periodo specificato.
  - Requisiti per la notifica di una violazione che riguarda i dati dell'organizzazione principale.
  - Un processo standardizzato per verificare l'identità della terza parte, inclusi nome legale completo, indirizzo, sedi operative e sito web. Una prassi consolidata consiste nell'utilizzare una checklist durante il processo di identificazione e nel verificare l'accuratezza delle informazioni.
  - Livelli di servizio chiari, che specifichino i risultati attesi e i diritti, gli obblighi, le penalità, gli incentivi e le responsabilità di ciascuna parte, inclusa la responsabilità per il pagamento del costo del lavoro (compresi i subfornitori della filiera).

- Una clausola di diritto di Audit che includa tutti i subfornitori della filiera, oppure un requisito che preveda evidenza del fatto che le parti sono state sottoposte ad Audit da parte di un fornitore di servizi di assurance indipendente e affidabile. In assenza di una clausola di diritto di Audit, la capacità della funzione di Internal Audit di ottenere o fornire assurance può risultare limitata.

- L'organizzazione principale ha accesso ai report di valutazione del sistema di controllo redatti da Auditor indipendenti; ad esempio, quelli finanziari, di compliance e di sicurezza dei dati, come gli International Standard on Assurance Engagements o i report SOC.
  - Qualora si faccia affidamento sul lavoro di fornitori di servizi di assurance esterni della terza parte, la documentazione viene esaminata per verificarne l'affidabilità.
  - I report SOC vengono utilizzati per individuare processi di gestione del rischio e change management inadeguati.

- Le policy e le procedure riguardano tutti gli elementi essenziali per specifiche organizzazioni o tipologie contrattuali:
  - Clausole ambientali e di sostenibilità.
  - Protocolli per il whistleblowing.
  - Requisiti per la valutazione della performance.
  - Test dei business continuity plan delle terze parti.
  - Utilizzo dell'intelligenza artificiale nell'erogazione dei servizi.
  - L'identificazione dei termini e dell'ambito di qualsiasi attività subappaltata nella filiera.
  - Processi di change management, che definiscono come affrontare modifiche all'ambito, ai termini o ai requisiti operativi (come cambiamenti tecnologici o aggiornamenti normativi) durante la durata contrattuale.
  - Limiti al numero delle modifiche agli ordini o agli importi che possono essere fatturati.

- Le policy e le procedure richiedono l'accettazione formale dei prodotti finali prima che venga effettuato il pagamento o rilasciata qualsiasi cauzione.

- Le terze parti sono tenute a condividere le proprie policy etiche o il proprio codice di condotta e/o ad aderire a quelli dell'organizzazione principale.

- Qualora sia la terza parte a fornire il contratto, l'organizzazione principale effettua una revisione legale e i rischi principali sono analizzati e supportati da una strategia di mitigazione adeguata.

C. I contratti o gli accordi vengono rivisti e approvati dagli stakeholder competenti, incluse le funzioni legale e compliance, archiviati in modo sicuro e affidati alla responsabilità di un contract manager.

- Un contratto o altro documento ufficiale che attesti un rapporto di esternalizzazione e gli obblighi della terza parte, nonché l'evidenza di eventuali verifiche legali e di compliance richieste.

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

- Un processo per l'inserimento di nuovi contratti o accordi con terze parti nell'elenco o nel sistema.
- Un processo per l'inserimento di potenziali terze parti nel sistema dei fornitori e per la loro rimozione qualora il contratto non venga approvato.
- Un processo per la rimozione di contratti o accordi con terze parti dall'elenco o dal sistema.
- Un sistema di tracciamento per documentare problematiche relative a specifici fornitori, da utilizzare come riferimento futuro.
- Un processo di revisione volto a determinare se l'insieme delle terze parti sia accurato e completo.

E. Vengono stabiliti e seguiti processi di onboarding per consentire alle terze parti di rispettare i termini del contratto o dell'accordo. Le revisioni possono includere la verifica di quanto segue:

- Procedure di onboarding standardizzate che garantiscono che tutta la documentazione necessaria, il training e le compliance review siano completate.
- I sistemi e i processi della terza parte possono integrarsi perfettamente con la tecnologia dell'organizzazione principale.
- I sistemi condivisi sono compatibili e sicuri. Le evidenze possono includere controlli complementari delle utenze della società nell'ambito del reporting SOC.
- L'organizzazione principale valuta i piani di continuità operativa della terza parte, che devono garantire la continuità dei servizi durante le emergenze. Sono inclusi piani di contingenza per affrontare interruzioni potenziali.

F. Processi per il monitoraggio continuo delle performance dei fornitori rispetto agli obiettivi del contratto o dell'accordo, inclusa la valutazione dei key performance indicator.

- I processi di monitoraggio supportano la valutazione del rischio terze parti e le carenze di controllo identificate vengono esaminate, segnalate ai livelli superiori e indirizzate secondo necessità.
- Report o osservazioni dei processi, tecnologie e strumenti per il monitoraggio in tempo reale.
- Processi per garantire che i pagamenti siano effettuati in conformità ai termini del contratto o dell'accordo, ad esempio in relazione al rispetto delle tempistiche di progetto, delle milestone e dei requisiti di comunicazione. I pagamenti vengono effettuati solo a fornitori approvati che hanno completato la fase di onboarding e sono stati inseriti nel sistema di pagamento dei fornitori. Quando il contratto prevede deliverable specifici, i pagamenti vengono effettuati solo dopo che tali deliverable sono stati verificati.
- Monitoraggio per controllare i costi associati agli accordi con terze parti al fine di garantire valore e determinare il rientro dell'investimento. I risultati delle analisi costi-benefici vengono utilizzati per rinegoziare i contratti.

- Processi per valutare le penali in caso di mancato rispetto dei livelli di servizio previsti dal contratto o dall'accordo. Vengono calcolate e addebitate penali quando tali casi si verificano.
- La prioritizzazione delle terze parti in base al rischio viene rivalutata periodicamente, in caso di modifiche a un accordo e quando un contratto è prossimo alla scadenza o al rinnovo automatico.
- Verifiche delle terze parti rilevanti, come verifiche in loco o business review trimestrali, per validare i controlli e l'integrità operativa.
- Le evidenze di un ulteriore monitoraggio continuo possono includere:
  - Analisi della stabilità finanziaria della terza parte.
  - Valutazioni dei reclami contro terze parti.
  - Revisioni da parte del management dei report redatti da Auditor indipendenti, come l'International Standard on Assurance Engagements, gli Statements on Standards for Attestation Engagements, e dei report finanziari, di Audit, di compliance e sulla sicurezza dei dati forniti dalle terze parti e delle certificazioni ISO.
  - Verifiche da parte del management dei test di resilienza operativa condotti dalla terza parte, incluse eventuali criticità rilevanti individuate.
  - Condizioni e restrizioni relative all'utilizzo di subfornitori.
  - Valutazioni dei valori etici, della cultura e della condotta della terza parte.
  - Risposte alle inchieste dei media.
  - Valutazioni dei protocolli privacy e cybersecurity per proteggere l'archiviazione e il trasferimento dei dati e delle informazioni dell'organizzazione principale, incluso l'utilizzo di tecnologie avanzate come l'intelligenza artificiale.
  - Identificazione da parte dell'organizzazione di opportunità per il miglioramento continuo delle performance e il raggiungimento degli obiettivi del contratto o dell'accordo.
  - Verifica della segregation of duties.

**G.** Protocolli per l'avvio di azioni correttive in caso di incidenti, quando una terza parte non soddisfa i requisiti di un contratto o di un accordo, oppure quando le sue azioni aumentano il rischio per l'organizzazione principale.

- Protocolli per l'escalation degli incidenti in base alla gravità dell'evento e alla priorità attribuita alla terza parte.
- Verifiche post-incidente, inclusa l'analisi delle root cause.

**H.** Processi per fornire avvisi in merito a contratti e accordi prossimi alla scadenza o al rinnovo automatico. I processi di rinnovo automatico includono la revisione di:

- Performance della terza parte.
- Termini del contratto o dell'accordo e degli eventuali addendum.
- Fattori di rischio.

I. Viene implementato e seguito un piano di offboarding per garantire che i requisiti contrattuali relativi a tempistiche e aspettative siano adeguatamente indirizzati, inclusi quelli riguardanti ogni subfornitore della filiera.

- Checklist o interviste con i principali stakeholder per garantire l'efficacia delle misure di sicurezza.
- Restituzione o distruzione delle informazioni o dei dati dell'organizzazione in custodia presso una terza parte.
- Revoca dell'accesso della terza parte ai dati, ai sistemi o alle strutture dell'organizzazione.
- Restituzione degli asset dell'organizzazione principale, come dispositivi, licenze software, proprietà intellettuale e documenti.
- Quando il rapporto con una terza parte viene interrotto per giusta causa, le circostanze attenuanti o i rischi vengono identificati e inoltrati al Top Management e/o al Board.
- Quando il contratto di una terza parte rilevante viene risolto, la parte viene sostituita sulla base del medesimo risk assessment, salvo che il contratto sia stato completato o non sia più necessario.

# Appendice A. Esempi di applicazione pratica

I seguenti esempi illustrano scenari in cui il Requisito Tematico sulle Terze Parti è applicabile:

Esempio 1: Un incarico di Internal Audit incluso nel Piano di Audit comprende un servizio o un output attualmente fornito da una terza parte.

Quando la funzione di Internal Audit completa il proprio processo di pianificazione basato sul rischio e include uno o più incarichi nel Piano di Audit relativi a servizi o output attualmente forniti da terze parti in base a un contratto o accordo, il Requisito Tematico è obbligatorio.

È possibile che non tutti i requisiti del Requisito Tematico siano applicabili a ogni incarico. Quando gli Internal Auditor, sulla base del proprio giudizio professionale, stabiliscono che uno o più requisiti del Requisito Tematico sulle Terze Parti non sono applicabili e pertanto dovrebbero essere esclusi da un incarico, devono documentare e conservare la motivazione dell'esclusione di tali requisiti. Ad esempio, la motivazione per l'esclusione di alcuni requisiti potrebbe essere che la funzione di Internal Audit ha stabilito che il livello di dipendenza dell'organizzazione da terze parti per servizi essenziali è basso, oppure che si tratta di un rapporto consolidato con impatto finanziario limitato.

Esempio 2: I rischi legati a terze parti vengono identificati nel corso di un incarico di assurance relativo a una tematica diversa dalle terze parti o dalla gestione dei contratti.

Gli Internal Auditor possono identificare un rischio significativo legato a terze parti durante la valutazione di un processo inizialmente non considerato correlato alle terze parti o alla gestione dei contratti. Ad esempio, durante la pianificazione di un incarico per valutare l'archiviazione dei dati, gli Internal Auditor scoprono che i servizi cloud sono erogati da una terza parte. Durante i colloqui con il management dei servizi forniti dalla terza parte, gli Internal Auditor individuano rischi di cybersecurity legati alla terza parte.

Una volta individuati i rischi rilevanti, gli Internal Auditor devono esaminare il Requisito Tematico sulle Terze Parti e il Requisito Tematico sulla Cybersecurity e determinare quali requisiti siano applicabili. Gli auditor potrebbero escludere dall'ambito dell'incarico il processo di governance o di gestione del rischio terze parti e concentrarsi sui controlli delle terze parti relativi ai servizi oggetto dell'audit. Lo stesso giudizio professionale si utilizza nell'applicazione del Requisito Tematico sulla Cybersecurity. Gli auditor devono documentare nelle carte di lavoro dell'incarico la motivazione per l'esclusione di eventuali requisiti dei Requisiti Tematici sulle Terze Parti o sulla Cybersecurity e conservarne la documentazione a supporto.

Esempio 3: È richiesto un incarico relativo a una terza parte che non era originariamente incluso nel Piano di Audit.

All'interno dell'organizzazione sorge un problema che coinvolge una terza parte rilevante e che richiede l'immediata attenzione della funzione di Internal Audit. Il problema riguarda un malfunzionamento dei

controlli. Il Chief Audit Executive dovrebbe confrontarsi con il Board per ridefinire le priorità del Piano di Audit e delle risorse della funzione Internal Audit, al fine di far fronte all'esigenza. L'auditor dovrebbe interfacciarsi con il management interessato per sviluppare gli obiettivi dell'incarico al fine di valutare la situazione e formulare raccomandazioni per prevenire il ripetersi dell'evento. Il Chief Audit Executive dovrebbe esaminare il Requisito Tematico per definire il perimetro dell'incarico, determinare quali requisiti siano applicabili e documentare di conseguenza le eventuali esclusioni.

# Appendice B. Strumento 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 seconda del giudizio professionale 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 sulle Terze Parti, ma il suo utilizzo non è obbligatorio.

## Governance delle Terze Parti

| Requisito | Applicabilità del requisito o giustificazione per l'esclusione | Documentazione di riferimento |
|---|---|---|
| **A.** Viene stabilito, implementato e periodicamente rivisto un approccio formale per determinare se stipulare un contratto con una terza parte. L'approccio include criteri adeguati a 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 allineate ai requisiti normativi applicabili e vengono periodicamente riviste e aggiornate per rafforzare l'ambiente di controllo. | | |

| Requisito | Applicabilità del requisito o giustificazione per l'esclusione | Documentazione di riferimento |
|---|---|---|
| **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. Gli stakeholder rilevanti possono includere il Board, il Top Management, le funzioni Procurement, Operation, Risk management, Compliance, Legale, Information technology, Information security, Risorse umane e altre. | | |

## Gestione del Rischio Terze Parti

| Requisito | Applicabilità del requisito o giustificazione per l'esclusione | Documentazione di riferimento |
|---|---|---|
| **A.** I processi per la gestione del rischio terze parti sono standardizzati e completi, includono ruoli e responsabilità e indirizzano adeguatamente i rischi rilevanti per l'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. Il risk assessment viene utilizzato per classificare e prioritizzare tutte le terze parti della filiera, incluse quelle più a valle. Anche le risposte al rischio vengono classificate e prioritizzate. Il risk assessment viene periodicamente rivisto e aggiornato. | | |
| **C.** Le risposte al rischio sono adeguate e accurate, 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 sulle Terze Parti

| Requisito | Applicabilità del requisito o giustificazione per l'esclusione | Documentazione di riferimento |
|---|---|---|
| **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. | | |

| Requisito | Applicabilità del requisito o giustificazione per l'esclusione | Documentazione di riferimento |
|---|---|---|
| **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 delle performance periodicamente e in caso di 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 root cause 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:<br>• Interrompere il rapporto con la terza parte.<br>• Sostituire, se necessario, la terza parte.<br>• Riassegnare la custodia, restituire o distruggere i dati sensibili dell'organizzazione conservati presso la terza parte.<br>• 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 ulteriori informazioni, visitare theiia.org.

## Esclusione di responsabilità

L'IIA pubblica questo documento a scopo informativo ed educativo. Questo materiale non è destinato a fornire risposte definitive a circostanze individuali specifiche e, in quanto tale, deve essere utilizzato solo come guida. L'IIA raccomanda di rivolgersi a esperti indipendenti per consulenze relative a situazioni specifiche. L'IIA non si assume alcuna responsabilità per chi si affida esclusivamente a questo materiale.

## 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
Phone: +1-407-937-1111
Fax: +1-407-937-1101