Tredje part

Ämnesrelaterat krav

Topical Requirement

The Institute of
Internal Auditors

Ämnesrelaterade krav avseende tredjepartsrelationer

International Professional Practices Framework® består av globala internrevisionsstandarder (Global Guidance™), ämnesrelaterade krav och global vägledning. Ämnesrelaterade krav är obligatoriska och ska användas tillsammans med standarderna och utgör yrkesmässig praxis.

Ämnesrelaterade krav tillhandahåller tydlig vägledning för internrevisorer genom att etablera en miniminivå för revision av specifika riskområden. Organisationens riskprofil kan innebära att internrevisorer behöver beakta ytterligare aspekter.

Ämnesrelaterade krav kommer att öka likformigheten i hur internrevisionstjänster utförs samt förbättra kvaliteten och tillförlitligheten i genomförande och resultat. Ämnesrelaterade krav utvecklar internrevisionsyrket.

Internrevisorer ska tillämpa ämnesrelaterade krav i enlighet med de globala standarderna. Ämnesrelaterade krav är obligatoriska för säkringsuppdrag och rekommenderas för rådgivningsuppdrag. Ämnesrelaterade krav är tillämpliga när något av följande föreligger:

1. Området är en del av revisionsplanen.
2. Området är identifierat i samband med utförandet av ett uppdrag.
3. Uppdrag som inte ingår i den ursprungliga internrevisionsplanen.

Dokumentation av att varje krav i det ämnesrelaterade kravet har bedömts med avseende på tillämplighet ska upprättas och bevaras. Alla delar av ett ämnesrelaterat krav behöver inte vara tillämpliga i varje uppdrag; om delar av området utesluts ska detta motiveras, dokumenteras och bevaras. Följsamhet mot ämnesrelaterade krav kommer att utvärderas under kvalitetsutvärderingen.

Tredjepartsrelationer

Tredjepartsrelationer kan omfatta externa individer, grupper eller enheter med vilken organisationen etablerar en affärsförbindelse. Relationen kan formaliseras genom ett kontrakt, överenskommelse eller på annat sätt. I detta ämnesrelaterade krav används termen "tredjepartsrelation" för att hänvisa till återförsäljare, leverantörer, entreprenörer, underentreprenörer, outsourcade tjänsteleverantörer samt andra bolag och konsulter. Termen inbegriper avtal mellan en tredje part och dess underleverantörer.

Det ämnesrelaterade kravet gäller när internrevisionsfunktionen utför säkringsuppdrag avseende tredje part och/eller eventuella underleverantörer och dess underleverantörer, som medges enligt den tredje partens kontrakt med organisationen. Internrevisorer bör prioritera tredje partsrisker baserat på riskanalys enligt beskrivningen i avsnittet om riskhantering. Internrevisorer måste tillämpa alla krav som framgår av riskbedömningen. Undantag måste dokumenteras.

Detta krav är inte avsett att behandla indirekta externa relationer, intressen eller engagemang med organisationen, såsom tillsynsmyndigheter, ombud, styrelseledamöter, eller anställda.

©2025, The Institute of Internal Auditors, Inc. Alla rättigheter reserverade. Endast för enskilt bruk.

Begreppet "tredje part" kan definieras och användas på olika sätt beroende på bransch eller andra sammanhang. Internrevisorer har flexibilitet och bör förlita sig på sin professionella bedömning för att anpassa det ämnesrelaterade kravet till organisationens definition av tredje part.

Den organisation som ingår ett avtal med tredje part behåller ansvaret för de risker som är förknippade med att uppnå mål, även när tredje part anlitas för att hjälpa organisationen att uppnå ett eller flera mål. Att arbeta med tredje part medför risker som måste identifieras, bedömas och hanteras genom lämpliga processer för ledning, riskhantering samt intern styrning och kontroll, enligt vad som beskrivs i detta ämnesrelaterade krav. Om en tredje part inte uppfyller sina åtaganden enligt avtal, deltar i oetiska handlingar eller drabbas av avbrott i verksamheten kan det få negativa konsekvenser på organisationen. Kategorier och exempel på risker relaterade till tredje part kan vara:

- Strategiska, t.ex. förmågan att fullfölja organisationens uppdrag och/eller mål på hög nivå eller att hantera effekterna av fusioner och förvärv.
- Anseende, t.ex. skador på miljön eller på organisationens relation till och förtroende hos kunder, klienter och andra intressenter.
- Etiska, till exempel bristande integritet, intressekonflikter, mutor och korruption.
- Operativa, till exempel fysisk säkerhet och informationssäkerhet, insiderrisker, avbrott i tjänster och att mål inte uppnås.
- Finansiella, till exempel insolvens hos tredje part och bedrägeri.
- Efterlevnad av tillämpliga nationella och internationella regelverk.
- Cybersäkerhet och annat dataskydd, t.ex. att känsliga uppgifter äventyras eller läcker ut.
- Informationsteknik, t.ex. avsaknad av stöd till kritiska processer.
- Juridiska, t.ex. intressekonflikter, tvister och rättstvister vid avtalsbrott.
- Hållbarhet, till exempel ESG frågor. Exempel på detta är risker relaterade till organisationens påverkan på miljön och risker relaterade till dess interaktion med samhället.
- Geopolitiska, t.ex. handelstvister/sanktioner och politisk instabilitet.

Livscykeln för en tredje part består av val, avtal, implementering, monitorering och avveckling. Internrevisorer bör beakta dessa faser när krav på styrning och ledning, riskhantering samt styrnings- och kontrollprocesser bedöms.

©2025, The Institute of Internal Auditors, Inc. Alla rättigheter reserverade. Endast för enskilt bruk.

Utvärdering och bedömning av tredjepartsstyrning, riskhantering och kontrollprocesser

Detta ämnesrelaterade krav ger ett konsekvent tillvägagångssätt för att bedöma utformning och genomförande av tredje parts processer för styrning, riskhantering och kontroll. Kraven utgör en miniminivå för utvärderingen.

STYRNING OCH LEDNING

Krav:

Internrevisorer måste bedöma följande aspekter av organisationens styrning av tredje part, inklusive styrelsens tillsyn:

- **A.** Ett formellt tillvägagångssätt inför att ingå avtal med tredje part är fastställt, implementerat och regelbundet granskat. Tillvägagångssättet omfattar lämpliga kriterier för att definiera och bedöma om tredje part har de resurser som är nödvändiga och tillgängliga för att uppfylla målen.
- **B.** Policyer och rutiner upprättas för att definiera, bedöma och hantera relationer och risker med tredje part under avtalsperioden. Policyerna och rutinerna är anpassade till tillämpliga lagkrav och granskas och uppdateras regelbundet för att stärka kontrollmiljön.
- **C.** Organisationens roller och ansvar för hantering av tredje part är definierade och anger vem som väljer ut, leder, hanterar, kommunicerar med och monitorerar tredje part samt vem som måste informeras om tredje parts aktiviteter. Det finns en process för att säkerställa att personer som tilldelas tredjepartsroller och -ansvar har rätt kompetens.
- **D.** Plan för kommunikation med relevanta intressenter har upprättats och omfattar snabb rapportering om status för prioriterade tredje parters resultat, risker och efterlevnad (särskilt överträdelser av lagar och förordningar). Tredjepartsrelationer är ett prioriterat område utifrån ett riskperspektiv. Relevanta intressenter kan vara styrelsen, högsta ledningen samt enheter för upphandling, drift, riskhantering, regelverksefterlevnad, juridik, IT, informationssäkerhet, HR och andra.

Riskhantering

Krav:

Internrevisorer måste bedöma följande aspekter av organisationens hantering av tredjepartsrisker.

- **A.** Processerna för riskhantering av tredje part och deras tjänster omfattar roller och ansvarsområden och hanterar de viktigaste riskerna som är relevanta för organisationen (t.ex. strategiska, ryktesrelaterade, etiska, operativa, finansiella, regelefterlevnad, cybersäkerhet, IT, legala, hållbarhetsrelaterade och geopolitiska). Följsamheten till processerna monitoreras och åtgärder vidtas vid eventuella avvikelser.
- **B.** Risker och riskhanteringen relaterade till tredje part identifieras, bedöms, rangordnas och prioriteras regelbundet under hela livscykeln. Riskbedömningen ska även inkluderaunderleverantörer. Åtgärderna ska även rankas och prioriteras. Riskbedömningen granskas och uppdateras regelbundet.,

©2025, The Institute of Internal Auditors, Inc. Alla rättigheter reserverade. Endast för enskilt bruk.

C. Åtgärderna ska vara adekvata och korrekta och stå i proportion till gjord rangordning. Riskhanteringsåtgärderna implementeras, granskas, godkänns, monitoreras , utvärderas och justeras vid behov.

D. Processer finns på plats för att hantera och vid behov eskalera frågor som rör tredje part, för att öka sannolikheten att villkoren i kontrakt eller andra överenskommelser uppfylls. Om en tredje part inte vidtar åtgärder finns processer på plats för att utvärdera riskerna med den pågående affärsrelationen och vidta ytterligare åtgärder som ytterst kan leda till uppsägning.

STYRNING OCH KONTROLL

Krav:

Internrevisorer måste bedöma följande kontroller för de tredjepartsrelationer som prioriterats efter gjord riskbedömning. Utvärderingen ska omfatta ledningens processer för löpande bedömning och uppföljning av organisationens tredjepartsrelationer.

A. En robust due diligence-process finns på plats för val av tredje part med en dokumenterad och godkänd affärsplan eller annat relevant dokument som beskriver och motiverar behovet av och karaktären på relationen med tredje part.

B. Kontrakt upprättas och godkännande sker i enlighet med organisationens policyer och rutiner för hantering av tredjepartsrisker och inkluderar samarbete med relevanta delar av organisationen.

C. Slutgiltiga kontrakt granskas och godkänns av alla relevanta intressenter, inklusive legala frågor och regelefterlevnad, undertecknas av behöriga personer från båda parter och arkiveras på ett säkert sätt. En avtalsansvarig eller administratör tilldelas ansvaret för varje avtal.

D. En korrekt, fullständig och aktuell förteckning över alla relationer med tredje part upprätthålls, t.ex. i ett centraliserat system för avtalshantering.

E. Dokumenterade processer för implementering etableras och följs upp för att säkerställa att villkoren i kontraktet uppfylls.

F. Löpande monitorering sker för att bedöma om tredje part agerar i enlighet med villkoren i kontraktet och uppfyller sina kontraktsenliga skyldigheter under hela livscykeln. Processerna innefattar att verifiera tillförlitligheten i den information som tillhandahålls och att utvärdera prestationerna regelbundet samt när ändringar sker av avtalet.

G. Protokoll upprättas för att initiera lämpliga åtgärder om en tredje part inte uppfyller förväntningarna eller utgör en ökad eller oväntad risk. Protokollen omfattar eskalering av incidenter baserat på allvarlighetsgrad, uppföljning efter en incident och analys av grundorsaken till incidenten.

H. Datum för när avtal löper ut och förnyas övervakas och förnyelseåtgärder vidtas vid behov.

I. En formaliserad avvecklingsplan implementeras och följs för att säkerställa att avtalskrav som rör tidpunkter och förväntningar uppfylls på ett adekvat sätt. Processerna inkluderar hur man:

- Avslutar relationen med tredje part.
- Ersätter tredje parten om det behövs.
- Omfördelar ägandet och återlämnandet eller förstörandet av organisationens känsliga data som lagras hos tredje part.
- Återkalla tredje partens tillgång till system, verktyg, lokaler och anläggningar.

©2025, The Institute of Internal Auditors, Inc. Alla rättigheter reserverade. Endast för enskilt bruk.

Om Institutet för internrevisorer

IIA är en internationell yrkesorganisation som har mer än 265.000 medlemmar globalt och har utfärdat mer än 200.000 certifieringar av Certified Internal Auditor® (CIA®) över hela världen. IIA grundades 1941 och är erkänt över hela världen som internrevisionsbranschens ledande aktör inom standarder, certifieringar, utbildning, forskning och teknisk vägledning. För mer information, besök theiia.org.

Upphovsrätt

© 2025 The Institute of Internal Auditors, Inc. Alla rättigheter förbehållna. För tillstånd att återge, vänligen kontakta copyright@theiia.org.

September 2025

The Institute of Internal Auditors

Globalt huvudkontor
The Institute of Internal Auditors
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746, USA
Telefon: +1-407-937-1111
Fax: +1-407-937-1101

©2025, The Institute of Internal Auditors, Inc. Alla rättigheter reserverade. Endast för enskilt bruk.