

Treća strana

Tematski zahtjev

Topical Requirement



The Institute of
Internal Auditors

Tematski zahtjev treća strana

Međunarodni okvir profesionalnog djelovanja® (International Professional Practices Framework®) obuhvaća Globalne standarde interne revizije™ (Global Internal Audit Standards™), Tematske zahtjeve i Globalne smjernice. Tematski zahtjevi su obvezni i moraju se primjenjivati zajedno sa Standardima, koji pružaju mjerodavnu osnovu za propisane prakse.

Tematski zahtjevi pružaju jasna očekivanja internim revizorima postavljanjem minimalne osnove za reviziju određenih područja rizika. Profil rizika organizacije može zahtijevati od internih revizora da razmotre dodatne aspekte treće strane.

Usklađenost s Tematskim zahtjevima pridonijet će većoj dosljednosti u pružanju usluga interne revizije te unaprijediti kvalitetu i pouzdanost usluga i rezultata interne revizije. U konačnici, Tematski zahtjevi podižu profesiju interne revizije na viši nivo.

Interni revizori moraju primjenjivati Tematske zahtjeve u skladu s Globalnim standardima interne revizije. Usklađenost s Tematskim zahtjevima obvezna je za usluge izražavanja uvjerenja, te se preporučuje se za savjetodavne usluge. Tematski zahtjev primjenjuje se kada je treća strana:

1. Predmet angažmana u planu interne revizije.
2. Identificirana tijekom obavljanja angažmana.
3. Predmet zatraženog angažmana koji nije bio u izvornom planu interne revizije.

Moraju se dokumentirati i sačuvati dokazi, koji ukazuju na to da je svaki zahtjev u Tematskom zahtjevu procijenjen po pitanju primjenjivosti. Ne moraju se svi pojedinačni zahtjevi primjenjivati u svakom angažmanu; no ako su neki od zahtjeva isključeni, obrazloženje za isključenje se mora dokumentirati. Usklađenost s Tematskim zahtjevom je obvezna i bit će ocijenjena tijekom procjene osiguranja kvalitete.

Treće strane

Treća strana je vanjska osoba, skupina ili entitet s kojim organizacija („primarna organizacija“) uspostavlja poslovni odnos radi pribavljanja proizvoda ili usluga. Odnos se može formalizirati ugovorom, sporazumom ili na druge načine. Ovaj Tematski zahtjev koristi pojam „treća strana“ za dobavljače, izvođače radova, podizvođače, vanjske pružatelje usluga, druge agencije i konzultante. Pojam uključuje sporazume između treće strane i njezinih podizvođača, često poznatih kao „nizvodni“ podizvođači.

Tematski zahtjev primjenjuje se kada funkcija interne revizije provodi angažmane s izražavanjem uvjerenja za treće strane i/ili za bilo koje podugovorene odnose, uključujući



četvrte ili dalje „nizvodne“ strane, dopuštene ugovorom ili sporazumom treće strane s primarnom organizacijom. Interni revizori trebaju odrediti prioritete trećih strana i daljnjih „nizvodnih“ strana na temelju rizika, kako je opisano u odjeljku o upravljanju rizicima u nastavku. Interni revizori moraju primjenjivati sve zahtjeve kako je naznačeno rezultatima procjene rizika, a izuzeća moraju biti dokumentirana.

Ovaj tematski zahtjev nije namijenjen obuhvaćanju slijedećih neizravnih vanjskih odnosa, interesa ili suradnje s primarnom organizacijom, kao što su odnosi regulatora, agenata ili zastupnika/članova odbora, te odnose unutar organizacije, kao što su odnosi sa zaposlenicima.

Pojam „treća strana“ može se definirati i koristiti različito ovisno o industriji ili drugim kontekstima. Internim revizorima se daje fleksibilnost i trebali bi se osloniti na svoju profesionalnu prosudbu kako bi Tematski zahtjev prilagodili definiciji treće strane koju koristi primarna organizacija.

Primarna organizacija (organizacija koja sklapa ugovor s trećom stranom) zadržava odgovornost za rizike povezane s postizanjem svojih ciljeva, čak i kada angažira treću stranu kako bi joj pomogla u postizanju jednog ili više ciljeva. Suradnja s trećim stranama uvodi rizike koji se moraju identificirati, procijeniti i njima upravljati putem odgovarajućih procesa upravljanja, upravljanja rizicima i kontrolnim procesima, kako je navedeno u ovom Tematskom zahtjevu. Ako treća strana ne izvrši ugovorene obveze, sudjeluje u neetičkim praksama ili doživi poremećaj u poslovanju, primarna organizacija može snositi posljedice. Kategorije i primjeri rizika povezanih s trećim stranama uključuju:

- Strateški rizici, poput sposobnosti ostvarivanja primarne misije i/ili ciljeva visoke razine primarne organizacije ili upravljanja utjecajima spajanja i akvizicija na organizaciju.
- Reputacijski rizici, primjerice šteta nanosena okolišu ili narušavanje odnosa i povjerenja primarne organizacije s klijentima, kupcima i dionicima.
- Etički rizici, kao što su propusti u integritetu, sukobi interesa, mito i korupcija.
- Operativni rizici, kao što su fizička i informacijska sigurnost, rizici od internih prijetnji, poremećaji u uslugama i neostvarivanje ciljeva.
- Financijski rizici, kao što su nesolventnost treće strane i prijevara.
- Usklađenost s primjenjivim lokalnim, nacionalnim i međunarodnim regulatornim zahtjevima.
- Kibernetička sigurnost i ostale vrste zaštite podataka, poput kompromitiranja i curenja osjetljivih podataka.
- Informacijska tehnologija, kao što je nedostatak usluga potrebnih za podršku kritičnim operacijama.
- Pravni rizici, kao što su sukobi interesa, sporovi i sudski postupci zbog kršenja ugovornih obveza.

- Rizici održivosti, uključujući okolišne, društvene i upravljačke aspekte (ESG).
Primjeri uključuju rizike povezane s utjecajem organizacije na prirodni okoliš i rizike koji se odnose na interakcije organizacije sa zajednicama.
- Geopolitički rizici, poput trgovinskih sporova/sankcija i političke nestabilnosti.

Životni ciklus treće strane sastoji se od faze odabira, ugovaranja, uključivanja, praćenja i završetka suradnje. Interni revizori trebaju uzeti u obzir ove faze prilikom procjene zahtjeva za procese upravljanja, upravljanja rizicima i kontrolne procese..



Evaluacija i procjena procesa upravljanja, upravljanja rizicima i kontrolnih proces trećih strana

Ovaj Tematski zahtjev pruža dosljedan, sveobuhvatan pristup procjeni dizajna i provedbe procesa upravljanja, upravljanja rizicima i kontrolnih procesa trećih strana. Zahtjevi predstavljaju minimalnu osnovu za procjenu.

KORPORATIVNO UPRAVLJANJE

Zahtjevi:

Interni revizori moraju procijeniti sljedeće aspekte upravljanja trećim stranama u primarnoj organizaciji, uključujući nadzor odbora:

- A. Uspostavlja se, provodi i periodično preispituje formalan pristup kako bi se utvrdilo treba li sklopiti ugovor s trećom stranom. Pristup uključuje odgovarajuće kriterije za definiranje i procjenu resursa potrebnih i dostupnih za postizanje ciljeva pružanjem proizvoda ili usluge.
- B. Uspostavljene su politike i postupci za definiranje, procjenu i upravljanje odnosima i rizicima s trećim stranama tijekom cijelog njihova životnog ciklusa treće strane. Politike i postupci su usklađeni s primjenjivim regulatornim zahtjevima te se periodički pregledavaju i ažuriraju radi jačanja kontrolnog okruženja.
- C. Uloge i odgovornosti upravljanja trećim stranama u organizaciji su definirane, s detaljnim opisom tko odabire, usmjerava, upravlja, komunicira s i nadzire treće strane te tko mora biti obaviješten o aktivnostima trećih strana. Uspostavljen je proces kojim se osigurava da pojedinci kojima su dodijeljene uloge i odgovornosti upravljanja trećim stranama, imaju odgovarajuće kompetencije.
- D. Definirani su protokoli za komunikaciju s relevantnim dionicima koji uključuju pravovremeno izvještavanje o statusu učinka, rizika i usklađenosti (posebno kršenja zakona i propisa) prioritetnih trećih strana. Treće strane imaju prioritet na temelju rizika. Relevantne dionike mogu činiti upravni odbor, viši menadžment, nabavu, operacije, upravljanje rizicima, usklađenost, pravni odjel, informacijsku tehnologiju, informacijsku sigurnost, ljudske resurse i druge.

UPRAVLJANJE RIZICIMA

Zahtjevi:

Interni revizori moraju procijeniti sljedeće aspekte upravljanja rizicima trećih strana u organizaciji.

- A. Proces upravljanja rizicima trećih strana i njihovih usluga su standardizirani i sveobuhvatni, uključuju definirane uloge i odgovornosti te se u dovoljnoj mjeri bave ključnim rizicima relevantnim za organizaciju (kao što su strateški,



reputacijski, etički, operativni, financijski, rizici usklađenosti, kibernetičke sigurnosti, informacijske tehnologije, pravni, održivosti i geopolitički rizici). Pridržavanje procesa se nadzire, a korektivne mjere se provode za sva odstupanja.

- B. Rizici povezani s trećim stranama tijekom cijelog životnog ciklusa redovito se identificiraju i procjenjuju. Procjena rizika koristi se za rangiranje i određivanje prioriteta trećih strana, uključujući i one dalje „nizvodno“. Odgovori na rizike se također rangiraju i određuju im se prioriteti. Procjena rizika se periodički pregledava i ažurira.
- C. Odgovori na rizike su adekvatni i točni, u skladu s njihovim rangiranjem. Odgovori na rizike se provode, pregledavaju, odobravaju, nadgledaju, evaluiraju i prilagođavaju prema potrebi.
- D. Postoje procesi za upravljanje i, ako je potrebno, eskalaciju problema koji proizlaze iz odnosa s trećim stranama, čime se osigurava odgovornost za ishode i povećava vjerojatnost postizanja uvjeta ugovora ili drugih sporazuma. Ako treća strana ne odgovori na eskalirane zabrinutosti, uspostavljeni su procesi pomoću kojih menadžment može procijeniti rizike svog tekućeg poslovnog odnosa i poduzeti daljnje mjere, sanaciju ili raskid suradnje prema potrebi.

KONTROLNI PROCESI

Zahtjevi:

Interni revizori moraju procijeniti sljedeće kontrole za treće strane, prioritizirane prema riziku. Evaluacija mora uključivati procese menadžmenta za kontinuiranu procjenu i nadzor trećih strana organizacije.

- A. Uspostavljen je robustan proces dubinske analize za pronalaženje i odabir trećih strana s dokumentiranim i odobrenim poslovnim planom ili drugim relevantnim dokumentom koji opisuje i opravdava potrebu za i prirodu odnosa s trećom stranom.
- B. Ugovaranje i odobravanje provode se u skladu s politikama i postupcima upravljanja rizicima trećih strana organizacije i uključuju suradnju među odgovarajućim dijelovima organizacije.
- C. Konačne ugovore ili sporazume pregledavaju i odobravaju sve relevantne zainteresirane strane, uključujući pravni odjel i odjel za usklađenost, potpisuju ih ovlaštene osobe obje strane i sigurno se pohranjuju. Za svaki ugovor imenuje se voditelj ugovora ili administrator kao odgovorna osoba.
- D. Održava se točan, potpun i ažuran popis svih odnosa s trećim stranama, primjerice u centraliziranom sustavu za upravljanje ugovorima.
- E. Uspostavljaju se i provode dokumentirani procesi uvođenja u posao (eng. onboarding), kako bi se stvorila osnova za to da treće strane ispune uvjete ugovora ili sporazuma.



- F. Postoje procesi kontinuiranog praćenja kako bi se procijenilo postupaju li treće strane u skladu s uvjetima ugovora ili sporazuma tijekom cijelog životnog ciklusa i ispunjavaju li treće strane svoje ugovorne obveze. Proces uključuje provjeru pouzdanosti pruženih informacija i periodičnu ponovnu procjenu učinka i kad god se ugovor promijeni.
- G. Uspostavljani su protokoli za pokretanje korektivnih radnji ako treća strana ne ispunji očekivanja ili predstavlja povećani ili neočekivani rizik. Protokoli uključuju eskalaciju incidenata prema ozbiljnosti, provođenje pregleda nakon incidenta i analizu temeljnog uzroka incidenata.
- H. Prate se datumi isteka i obnove ugovora te se po potrebi poduzimaju mjere obnove.
- I. Provodi se i slijedi formalizirani plan okončanja suradnje (eng. *offboarding*) kako bi se osiguralo da se ugovorni zahtjevi koji se odnose na rokove i očekivanja adekvatno ispune. Proces uključuje sljedeće:
- Raskinuti suradnju s trećom stranom.
 - Zamijenite treću stranu po potrebi.
 - Ponovno dodijeliti skrbništvo nad podacima i vratiti ili uništiti osjetljive podatke organizacije pohranjene kod treće strane.
 - Poništiti pristup treće strane sustavima, alatima i objektima.

O Institutu internih revizora

IIA je međunarodno profesionalno udruženje koje okuplja više od 265.000 članova diljem svijeta i dodijelilo je više od 200.000 certifikata Certified Internal Auditor® (CIA®) diljem svijeta. Osnovan 1941. godine, IIA je diljem svijeta prepoznat kao vodeća institucija u struci interne revizije u standardima, certifikatima, obrazovanju, istraživanju i tehničkom vodstvu. Za više informacija posjetite theiia.org.

Autorska prava

© 2025 The Institute of Internal Auditors, Inc. Sva prava pridržana. Za dopuštenje reprodukcije obratite se na copyright@theiia.org.

Rujan 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

