

Třetí strany

Tematické požadavky

Topical Requirement



The Institute of
Internal Auditors

Tematické požadavky na třetí strany

Mezinárodní rámec profesní praxe (International Professional Practices Framework®) se skládá z Globálních standardů interního auditu™ (Global Internal Audit Standards™), Tematických požadavků a Globálních návodů. Tematické požadavky jsou závazné a musí se využívat společně se Standardy, které představují požadovaný základ pro praxi.

Tematické požadavky stanovují minimální základ pro audit určitých oblastí rizik a poskytují tak interním auditorům jasná očekávání. Rizikový profil organizace může vyžadovat, aby interní auditoři zvažili další aspekty dané oblasti.

Soulad s Tematickými požadavky zvýší konzistentnost při poskytování služeb interního auditu alepší kvalitu a spolehlivost služeb a výsledků interního auditu. Tematické požadavky v konečném důsledku podvívají profesi interního auditu.

Interní auditoři musí uplatňovat Tematické požadavky v souladu s Globálními standardy interního auditu. Dodržování Tematických požadavků je povinné pro ujišťovací služby a doporučené pro poradenské služby. Tematické požadavky se uplatní, pokud je dané téma:

1. Předmětem zakázky v plánu interního auditu.
2. Identifikováno při provádění zakázky.
3. Předmětem žádosti o zakázku, která nebyla v původním plánu interního auditu.

Každý jednotlivý požadavek v Tematických požadavcích musí být posouzen z hlediska jeho uplatnitelnosti a musí o tom být vypracována a uchována evidence. Ne všechny požadavky se musí uplatnit v každé zakázce; pokud jsou ale některé požadavky vynechány, musí být zdokumentováno a uchováno odůvodnění. Soulad s Tematickými požadavky je povinný a bude hodnocen při hodnocení kvality.

Třetí strany

Třetí strana je externí osoba, skupina nebo subjekt, se kterým organizace ("primární organizace") naváže obchodní vztah za účelem získání produktů nebo služeb. Vztah může být formálně ustanoven smlouvou, dohodou nebo jiným způsobem. Tyto Tematické požadavky používají termín "třetí strana" pro prodejce, dodavatele, zhotovitele, subdodavatele, externí poskytovatele služeb, jiné zprostředkovatele a konzultanty. Tento pojem zahrnuje dohody mezi třetí stranou a jejími subdodavateli, často známými jako "následní" subdodavatelé.

Tematické požadavky se uplatní, pokud útvar interního auditu provádí ujišťovací zakázky u třetích stran a/nebo jakýchkoli subdodavatelských vztahů, včetně těch čtvrtých nebo dále navazujících, které umožňuje smlouva nebo dohoda primární organizace se třetí stranou. Interní auditoři by měli stanovovat priority třetích a dalších navazujících stran na základě rizik, jak je popsáno v části o řízení rizik níže. Interní auditoři musí zohlednit všechny požadavky, které vyplývají z výsledků hodnocení rizik, a výjimky musí být zdokumentovány.



Tyto Tematické požadavky se netýkají nepřímých externích vztahů a zájmových nebo angažovaných stran primární organizace, jako jsou regulační orgány, zástupci, správci/členové představenstva, ani interních vztahů, jako jsou zaměstnanci.

Pojem "třetí strana" může být definován a používán různě v závislosti na odvětví nebo jiných souvislostech. Interním auditorům je ponechána flexibilita a měli by se spoléhat na svůj odborný úsudek při přizpůsobování Tematických požadavků definici třetí strany v primární organizaci.

Primární organizace (organizace uzavírající dohodu s třetí stranou) zůstává plně zodpovědná za rizika spojená s dosahováním svých cílů, i když zapojí třetí stranu, aby jí jednoho nebo více cílů pomohla dosáhnout. Spolupráce s třetími stranami přináší rizika, která je třeba identifikovat, posoudit a řídit prostřednictvím vhodných procesů řízení a správy společnosti, řízení rizik a řídicích a kontrolních mechanismů, jak je uvedeno v tomto tematickém požadavku. Pokud třetí strana neplní smluvní ujednání, podílí se na neetických praktikách nebo u ní dojde k narušení provozu, může to mít pro primární organizaci následky. Kategorie a příklady rizik souvisejících s třetími stranami zahrnují:

- Strategická rizika, jako je schopnost plnit poslání primární organizace a/nebo její nejvyšší cíle nebo řídit dopady fúzí a akvizic.
- Reputační rizika, jako jsou škody způsobené na životním prostředí nebo na vztazích primární organizace a důvěře klientů, zákazníků a zainteresovaných subjektů.
- Etická rizika, jako jsou ztráta integrity, střety zájmů, úplatky a korupce.
- Provozní rizika, jako je fyzická a informační bezpečnost, riziko spojené s interními pracovníky, narušení provozu a nedosažení cílů.
- Finanční rizika, jako je platební neschopnost třetích stran a podvody.
- Compliance, dodržování platných místních, národních a mezinárodních regulačních požadavků.
- Kybernetickou bezpečnost a další ochranu dat, například ohrožení a únik citlivých údajů.
- Informační technologie, například nedostatek služeb zajišťujících stabilitu kritických operací.
- Právní otázky, jako jsou střety zájmů, rozepře a soudní spory v případě porušení smlouvy.
- Udržitelnost, například v oblasti ESG (životního prostředí, sociální a řízení a správy společnosti). Příkladem jsou rizika související s dopadem organizace na životní prostředí a rizika týkající se interakcí organizace s komunitami.
- Geopolitická rizika, jako jsou obchodní spory/sankce a politická nestabilita.

Cyklus spolupráce se třetí stranou se skládá z výběru, uzavření smlouvy, zahájení spolupráce, monitorování a ukončení spolupráce. Interní auditoři by měli tyto fáze zohlednit při posuzování požadavků na řízení a správu společnosti, řízení rizik a řídicích a kontrolních procesy.

Hodnocení a posuzování procesů řízení a správy společnosti, řízení rizik a řídicích a kontrolních procesů u třetích stran

Tyto tematické požadavky poskytují konzistentní a komplexní přístup k hodnocení, jak má třetí strana navržený a implementovaný procesy řízení a správy společnosti, řízení rizik a řídicí a kontrolní procesy. Požadavky představují minimální základ pro posouzení.

ŘÍZENÍ A SPRÁVA

Požadavky:

Interní auditoři musí posoudit řízení a správu třetích stran v primární organizaci, včetně dohledu orgánů společnosti, a to z hlediska následujících aspektů:

- A.** Je stanoven, zaveden a pravidelně přezkoumáván formální postup k rozhodnutí, zda uzavřít smlouvu s třetí stranou. Tento postup zahrnuje odpovídající kritéria pro určení a posouzení zdrojů, které jsou nezbytné a dostupné pro splnění cílů spojených s poskytováním produktu nebo služby.
- B.** Jsou zavedeny zásady a postupy pro definování, hodnocení a řízení vztahů a rizik třetích stran v průběhu celého cyklu spolupráce se třetí stranou. Zásady a postupy jsou v souladu s platnými regulačními požadavky a jsou pravidelně revidovány a aktualizovány s cílem posílit kontrolní prostředí.
- C.** Jsou definovány role a odpovědnosti v organizaci při řízení třetích stran, přičemž je podrobně uvedeno, kdo vybírá, řídí, spravuje, komunikuje a monitoruje třetí strany a kdo musí být informován o činnostech třetích stran. Existuje proces, který zajišťuje, že osoby, kterým jsou přiděleny role a odpovědnosti vůči třetím stranám, mají odpovídající kompetence.
- D.** Jsou stanoveny protokoly pro komunikaci s příslušnými zainteresovanými subjekty, které zahrnují včasné podávání zpráv o stavu výkonnosti, rizik a compliance (zejména porušení zákonů a nařízení) prioritních třetích stran. Třetím stranám je stanovena priorita podle míry rizika. Mezi příslušné zainteresované subjekty mohou patřit orgány společnosti, vrcholové vedení, nákupní oddělení, provozní oddělení, řízení rizik, compliance, právní oddělení, informační technologie, informační bezpečnost, lidské zdroje a další.

ŘÍZENÍ RIZIK

Požadavky:

Interní auditoři musí posoudit řízení rizik třetích stran v primární organizaci, a to z hlediska následujících aspektů:

- A.** Procesy řízení rizik třetích stran a jejich služeb jsou standardizované a komplexní, zahrnují definované role a odpovědnosti a dostatečně řeší klíčová rizika relevantní pro organizaci (například strategická, reputační, etická, provozní, finanční, compliance, kybernetickou bezpečnost, informační technologie, právní oblast, udržitelnost a geopolitická rizika). Dodržování procesů je sledováno a v případě odchylek jsou prováděna nápravná opatření.
- B.** Rizika spojená s třetími stranami v průběhu celého cyklu spolupráce jsou pravidelně identifikována a vyhodnocována. Posouzení rizik se využívá ke stanovení kategorie a priority



třetích stran, včetně těch následných. Jsou stanoveny také kategorie a priority reakcí na rizika. Hodnocení rizik se pravidelně přezkoumává a aktualizuje.

- C. Reakce na rizika jsou přiměřené a přesné a odpovídají kategorizaci. Reakce na rizika jsou implementovány, přezkoumávány, schvalovány, monitorovány, vyhodnocovány a upravovány podle potřeby.
- D. Jsou zavedeny procesy pro řízení a případnou eskalaci problémů, které vzniknou u třetích stran, aby byla zajištěna výsledná odpovědnost a pravděpodobnost dodržení podmínek smluv nebo jiných dohod. Pokud třetí strana nereaguje na eskalované obavy, jsou zavedeny postupy, které umožňují vedení vyhodnotit rizika probíhajícího obchodního vztahu a v případě potřeby podniknout další kroky, zjednat nápravu nebo ukončit spolupráci.

ŘÍDICÍ A KONTROLNÍ MECHANISMY

Požadavky:

Interní auditoři musí posoudit následující kontrolní mechanismy třetích stran, které mají prioritu podle míry rizika. Hodnocení musí zahrnovat procesy pro průběžné hodnocení a monitorování třetích stran organizace vedením.

- A. Je zaveden důkladný proces hloubkové kontroly pro získávání a výběr třetích stran, který zahrnuje dokumentaci a schválení obchodních případů nebo jinou relevantní dokumentaci popisující a odůvodňující potřebu navázání vztahu se třetí stranu a povahu tohoto vztahu.
- B. Uzavírání a schvalování smluv probíhá v souladu se zásadami a postupy organizace pro řízení rizik třetích stran a zahrnuje spolupráci mezi příslušnými složkami organizace.
- C. Konečné smlouvy nebo dohody jsou zkontrolovány a schváleny všemi příslušnými zainteresovanými subjekty, včetně právního oddělení a compliance, jsou podepsány oprávněnými osobami obou stran a bezpečně uloženy. Pro každou smlouvu je stanovený odpovědný manažer nebo vykonavatel.
- D. Je veden přesný, úplný a aktuální seznam všech vztahů s třetími stranami, například v centralizovaném systému správy smluv.
- E. Jsou zavedeny a dodržovány zdokumentované postupy pro navázání spolupráce, aby byly pro třetí strany vytvořeny podmínky pro splnění závazků smlouvy nebo dohody.
- F. Existují průběžné monitorovací procesy, jejichž cílem je posoudit, zda třetí strany jednají v souladu s podmínkami smlouvy nebo dohody v průběhu celého cyklu spolupráce a zda třetí strany plní své smluvní závazky. Tyto procesy zahrnují ověřování spolehlivosti poskytovaných informací a přehodnocování výkonu pravidelně a také pokaždé, když dojde ke změně dohody.
- G. Jsou zavedeny protokoly pro zahájení nápravných opatření, pokud třetí strana nesplní očekávání nebo představuje zvýšené či neočekávané riziko. Protokoly zahrnují eskalaci incidentů podle závažnosti, provádění přezkumů po incidentu a analýzu kořenových příčin incidentů.
- H. Jsou sledována data vypršení platnosti smluv a jejich prodloužení a případně se podnikají potřebné kroky k prodloužení.



- I. Je zaveden a dodržován formalizovaný plán ukončení spolupráce, aby bylo zajištěno, že jsou náležitě zohledněny smluvní požadavky týkající se načasování a očekávání. Procesy zahrnují:
- Ukončení činnosti třetí strany.
 - V případě potřeby nahrazení třetí strany jinou.
 - Předání uchovávání a vrácení nebo zničení citlivých dat organizace uložených u třetí strany.
 - Odebrání přístupů třetí strany k systémům, nástrojům a zařízením.

O Institutu interních auditorů

IIA je mezinárodní profesní sdružení, které reprezentuje více než 265 000 členů po celém světě a udělilo více než 200 000 certifikací Certified Internal Auditor® (CIA®). Organizace IIA byla založena v roce 1941 a je celosvětově uznávána jako lídr v oblasti standardů, certifikací, vzdělávání, výzkumu a odborného poradenství pro profesi interního auditu. Další informace najdete na webu theiia.org.

Autorská práva

© 2025 The Institute of Internal Auditors, Inc. Všechna práva vyhrazena. Pro povolení k reprodukci kontaktujte prosím copyright@theiia.org.

Září 2025



The Institute of
Internal Auditors

Globální ústředí

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