

# Třetí strany

*Tematické požadavky*

*Uživatelská příručka*



# Obsah

---

<b>Přehled Tematických požadavků .....</b>	<b>2</b>
Použitelnost, riziko a odborný úsudek .....	2
<b>Přístupy .....</b>	<b>7</b>
Přístupy k řízení a správě společnosti .....	7
Přístupy k řízení rizik .....	8
Přístupy k řídicím a kontrolním procesům .....	10
<b>Příloha A. Příklady praktického použití .....</b>	<b>16</b>
<b>Příloha B. Volitelný dokumentační nástroj .....</b>	<b>17</b>
Řízení a správa třetích stran .....	17
Řízení rizik třetích stran .....	18
Kontroly třetích stran .....	19

# Přehled Tematických požadavků

---

Tematické Požadavky, spolu s Globálními standardy interního auditu™ a Globálními návody tvoří základní součást Mezinárodního rámce profesní praxe®. Institut interních auditorů požaduje, aby se Tematické požadavky používaly ve spojení s Globálními standardy interního auditu, které poskytují autoritativní základ pro požadované postupy interního auditu. Odkazy na Standardy jsou v této příručce uvedeny průběžně jako zdroj podrobnějších informací.

Tematické požadavky formalizují způsob, jakým způsobem interní auditoři přistupují k převládajícím rizikovým oblastem, a tím podporují kvalitu a konzistentnost v rámci profese. Stanovují základ a poskytují relevantní kritéria pro provádění ujišťovacích služeb vztahujících se k předmětu Tematických požadavků (standard 13.4 Hodnotící kritéria). Soulad s Tematickými požadavky je povinný pro ujišťovací služby a doporučená pro hodnocení poradenských služeb. Tematické požadavky nemají za cíl pokrýt všechny možné aspekty, které by měly být při provádění ujišťovacích zakázek zvažovány; jejich hlavním účelem je spíše stanovit minimální soubor požadavků, které umožní konzistentní a spolehlivé posouzení daného tématu.

Tematické požadavky jasně odkazují na Model tří linií IIA a na Globální standardy interního auditu. Řízení a správa společnosti, řízení rizik a kontrolní procesy tvoří hlavní složky Tematických požadavků, které jsou v souladu se standardem 9.1 Porozumění řízení, řízení rizik a kontrolním procesům. Model tří linií řadí řízení a správu společnosti pod orgány společnosti, řízení rizik pod druhou linii a kontroly a kontrolní procesy pod první linii. Zatímco vedení má zastoupení v první i druhé linii, útvar interního auditu je umístěna ve třetí linii jako nezávislý a objektivní poskytovatel ujištění, který je přímo podřízen orgánům společnosti (Princip 8 Dohled orgánů společnosti).

## Použitelnost, riziko a odborný úsudek

Tematické požadavky je nutné dodržovat, když útvar interního auditu provádí ujišťovací zakázky týkající se oblastí, pro která Tematické požadavky existují, nebo pokud jsou prvky Tematických požadavků identifikovány v rámci jiných ujišťovacích zakázek.

Jak je uvedeno ve standardech, hodnocení rizik je důležitou součástí plánování vedoucího auditora. Určení ujišťovacích zakázek, které mají být zahrnuty do plánu interního auditu, vyžaduje alespoň jednou ročně posoudit strategie, cíle a rizik organizace (standard 9.4 Plán interního auditu). Při plánování jednotlivých ujišťovacích zakázek musí interní auditoři vyhodnotit rizika relevantní pro danou zakázku (standard 13.2 Posouzení rizik zakázky).

Pokud je oblast Tematických požadavků identifikována během procesu plánování interního auditu s ohledem na rizika a je zahrnuto do plánu auditu, je nutné při posuzování daného tématu v příslušných zakázkách uplatnit požadavky uvedené v Tematických požadavcích. Dále, pokud interní auditoři při provádění zakázky (bez ohledu na to, zda je součástí plánu) a narazí na prvky Tematických požadavků, musí tento požadavek posoudit z hlediska jeho relevance pro danou zakázku. Nakonec, pokud je vyžádána zakázka, která původně nebyla v plánu auditu a týká se daného tématu, je třeba posoudit, zda je v daném kontextu použitelný.

Při uplatňování Tematických požadavků hraje klíčovou roli odborný úsudek. Posouzení rizik je podkladem pro rozhodování vedoucích pracovníků auditu o tom, které zakázky zahrnout do plánu interního auditu (standard 9.4 Plán interního auditu). Vedle toho interní auditoři využívají odborný úsudek k určení, které aspekty budou v rámci každé zakázky zahrnuty (standards 13.3 Cíle a rozsah zakázky, 13.4 Kritéria hodnocení a 13.6 Pracovní program). Příloha A "Příklady praktického použití" popisuje, jak interní auditoři určují, zda se na ně vztahují Tematické požadavky.

Musí být zachovány důkazy o tom, že každý požadavek v Tematických požadavcích byl posouzen z hlediska použitelnosti, včetně odůvodnění, které vysvětluje vyloučení jakýchkoli požadavků. Soulad s Tematickými požadavky musí být zdokumentován s využitím odborného úsudku auditora, jak je popsáno ve standardu 14.6 Dokumentace zakázky.

Zatímco Tematické požadavky poskytují základní rámec kontrolních procesů, které je třeba zvážit, organizace, které hodnotí kybernetické riziko jako velmi vysoké, mohou potřebovat posoudit další aspekty.

Pokud vedoucí interního auditu rozhodne, že útvar interního auditu nemá potřebné znalosti k provádění auditních zakázek na téma Tematických požadavků, může být práce na zakázce zadána externě (standards 3.1 Kompetence, 7.2 Kvalifikace vedoucího auditora, 10.2 Řízení lidských zdrojů). Ani v takovém případě outsourcing nezbavuje útvar interního auditu odpovědnosti za dodržování Tematických požadavků. Konečnou odpovědnost za zajištění souladu si ponechává vedoucí interního auditu. Navíc pokud vedoucí auditor rozhodne, že zdroje interního auditu jsou nedostatečné, musí informovat orgány společnosti o dopadu nedostatečných zdrojů a způsobu řešení jejich případného nedostatku (standard 8.2 Zdroje).

### ***Výkon, dokumentace a podávání zpráv***

Při uplatňování Tematických požadavků musí interní auditoři rovněž dodržovat standardy a vykonávat svou práci v souladu s Doménou V: Provádění služeb interního auditu. Standardy v Doméně V popisují plánování zakázek (Princip 13 Plánujte zakázky účinně), provádění zakázek (Princip 14 Realizujte zakázku řádně) a komunikaci výsledků zakázek (Princip 15 Komunikujte závěry zakázky a monitorujte akční plány).

Zahrnutí Tematických požadavků lze zdokumentovat buď v plánu interního auditu, nebo v pracovních dokumentech zakázky, a to na základě odborného úsudku auditora. Jedna nebo více zakázek interního auditu může pokrýt dané požadavky. Navíc nemusí být všechny požadavky vždy použitelné. Musí být zachovány důkazy o tom, že Tematické požadavky



byly posouzeny z hlediska použitelnosti, včetně odůvodnění vysvětlujícího případné vyloučení.

### **Zajištění kvality**

Standardy vyžadují, aby vedoucí auditu vypracoval, implementoval a udržoval program pro zajišťování a zvyšování kvality, který pokrývá všechny aspekty fungování interního auditu (standard 8.3 Kvalita). Výsledky musí být sděleny orgánům společnosti a vrcholovému vedení, které musí být informováno o souladu útvaru interního auditu se Standardy a o dosažení výkonnostních cílů.

Soulad s Tematickými požadavky bude hodnocen v rámci posuzování kvality.

### **Third Party**

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 ustanovený smlouvou, dohodou nebo jiným způsobem, aby organizace získala produkty, služby, pracovní sílu, výrobu nebo řešení informačních technologií, jako je ukládání, zpracování a údržba dat.

Pojem "třetí strana" může být používán různě v závislosti na odvětví nebo jiných souvislostech. Každý útvar interního auditu může přizpůsobit na základě svého úsudku uplatňování Tematických požadavků podle toho, jak primární organizace (organizace uzavírající dohodu s třetí stranou) definuje třetí strany. V Tematických požadavcích na třetí strany a v uživatelské příručce se pojem "třetí strana" používá pro prodejce, dodavatele, zhotovitele, subdodavatele, externí poskytovatele služeb, jiné zprostředkovatele a konzultanty. Pojem "třetí strana" zahrnuje všechna taková ujednání, včetně ujednání mezi třetí stranou a jejími subdodavateli, často označovanými jako "následní subdodavatelé" nebo "čtvrté strany", "páté strany" nebo "N-té strany"

Tyto Tematické požadavky se netýkají nepřímých externích vztahů, zájmů nebo zapojení do primární organizace, jako jsou regulační orgány, zástupci, makléři, investoři, správci/členové orgánů společnosti, veřejné služby a členové veřejnosti, ani interních vztahů, jako jsou zaměstnanci nebo poskytovatelé služeb uvnitř skupiny.

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.

Účinnost procesů organizace při řízení vztahů s třetími stranami může být hodnocena napříč celou organizací a/nebo na úrovni jedné či více jednotlivých smluv, dohod nebo vztahů. Interní auditoři by měli používat přístup shora dolů, aby získali přehled o zásadách, postupech, procesech, rámcích a cyklech spolupráce organizace se třetími stranami. Interní auditoři by měli používat úsudek, aby pochopili nuance v rizicích třetích stran na základě jednotlivých odvětví, organizací a témat zakázek. V souladu se standardem 5.1 Používání informací by interní auditoři měli znát a dodržovat veškeré zásady a postupy týkající se informací třetích stran, ke kterým mohou mít přístup.

Tematické požadavky se uplatní, pokud útvar interního auditu provádí ujišťovací zakázky u třetích stran a/nebo jakýchkoli subdodavatelských vztahů, včetně těch čtvrtých nebo dalších

navazujících, které umožňuje smlouva nebo dohoda třetí strany s primární organizací. Interní auditoři by měli upřednostňovat třetí a další navazující strany na základě rizika, jak je popsáno v části o řízení rizik níže. Interní auditoři musí uplatnit všechny požadavky, které vyplývají z výsledků posouzení rizik, a vyloučení musí být zdokumentována.

Tematické požadavky na třetí strany a uživatelská příručka odkazují na fáze vztahu organizace s třetími stranami, známé také jako fáze cyklu spolupráce: výběru, uzavření smlouvy, zahájení spolupráce, monitorování a ukončení spolupráce. Tyto fáze budou použity pro účely Tematických požadavků na třetí strany a uživatelské příručky, i když některá odvětví mají vlastní verze cyklu spolupráce. Tyto fáze jsou:

- **Výběr:** zahrnuje postupy pro rozhodnutí o potřebě třetí strany, plán jejího využití a náležitou péči při výběru. Navíc by měl výběr zahrnovat posouzení rizik potenciálních a zapojených třetích stran.
- **Uzavření smlouvy:** zahrnuje procesy náležité péče pro přípravu, vyjednávání, schvalování a implementace právní dohody s třetí stranou.
- **Zahájení spolupráce:** začíná podpisem smlouvy, která zahajuje vztah, a vytváří základ pro to, aby třetí strany splnily podmínky smlouvy nebo dohody.
- **Monitorování:** zahrnuje postupy pro řízení v průběhu cyklu spolupráce a průběžné monitorování třetí strany po uzavření a schválení smlouvy. Přístup je obvykle systematický a založený na rizicích a měl by brát v potaz průběžné zlepšování. Monitorování zahrnuje obnovování stávajících smluv nebo dohod s třetími stranami, když je to nutné.
- **Ukončení spolupráce:** zahrnuje procesy ukončování smluv a dohod, udržitelnou strategii pro odchod třetích stran, kterým byla stanovena priorita na základě rizika, a ukončování vztahů v momentě potřeby. Tyto procesy obvykle využívají přístup založený na rizicích a mohou zahrnovat formální plán ukončení spolupráce.

Primární organizace zůstává plně zodpovědná za rizika spojená s dosahováním svých cílů, i když zapojí třetí stranu, aby jí jednoho nebo více cílů pomohla dosáhnout. Zapojení třetích stran může snížit některé náklady organizace na provádění procesů. Může však přinést provozní rizika, protože primární organizace má menší přehled a pravomoci v kontrolních procesech třetí strany. Pokud třetí strana nesplní to, co bylo sjednáno ve smlouvě, podílí se na neetických praktikách nebo dojde k narušení provozu, může to mít pro primární organizaci následky.

Primární organizace musí identifikovat, vyhodnocovat a řídit rizika prostřednictvím vhodných procesů správy, řízení rizik a kontroly. Kategorie a příklady rizik souvisejících s třetími stranami zahrnují:

- **Strategické,** jako je schopnost plnit poslání organizace a/nebo cíle na vysoké úrovni nebo řídit dopady fúzí a akvizic.
- **Reputační,** jako jsou škody způsobené na životním prostředí nebo na vztazích a důvěře primární organizace s klienty, zákazníky a zainteresovanými subjekty.
- **Etické,** jako jsou selhání integrity, střety zájmů, úplatky a korupce.



- Operační, jako je fyzická a informační bezpečnost, riziko zasvěcených osob, narušení služeb a nedosažení cílů.
- Finanční, jako je platební neschopnost třetích stran a podvody.
- Dodržování platných místních, národních a mezinárodních regulačních požadavků.
- Kybernetická bezpečnost a další ochrana dat, například ohrožení a únik citlivých údajů.
- Informační technologie, například nedostatek služeb na podporu kritických operací.
- Právní otázky, jako jsou střety zájmů, spory a soudní spory v případě porušení smlouvy.
- Udržitelnost, například v oblasti ESG (životního prostředí, sociální a řízení a správy společnosti). Příklady zahrnují rizika související s dopadem organizace na přírodní prostředí a rizika týkající se interakcí organizace s komunitami.
- Geopolitická, jako jsou obchodní spory/sankce a politická nestabilita.

Interní auditoři by měli při posuzování požadavků na řízení a správu společnosti, řízení rizik a kontrolní procesy zohlednit každou fázi cyklu spolupráce se třetí stranou.

Požadavky v Tematických požadavcích na třetí strany jsou rozděleny do tří oddílů podle standardu 9.1 Porozumění procesům řízení a správy společnosti, řízení rizik a řídicím a kontrolním procesům:

- Řízení a správa společnosti – jasně definované základní cíle a strategie pro využívání třetích stran k podpoře cílů, zásad a postupů organizace.
- Řízení rizik – procesy pro identifikaci, analýzu, řízení a monitorování rizik spojených s využíváním třetích stran, včetně procesu pro včasnou eskalaci incidentů.
- Kontroly – vedením zavedené, pravidelně vyhodnocované kontrolní procesy ke zmírnění rizik při využívání třetích stran.

Kromě Tematických požadavků a této uživatelské příručky mohou interní auditoři využít další odborné návody týkající se třetích stran, například globální pokyny IPPF a zdroje specifické pro dané odvětví.

# Přístupy

Následující přístupy mohou interním auditorům pomoci při implementaci požadavků obsažených v Tematických požadavcích na třetí strany. Níže uvedená ustanovení v jednotlivých oddílech opakují nebo parafrázuji odpovídající požadavky Tematických požadavků. Tyto nepovinné přístupy jsou ilustrativní, aby poskytly příklady způsobů, jak požadavky posoudit. Interní auditoři by měli při rozhodování o tom, co zahrnout do svých hodnocení, uplatňovat svůj odborný úsudek.

## Přístupy k řízení a správě společnosti

Za účelem posouzení, jak jsou procesy řízení, včetně dohledu orgánů společnosti, uplatňovány na cíle třetích stran, mohou interní auditoři prověřit důkazy o:

- A. Formalizovaný a zdokumentovaný přístup nebo strategie založená na riziku pro určení, zda využít třetí stranu. Tento přístup je pravidelně revidován a zahrnuje:
  - Jasně definovaný a standardizovaný proces pro implementaci přístupu, schválený pro použití v organizaci.
  - Rozpočtované zdroje na základě analýzy nákladů a přínosů, která odůvodňuje zapojení třetí strany, zajišťuje strategické sladění a efektivitu zdrojů.
  - Vyhodnocení rizik a kontrolních mechanismů vedením, včetně těch, které se týkají problémů se třetími stranami.
  - Přiměřené zdroje pro uzavírání smluv, řízení a monitorování výkonu třetích stran.
  - Zapracování zpětné vazby zainteresovaných subjektů do přístupu nebo strategie.
- B. Zásady, postupy a další příslušná dokumentace používaná k definování, hodnocení a řízení vztahů s třetími stranami v průběhu cyklu spolupráce. Tyto zásady a postupy mohou zahrnovat:
  - Standardizované nástroje a šablony pro usnadnění klíčových procesů správy, řízení rizik a kontroly.
  - Procesy pravidelného hodnocení zásad a postupů, zjišťování jejich přiměřenosti a jejich případné aktualizace.
  - Stanovení kritérií pro výběr, uzavírání smluv, zahájení spolupráce, monitorování a ukončení spolupráce se třetími stranami.
  - Identifikace a pravidelná revize platných regulačních požadavků z hlediska souladu se zásadami a postupy.
  - Benchmarking prováděný za účelem identifikace a porovnání hlavních řídicích procesů třetích stran.

- C. Definované role a odpovědnosti, které napomáhají dosažení cílů třetích stran. Další evidence může zahrnovat:
- Procesy hodnocení, zda jsou hodnoty, etika a společenská odpovědnost třetí strany v souladu se zásadami primární organizace. Tento proces by měl zahrnovat způsob, jak okamžitě řešit případné střety zájmů nebo neetické praktiky.
  - Pravidelné školení pracovníků zastávajících řídicí funkce třetích stran a pravidelné hodnocení jejich kompetencí.
  - Proces vyhodnocování, zda jsou prováděna školení s cílem zajistit v celé organizaci povědomí o třetích stranách.
  - Role a odpovědnosti jsou v souladu s modelem tří linií.
- D. Včasná komunikace a zapojení příslušných zainteresovaných subjektů v průběhu celého cyklu spolupráce se třetí stranou (například orgány společnosti, vrcholové vedení, nákupní oddělení, provozní oddělení, řízení rizik, compliance, právní oddělení, informační technologie, informační bezpečnost, lidské zdroje a další), což zahrnuje:
- Informace o rizicích třetích stran a známých potenciálních zranitelnostech v zápisech z jednání, zprávách nebo e-mailech.
  - Výměna informací o řízení třetích stran a podpora spolupráce (například prostřednictvím pravidelných mezioborových setkání).

## Přístupy k řízení rizik

Za účelem posouzení, jak jsou procesy řízení rizik uplatňovány na cíle týkající se třetích stran, mohou interní auditoři prověřit důkazy, které zahrnují:

- A. Standardizované a komplexní procesy řízení rizik pro uživatele služeb třetích stran zahrnují definované role a odpovědnosti a dostatečně řeší klíčová rizika relevantní pro organizaci:
- Procesy hodnocení a řízení rizik třetích stran zahrnují způsob, jakým jsou klíčová rizika:
    - Prvotně identifikována a hlášena.
    - Analyzována za účelem vyhodnocení jejich dopadu na schopnost dosáhnout cílů organizace.
    - Zmírňována, včetně akčních plánů na snížení rizika na přijatelnou úroveň.
    - Monitorována, včetně detekce a reakce na prvotní výstrahy a plánu průběžného hlášení až do úplného vyřešení hrozeb.
  - Je monitorováno dodržování procesů a zavádění nápravných opatření v případě jakýchkoli odchylek, aby se zabránilo ohrožení dlouhodobých cílů nebo strategie organizace.

- Výbor pro řízení rizik nebo jiný příslušný výbor zajišťuje přímý dohled nad třetími stranami a poskytuje podklady orgánům společnosti. Výbor má definovaný účel a pravidelně se schází. Jako evidence mohou sloužit zápisy ze schůzí.
- B. Rizika spojená s třetími stranami v průběhu cyklu spolupráce jsou pravidelně identifikována a vyhodnocována. Hodnocení rizik kategorizuje třetí strany a stanoví jejich priority. Reakcím na rizika jsou přiřazeny priority a kategorie.
  - Primární organizace při vypracovávání hodnocení rizik třetích stran zohledňuje faktory, jako je její velikost, vyspělost a počet zapojených třetích stran.
  - Posouzení rizik je zdokumentováno a identifikuje inherentní a zbytková rizika.
  - Organizace postupuje při přezkumu a aktualizaci hodnocení rizik v souladu s procesem náležité péče.
  - Jsou stanovena kritéria pro kategorizaci a prioritizaci třetích stran podle rizik. Mezi tato kritéria patří například:
    - Poskytované služby jsou pro provoz organizace zásadní.
    - Finanční hodnota této spolupráce je významná.
    - Zda je spolupráce nová, navázaná rychle a/nebo je dlouhodobá.
    - Je zapojeno více externích stran.
    - Třetí strana plánuje zadat část nebo všechny práce subdodatelům.
  - Organizace dodržuje všeobecně uznávané postupy hodnocení rizik, včetně toho, že hodnocení rizik se provádí v co nejranější fázi, obvykle při analýze návrhu ve fázi výběru a před zahájením spolupráce.
  - Dodavatelé vyplní dotazník, který určí jejich kategorizaci rizik a prioritu na základě inherentních rizik. Organizace zajistí, že dotazníky jsou vyplněny relevantními pracovníky a byla zkontrolována jejich přesnost a správnost.
  - Organizace pravidelně získává podklady týkající se řízení rizik třetích stran z provozních oblastí, jako jsou informační technologie, zadávání veřejných zakázek, řízení podnikových rizik, lidské zdroje, právní oddělení, oddělení compliance, provozní oddělení, účetnictví a finance.
- C. Reakce na rizika, jako je zmírnění, přijetí, eliminace a sdílení jsou určené a úměrné rizikovému hodnocení.
  - Reakce na rizika jsou zdokumentované a zahrnují zohlednění kontrolního prostředí třetí strany.
  - Dokumentace, že reakce na rizika, která překračují toleranci primární organizace, jsou přezkoumány z hlediska vhodnosti, zejména pokud jsou rizika akceptována. Tyto reakce zahrnují i ty, které se týkají možných střetů zájmů třetích stran.
- D. Procesy řízení a eskalace rizik třetích stran, včetně způsobu vyhodnocování, přiřazování úrovně ohrožení nebo rizika a stanovení priorit. Přezkum může identifikovat:
  - Definice a vysvětlení úrovně rizik organizace – například vysoké, střední a nízké – a postupy eskalace pro každou kategorii rizik.

- Seznam třetích stran seřazených podle zjištěných rizik a stav zmírnění všech rizikových událostí.
- Platné právní, regulatorní a compliance požadavky.
- Dopady rizik, a to jak finančních, tak nefinančních (například pověst).
- Procesy informování vedení a zaměstnanců o rizicích třetích stran, včetně pravidelného podávání zpráv o rizikovém profilu představenstvu (nebo jinému vhodnému orgánu). Komunikace by měla zahrnovat aktuální informace o nápravě všech problémů zjištěných u prioritních třetích stran.
- Procesy pro přehodnocení kategorizace a stanovení priorit, když se změň úroveň rizikového apetitu a rizikové tolerance primární organizace.

## Přístupy k řídicím a kontrolním procesům

Při posuzování toho, jak jsou kontrolní procesy uplatňovány ve vztahu ke třetím stranám, mohou interní auditoři prověřit evidenci, že:

- A. Je zaveden proces náležité péče pro získávání a výběr třetích stran se zdokumentovaným a schváleným obchodním případem nebo jinou příslušnou dokumentací popisující a odůvodňující potřebu a povahu vztahu s třetí stranou.
  - Obchodní případ může také:
    - Zabývat se riziky, která ohrožují schopnost třetí strany splnit očekávání, a možnými dopady na organizaci.
    - Zahrnovat podrobnou analýzu nákladů a přínosů.
  - Jsou stanoveny procesy získávání zdrojů, jako jsou výběrová řízení, žádosti o nabídky a výhradní zdroje. Tyto procesy zahrnují:
    - Kritéria důležitých aspektů, jako je přezkoumání protokolů o kybernetické bezpečnosti, ověření bankovních údajů, prověření finanční minulosti a zkoumání organizační struktury třetí strany, trestních a právních záznamů, záznamů o dopravních přestupcích, politických aktivitách a vazeb na trestnou činnost.
    - Dobře definovaná kritéria výběru, včetně hodnocení dosavadní výkonnosti, referencí, pověsti a nákladů na zakázku.
    - Náležitou péči pro zajištění vhodného výběru dodavatelů, například vytvoření meziodborových týmů pro přezkum návrhů. Aby se snížilo riziko podjatosti, zahrnují kontroly přezkumných týmů postupy pro vytváření týmů a požadavky na zveřejňování potenciálních střetů zájmů.
    - Náležitou péči při posuzování kontrolního prostředí třetí strany, například provedení návštěvy na místě nebo přezkoumání u třetí strany:
      - Zprávy o kontrole systému a organizace (SOC).
      - Finanční stability.
      - Zakladatelských listin nebo osvědčení o bezúhonnosti.

- Transparentnosti rozhodování klíčového vedení a zainteresovaných subjektů.
  - Organizační struktury.
  - Provozní stability.
  - Protokolů kybernetické bezpečnosti.
  - Dodržování příslušných zákonů, předpisů a norem.
  - Etiky.
  - Historie v rámci primární organizace.
  - Pověsti.
- Důkazy o tom, že potenciální dodavatelé nebo zhotovitelé postupují do fáze uzavírání smluv v rámci cyklu spolupráce až po provedení příslušných procesů náležité péče a analýze jejich výsledků.
- B.** Jsou stanoveny a dodržovány zásady a postupy pro uzavírání smluv.
- Smlouvy jsou psány jednoznačně.
  - Klíčová rizika jsou zvažována ve fázi přípravy smlouvy a jsou do ní zahrnuty příslušné doložky. V této fázi se s třetí stranou komunikují problémy, které vyžadují řešení.
  - Podstatné prvky smluv jsou stanoveny na základě zásad a postupů organizace pro uzavírání smluv a úrovně priority třetí strany. Prvky mohou zahrnovat:
    - Dohody o mlčenlivosti (ochraně osobních údajů).
    - Ukončovací doložky a definované parametry pro přístup k datům.
    - Požadavky na kybernetickou bezpečnost, včetně požadavků na přístup ke všem údajům a jejich sdílení a hlášení incidentů nebo narušení bezpečnosti ve stanovené lhůtě.
    - Požadavky na oznámení o narušení, které se týká údajů primární organizace.
    - Standardizovaný postup pro ověření identifikace třetí strany, včetně úplného zákonného názvu, adresy, fyzického umístění a webových stránek. Standardním postupem je použití kontrolního seznamu během procesu identifikace a kontrola správnosti informací.
    - Jasně definované dohody o úrovni služeb, které specifikují očekávané výsledky a práva, povinnosti, sankce, odměny a odpovědnosti jednotlivých stran, včetně odpovědnosti za úhradu mzdových nákladů (včetně dalších navazujících subdodavatelů).
    - Doložka o právu na audit, která zahrnuje navazující subdodavatele, nebo požadavek na doložení, že renomovaný nezávislý poskytovatel ujištění provedl audit smluvních stran. Bez doložky o právu na audit může být schopnost interního auditu získat nebo poskytnout ujištění omezena.

- Primární organizace má přístup ke zprávám nezávislých auditorů o hodnocení kontrol, například zprávám o finančních otázkách, compliance a zabezpečení dat, jako jsou mezinárodní standard pro ujišťovací zakázky nebo zprávy SOC.
  - Pokud se spoléháme na práci externích poskytovatelů ujištění třetí strany, jsou dokumenty přezkoumány, aby byla zajištěna jejich spolehlivost.
  - Zprávy SOC se používají k identifikaci nedostatečných procesů řízení rizik a změn.
- Zásady a postupy se týkají všech složek, které jsou pro konkrétní organizace nebo typy zakázek zásadní:
  - Ustanovení o životním prostředí a udržitelnosti.
  - Protokoly o whistleblowingu.
  - Požadavky na hodnocení výkonu.
  - Testovaný plán kontinuity provozu pro třetí strany.
  - Využití umělé inteligence při poskytování služeb.
  - Jasná identifikace, zveřejnění, podmínky a rozsah všech navazujících subdodavatelských prací.
  - Proces řízení změn, který popisuje, jak se mají řešit změny rozsahu, podmínek nebo provozních požadavků (například změny technologie nebo aktualizace předpisů) v průběhu trvání smlouvy.
  - Omezení počtu změnových příkazů nebo částek, které lze vyúčtovat.
- Zásady a postupy vyžadují formální přijetí finálních produktů před provedením platby nebo uvolněním zádržného.
- Třetí strany jsou povinny sdílet své etické zásady nebo kodex chování a/nebo dodržovat zásady a kodex primární organizace.
- Pokud smlouvu poskytuje třetí strana, primární organizace provedla právní přezkum a klíčová rizika jsou pochopena a podpořena vhodnou strategií pro jejich zmírnění.
- C. Finalizované smlouvy nebo dohody jsou přezkoumány a schváleny příslušnými zainteresovanými subjekty, včetně právních a compliance, bezpečně uloženy a přiděleny správci nebo administrátorovi smluv, který za ně nese odpovědnost.
  - Smlouva nebo jiný oficiální dokument označující externě zajišťovaný vztah a závazek třetí strany a doklad o všech požadovaných právních a compliance přezkumech.
- D. Je veden přesný, úplný a aktuální seznam všech vztahů se třetími stranami, například v centralizovaném systému správy smluv.
  - Proces přidávání nových smluv nebo dohod třetích stran do seznamu nebo systému.
  - Proces zadávání potenciálních třetích stran do systému dodavatelů a jejich odstranění v případě, že smlouva není schválena.

- Postup pro odstranění smluv nebo dohod třetích stran ze seznamu nebo systému.
  - Systém sledování, který umožňuje dokumentovat problémy s konkrétními dodavateli nebo prodejci pro budoucí použití.
  - Proces přezkoumání, jehož cílem je určit, zda je soubor třetích stran přesný a úplný.
- E. Jsou zavedeny a dodržovány zdokumentované postupy pro zahájení spolupráce, které třetím stranám umožňují splnit podmínky smlouvy nebo dohody. V rámci přezkumu lze ověřit, zda:
- Standardizované postupy pro zahájení spolupráce zajišťují, že je dokončena veškerá potřebná dokumentace, školení a kontroly dodržování předpisů.
  - Systémy a procesy třetí strany se mohou bezproblémově integrovat s technologiemi primární organizace.
  - Sdílené systémy jsou kompatibilní a bezpečné. Důkazy mohou zahrnovat doplňkové kontroly uživatelského subjektu v rámci vykazování SOC.
  - Primární organizace posuzuje plány kontinuity provozu třetí strany, které zajišťují pokračování služeb v případě mimořádných událostí. Pro případné narušení jsou zahrnuty pohotovostní plány.
- F. Procesy průběžného sledování výkonnosti dodavatele ve vztahu k cílům smlouvy nebo dohody, včetně hodnocení klíčových ukazatelů výkonu.
- Monitorovací procesy poskytují informace pro hodnocení rizik třetí stranou a zjištěné nedostatky v kontrole jsou přezkoumávány, eskalovány a podle potřeby řešeny.
  - Zprávy nebo pozorování procesů, technologií a nástrojů zavedených pro řízení monitorování v reálném čase.
  - Procesy zajišťující provádění plateb v souladu s podmínkami smlouvy nebo dohody, jako je dodržování časového harmonogramu projektu, milníků a požadavků na komunikaci. Platby se provádějí pouze schváleným dodavatelům, kteří dokončili fázi zahájení spolupráce a byli zadáni do systému pro platby dodavatelům. Pokud jsou ve smlouvě specifikovány výsledky, konečné platby se provádějí až po jejich ověření.
  - Sledování kontroly nákladů spojených s dohodami s třetími stranami s cílem zajistit hodnotu a určit návratnost investic. Výsledky analýz nákladů a přínosů se používají k novému projednávání smluv.
  - Postupy pro vyměřování sankcí za nedodržení případných dohod o úrovni služeb ve smlouvě nebo dohodě. Sankce se vypočítávají a účtují v okamžiku jejich vzniku.
  - Pořadí prioritních třetích stran na základě rizik se pravidelně přehodnocuje, když dojde ke změnám v dohodě a když se blíží vypršení platnosti smlouvy nebo její automatické obnovení.

- Kontroly prioritních třetích stran, jako jsou kontroly na místě nebo čtvrtletní kontroly činnosti, za účelem ověření kontrol a provozní integrity.
- Důkazy o dalším průběžném monitorování mohou zahrnovat:
  - Analýzy finanční stability třetí strany.
  - Posuzování stížností na třetí strany.
  - Přezkoumání zpráv nezávislých auditorů, jako jsou mezinárodní standard pro ujišťovací zakázky, Prohlášení o standardech pro ověřovací zakázky, finanční zprávy, zprávy o auditu, zprávy o dodržování předpisů a zprávy o zabezpečení dat poskytované třetími stranami, certifikace ISO.
  - Přezkoumání testů odolnosti podniku provedených třetí stranou ze strany vedení, včetně všech zjištěných významných problémů.
  - Podmínky a omezení pro využívání subdodavatelů nebo dalších navazujících subjektů.
  - Hodnocení etických hodnot, kultury a chování třetích stran.
  - Odpovědi na dotazy médií.
  - Vyhodnocení protokolů o ochraně soukromí a kybernetické bezpečnosti na ochranu ukládání a přenosu dat a informací primární organizace, včetně využití pokročilých technologií, jako je umělá inteligence.
  - Identifikace příležitostí k neustálému zlepšování výkonu a plnění cílů smlouvy nebo dohody ze strany organizace.
  - Kontrola rozdělení povinností.
- G. Protokoly pro zahájení nápravných opatření u zjištěných incidentů, pokud třetí strana neplní požadavky smlouvy nebo dohody nebo pokud činnosti třetí strany zvyšují riziko pro primární organizaci.
  - Protokoly pro eskalaci incidentů na základě závažnosti incidentu a priority třetí strany.
  - Přezkoumání po incidentu, včetně analýzy příčin.
- H. Procesy pro poskytování upozornění na smlouvy a dohody, jejichž platnost se blíží ke konci nebo k automatickému prodloužení. Procesy automatického obnovení zahrnují kontrolu:
  - Výkonu třetí strany.
  - Podmínek smlouvy nebo dohody a případné dodatky.
  - Rizikových faktorů.
- I. Je zaveden a dodržován formalizovaný plán ukončení spolupráce, aby bylo zajištěno, že jsou náležitě řešeny smluvní požadavky týkající se načasování a očekávání, a to i pro případné navazující subdodavatele.
  - Kontrolní seznamy nebo rozhovory s klíčovými zainteresovanými subjekty s cílem zajistit účinnost bezpečnostních opatření.

- Organizační informace nebo údaje v úschově třetí strany byly vráceny nebo zničeny.
- Přístup třetí strany k datům, systémům nebo zařízením organizace byl zrušen.
- Majetek primární organizace, jako jsou zařízení, softwarové licence, duševní vlastnictví a dokumentace, byl vrácen.
- Při odůvodněném ukončení spolupráce s třetí stranou jsou zjištěny zbývající okolnosti nebo rizika a jsou předány vrcholovému vedení a/nebo orgánům společnosti.
- Pokud je smlouva s prioritní třetí stranou ukončena, je tato strana nahrazena na základě stejného posouzení rizik, pokud není předmět dohody splněn nebo neprestal být potřeba.

# Příloha A. Příklady praktického použití

---

Následující příklady popisují scénáře, ve kterých by se uplatnily Tematické požadavky na třetí strany:

**Příklad 1:** Zakázka interního auditu v plánu interního auditu zahrnuje službu nebo výstup, který v současné době poskytuje třetí strana.

Pokud útvar interního auditu dokončí svůj proces plánování založený na rizicích a do plánu interního auditu zahrne jednu nebo více zakázek služeb nebo výstupů, které jsou v současné době poskytovány třetími stranami na základě smlouvy nebo dohody, jsou tyto Tematické požadavky povinné.

Ne všechny Tematické požadavky se musí vztahovat na každou zakázku. Pokud interní auditoři uplatní odborný úsudek a rozhodnou, že jeden nebo více Tematických požadavků na třetí stranu nejsou použitelné, a proto by měly být ze zakázky vyloučeny, musí interní auditoři zdokumentovat a uchovat odůvodnění vyloučení těchto požadavků. Důvodem pro vyloučení některých požadavků může být například to, že útvar interního auditu zjistil, že závislost organizace na třetích stranách v oblasti kritických služeb je nízká, nebo že se jedná o zavedený vztah s nízkým finančním dopadem.

**Příklad 2:** Rizika třetích stran jsou identifikována během ujišťovací zakázky na jiné téma než třetí strany nebo řízení smluv.

Interní auditoři mohou identifikovat významné riziko třetí strany při posuzování procesu, který nebyl původně určen jako proces související se třetími stranami nebo řízením smluv. Například při plánování zakázky na posouzení ukládání dat se interní auditoři dozvědí, že cloudové služby jsou hostovány prostřednictvím třetí strany. Během rozhovorů s vedením služeb poskytovaných třetí stranou interní auditoři identifikují rizika kybernetické bezpečnosti související s třetí stranou.

Po identifikaci relevantních rizik musí interní auditoři prověřit Tematické požadavky na třetí strany i kybernetickou bezpečnost a určit, které požadavky jsou použitelné. Auditoři mohou z rozsahu zakázky vyloučit procesy řízení třetí strany nebo proces řízení rizik třetí strany a zaměřit se na kontroly třetích stran nad auditovanými službami. Stejný odborný úsudek platí i pro uplatňování Tematického požadavku kybernetické bezpečnosti. Auditoři musí v pracovní dokumentaci k zakázce zdokumentovat odůvodnění vyloučení jakýchkoli Tematických požadavků na třetí strany nebo kybernetickou bezpečnost a dokumentaci uchovat.

**Příklad 3:** Je třeba provést zakázku u třetí strany, která nebyla původně zahrnuta do plánu interního auditu.

V organizaci vznikne problém týkající se prioritní třetí strany, který vyžaduje okamžitou pozornost útvaru interního auditu. Problém se týkal selhání kontroly. Vedoucí interního auditu by měl komunikovat s orgány společnosti o změně priorit plánu auditu a zdrojů útvaru interního auditu, aby se přizpůsobil této potřebě. Auditor by měl spolupracovat s vedením, na které tato skutečnost dopadá, na vypracování cílů zakázky, aby vyhodnotil situaci a navrhl doporučení, která by zabránila budoucím událostem. Vedoucí interního auditu by měl prověřit Tematické požadavky, aby mohl stanovit rozsah zakázky, určit, které požadavky se na ni vztahují, a odpovídajícím způsobem zdokumentovat případné výjimky.



# Příloha B. Volitelný dokumentační nástroj

Od interních auditorů se očekává, že při určování použitelnosti požadavků na základě posouzení rizik budou uplatňovat odborný úsudek a vhodně dokumentovat vyloučení některých požadavků. Tematický požadavek může být zdokumentován v plánu interního auditu nebo v pracovních dokumentech zakázky na základě odborného úsudku auditora. Požadavky může pokrývat jedna nebo více zakázek interního auditu. Kromě toho nemusí být použitelné všechny požadavky. Níže uvedený formulář k vytištění poskytuje jednu z možností, jak doložit shodu s Tematickými požadavky na třetí strany, ale jeho použití není povinné.

## Řízení a správa třetích stran

Požadavek	Provedené pokrytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
<b>A.</b> Je stanoven, zaveden a pravidelně přezkoumáván formální přístup k určení, zda uzavřít smlouvu s třetí stranou. Tento přístup zahrnuje vhodná kritéria pro definování a posouzení zdrojů, které jsou nezbytné a dostupné pro splnění cílů poskytováním produktu nebo služby.		
<b>B.</b> Jsou zavedeny zásady a postupy pro definování, hodnocení a řízení vztahů a rizik s třetími stranami v průběhu celého cyklu spolupráce s třetí stranou. Zásady a postupy jsou v souladu s platnými regulatorními požadavky a jsou pravidelně revidovány a aktualizovány s cílem posílit kontrolní prostředí.		
<b>C.</b> 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 pověřené rolemi a povinnostmi vůči třetími stranám mají odpovídající kompetence.		

Požadavek	Provedené pokrytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
<p><b>D.</b> Jsou definovány protokoly pro komunikaci s příslušnými zainteresovanými subjekty, které zahrnují včasné podávání zpráv o stavu výkonu, rizicích a compliance (zejména porušení zákonů a nařízení) prioritních třetích stran. Třetí strany jsou prioritizovány podle rizika. Mezi příslušné zainteresované subjekty mohou patřit orgány společnosti, vrcholové vedení, zadávání zakázek, provoz, řízení rizik, compliance, právní oddělení, informační technologie, bezpečnost informací, lidské zdroje a další.</p>		

## Řízení rizik třetích stran

Požadavek	Provedené pokrytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
<p><b>A.</b> 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, kybernetická bezpečnost, informační technologie, právní, udržitelnost a geopolitická). Dodržování procesů je sledováno a v případě odchylek jsou prováděna nápravná opatření.</p>		
<p><b>B.</b> Rizika spojená s třetími stranami v průběhu celého cyklu spolupráce jsou pravidelně identifikována a vyhodnocována. Posouzení rizik se používá ke kategorizaci a určení priorit třetích stran, včetně těch dále navazujících. Reakce na rizika jsou také seřazeny a prioritizovány. Hodnocení rizik se pravidelně přezkoumává a aktualizuje.</p>		

Požadavek	Provedené pokrytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
<b>C.</b> Reakce na rizika jsou přiměřené a přesné a odpovídají kategorizaci. Reakce na rizika jsou zavedeny, přezkoumávány, schvalovány, monitorovány, vyhodnocovány a podle potřeby upravovány.		
<b>D.</b> Jsou zavedeny procesy pro řízení a případnou eskalaci problémů, které vzniknou u třetích stran, což zajišťuje odpovědnost za výsledky a zvyšuje pravděpodobnost dosažení 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.		

## Kontroly třetích stran

Požadavek	Provedené pokrytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
<b>A.</b> Je zaveden důkladný proces náležitě péče pro získávání a výběr třetích stran se zdokumentovaným a schváleným obchodním případem nebo jiným příslušným dokumentem, který popisuje a odůvodňuje potřebu a povahu vztahu s třetí stranou.		
<b>B.</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.		
<b>C.</b> Konečné smlouvy nebo dohody jsou zkontrolovány a schváleny všemi příslušnými zainteresovanými subjekty, včetně právních a compliance, podepsány oprávněnými osobami obou stran a bezpečně uloženy. Za každou smlouvu je odpovědný manažer nebo správce.		

Požadavek	Provedené pokrytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
D. Je veden přesný, úplný a aktuální seznam všech vztahů se třetími stranami, například v centralizovaném systému správy smluv.		
E. Jsou zavedeny a dodržovány zdokumentované postupy pro zahájení spolupráce, aby se vytvořil základ pro to, aby třetí strany splnily podmínky smlouvy nebo dohody.		
F. Existují průběžné monitorovací procesy, jejichž cílem je posoudit, zda třetí strany plní podmínky smlouvy nebo dohody v průběhu celého cyklu spolupráce a zda třetí strany plní své smluvní závazky. Tyto postupy zahrnují ověřování spolehlivosti poskytovaných informací a pravidelné přehodnocování výkonnosti a vždy, když se změní dohoda.		
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 příčin incidentů.		
H. Sledují se data vypršení platnosti smluv a jejich prodloužení a v případě potřeby se přijímají opatření 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: <ul style="list-style-type: none"> <li>• Ukončení činnosti třetí strany.</li> <li>• V případě potřeby výměnu třetí stranu.</li> <li>• Předání uchování a vrácení nebo zničení citlivých údajů organizace uložených u třetí strany.</li> <li>• Odebrání přístupů třetí strany k systémům, nástrojům a zařízením.</li> </ul>		

## O Institutu interních auditorů

Institut interních auditorů (The IIA) je mezinárodní profesní sdružení, které sdružuje více než 255 000 členů po celém světě a udělilo více než 200 000 certifikátů Certified Internal Auditor® (CIA®) po celém světě. IIA byla založena v roce 1941 a je celosvětově uznávána jako lídr v oblasti standardů, certifikací, vzdělávání, výzkumu a technického poradenství v profesi interního auditu. Více informací naleznete na [www.theiia.org](http://www.theiia.org).

## Odmítnutí odpovědnosti

IIA vydává tento dokument pro informační a vzdělávací účely. Cílem tohoto materiálu není poskytnout definitivní odpovědi na konkrétní individuální okolnosti a jako takový má sloužit pouze jako vodítko. IIA doporučuje vyhledat nezávislé odborné poradenství týkající se přímo konkrétní situace. IIA nepřebírá žádnou odpovědnost za to, že se někdo bude spoléhat pouze na tento materiál.

## Autorská práva

© 2025 The Institute of Internal Auditors, Inc. Všechna práva vyhrazena. Pro povolení k reprodukci kontaktujte prosím [copyright@theiia.org](mailto:copyright@theiia.org).

září 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