Третя сторона

Тематична Вимога

Topical Requirement

Посібник користувача

The Institute of Internal Auditors

Перекладено:

Institute of Internal Auditors Ukraine

Зміст

Огляд Тематичних Вимог

Тематичні Вимоги є важливим компонентом Основних Положень Міжнародної Професійної Практики® разом із Глобальними Стандартами Внутрішнього Аудиту™ та Глобальними Настановами. Інститут внутрішніх аудиторів (IBA) вимагає, щоб Тематичні Вимоги використовувалися разом зі Стандартами, які забезпечують авторитетну основу для належної практики. Посилання на Стандарти з'являються в цьому посібнику як джерело більш детальної інформації.

Тематичні Вимоги формалізують те, як внутрішні аудитори працюють з поширеними сферами ризику, щоб сприяти підвищенню якості та послідовності в професії. Тематичні Вимоги встановлюють базовий рівень та надають відповідні критерії для виконання послуг з надання впевненості, пов'язаних з предметом Тематичної Вимоги (Стандарт 13.4 Критерії оцінки). Відповідність Тематичним Вимогам є обов'язковою для послуг з надання впевненості та рекомендованою для оцінки під час надання консультаційних послуг. Тематичні Вимоги не мають на меті охопити всі потенційні аспекти, які необхідно враховувати при виконанні завдань з надання впевненості; скоріше, вони мають на меті забезпечити мінімальний набір вимог, які дозволять провести послідовну та надійну оцінку теми.

Тематичні Вимоги чітко пов'язані з моделлю «трьох ліній» IBA та Глобальними Стандартами Внутрішнього Аудиту. Процеси управління, ризик-менеджменту та контролю є основними компонентами Тематичних Вимог, які відповідають Стандарту 9.1 Розуміння процесів управління, ризик-менеджменту та контролю. Відповідно до моделі «трьох ліній», управління пов'язане з радою/керівним органом, ризик-менеджмент - з другою лінією, а заходи контролю або контрольні процеси - з першою лінією. У той час, як керівництво представлене як на першій, так і на другій лініях, функція внутрішнього аудиту відображена на третій лінії, як незалежний та об'єктивний постачальник послуг з надання впевненості, підзвітний раді/керівному органу (Принцип 8 Перебувати під наглядом ради).

Сфери застосування, Ризик та Професійне Судження

Тематичних вимог слід дотримуватися, коли підрозділи внутрішнього аудиту виконують завдання з надання впевненості з питань, для яких існує Тематична Вимога, або коли окремі аспекти Тематичної Вимоги висвітлені в рамках інших завдань з надання впевненості.

Як зазначено в Стандартах, оцінка ризиків є важливою частиною планування, здійснюваного керівником внутрішнього аудиту. Визначення завдань з надання впевненості для включення до плану внутрішнього аудиту вимагає оцінки стратегій, цілей та ризиків організації щонайменше на щорічній основі (Стандарт 9.4 План внутрішнього аудиту). Плануючи окремі завдання з надання впевненості, внутрішні аудитори повинні оцінювати ризики, пов'язані із завданням (Стандарт 13.2 Оцінка ризиків завдання).

Якщо тема Тематичної Вимоги визначена в процесі планування внутрішнього аудиту на основі оцінки ризиків і включена до плану аудиту, то вимоги, які викладені в Тематичній

Вимозі, повинні бути використані для оцінки теми в рамках відповідних завдань. Крім того, коли внутрішні аудитори виконують завдання (включені чи не включені до плану) і виявляють елементи Тематичної Вимоги, вони повинні оцінити застосовність цієї Тематичної Вимоги в рамках виконання завдання. Нарешті, якщо з'являється запит на виконання завдання, яке спочатку не було передбачено планом, але включає в себе цю тему, Тематична Вимога повинна бути оцінена на предмет її застосовності.

Професійне судження відіграє ключову роль у застосуванні Тематичної Вимоги. Оцінки ризиків є визначальним фактором для рішення керівників внутрішнього аудиту щодо того, які завдання включати до плану внутрішнього аудиту (Стандарт 9.4). Крім того, внутрішні аудитори використовують професійне судження для визначення того, які аспекти будуть охоплені в рамках кожного завдання (Стандарти 13.3 Цілі та обсяг завдання, 13.4 Критерії оцінки та 13.6 Робоча програма).

Необхідно зберігати докази того, що кожна вимога в Тематичній Вимозі була оцінена на предмет застосовності, включаючи обґрунтування виключення будь-яких вимог. Відповідність Тематичній Вимозі повинна бути задокументована з використанням професійного судження аудиторів, як це описано в Стандарті 14.6 Документування завдання.

Хоча Тематична Вимога забезпечує базовий рівень процесів контролю для розгляду, організаціям, які оцінюють тематичний ризик, як дуже високий, може знадобитися оцінити додаткові аспекти.

Якщо підрозділ внутрішнього аудиту не має необхідних компетенцій для виконання завдань за напрямком Тематичної Вимоги, керівник внутрішнього аудиту повинен визначити, як отримати ресурси, і своєчасно повідомити раді та вищому керівництву про вплив таких обмежень і про те, як буде вирішуватися проблема дефіциту ресурсів. Керівник внутрішнього аудиту несе остаточну відповідальність за забезпечення відповідності функції внутрішнього аудиту Тематичним Вимогам, незалежно від того, яким чином отримані ресурси (Стандарти 3.1 Компетентність, 7.2 Кваліфікація керівника внутрішнього аудиту, 8.2 Ресурси, 10.2 Управління людськими ресурсами).

Проведення аудиту, Документування та Звітність

Застосовуючи Тематичні Вимоги, внутрішні аудитори також повинні дотримуватися Стандартів, виконуючи свою роботу відповідно до Розділу V: Проведення внутрішнього аудиту. Стандарти Розділу V описують планування завдань (Принцип 13 Ефективно планувати завдання), виконання завдань (Принцип 14 Виконувати завдання) та інформування про результати завдання (Принцип 15 Повідомляти про результати завдання та здійснювати моніторинг планів заходів).

Тематичні Вимоги розроблені для підтримки послідовної та високоякісної практики внутрішнього аудиту. Місцеві закони, нормативні акти, очікування кураторів та інші професійно визнані положення можуть накладати додаткові або більш точні вимоги. Внутрішні аудитори повинні розуміти та дотримуватися законів та/або нормативних актів, що стосуються галузі та юрисдикцій, в яких працює організація, в тому числі розкривати інформацію відповідно до Стандарту 1.3 Правомірна та етична поведінка. В разі, якщо внутрішні аудитори вже інтегрували ці додаткові вимоги в аудиторські програми та процедури тестування, вони повинні звірити їх з Тематичною Вимогою, щоб забезпечити належне охоплення.

Застосовність Тематичної Вимоги може бути задокументована або в плані внутрішнього аудиту, або в робочих документах завдань на основі професійного судження аудиторів. Одне або декілька завдань з внутрішнього аудиту можуть відповідати цим Вимогам. Крім того, не всі вимоги можуть бути застосовані. Необхідно зберігати докази того, що Тематична Вимога була оцінена на предмет застосовності, включаючи обґрунтування будь-яких винятків.

Забезпечення якості

Стандарти вимагають від керівника внутрішнього аудиту розробляти, впроваджувати та підтримувати програму забезпечення та підвищення якості, яка охоплює всі аспекти функціонування внутрішнього аудиту (Стандарт 8.3 Якість). Результати повинні бути повідомлені раді та вищому керівництву. Комунікації повинні інформувати про відповідність функції внутрішнього аудиту Стандартам та досягнення цілей діяльності.

Відповідність Тематичним Вимогам буде оцінюватися під час оцінок якості.

Третя Сторона

Третьою стороною вважається зовнішня фізична особа, група або суб'єкт господарювання, з якою організація ("основна організація") встановлює ділові відносини з метою отримання товарів або послуг. Такі відносини можуть бути оформлені шляхом укладення контракту, угоди або іншим чином, щоб забезпечити організацію товарами, послугами, робочою силою, виробництвом або інформаційними технологічними рішеннями, такими як зберігання, обробка та обслуговування даних.

Примітка

У Тематичних Вимогах використовується загальна термінологія внутрішнього аудиту, визначена у Глобальних стандартах внутрішнього аудиту. Читачі повинні звернутися до термінів і визначень, наведених у глосарії Стандартів.

Термін "третя сторона" може використовуватися по-різному залежно від галузі або інших контекстів. Кожен підрозділ внутрішнього аудиту може гнучко використовувати своє судження при застосуванні Тематичної Вимоги відповідно до того, як основна організація (організація, що укладає угоду з третьою стороною) визначає третіх сторін. У Тематичній Вимозі щодо Третьої Сторони та в посібнику користувача термін "третя сторона" стосується продавців, постачальників, підрядників, субпідрядників, аутсорсингових постачальників послуг, інших організацій та консультантів. Термін "третя сторона" охоплює всі такі домовленості, включаючи домовленості між третьою стороною та її субпідрядниками, часто відомими як субпідрядники "нижчого рівня", або "четверті сторони", "п'яті сторони" чи "N-ні сторони".

Ця Тематична Вимога не стосується непрямих зовнішніх відносин, інтересів або участі в діяльності основної організації, таких як регуляторні органи, агенти, брокери, інвестори, ради (повірені/довірені особи)/члени рад, державні служби та представники громадськості, або внутрішніх зв'язків, таких як співробітники або внутрішньогрупові постачальники послуг.

Термін "третя сторона" може визначатися і використовуватися по-різному, залежно від галузі або інших контекстів. Внутрішні аудитори наділені гнучкістю, щоб покладатися на своє професійне судження для адаптації Тематичної Вимоги до визначення третьої сторони, прийнятого в основній організації.

Ефективність процесів управління взаємовідносинами з третіми сторонами в організації можна оцінити в масштабах всієї організації та/або на рівні одного чи кількох окремих контрактів, угод або взаємовідносин. Внутрішні аудитори повинні використовувати підхід "зверху-вниз", щоб зрозуміти політику, процедури, процеси, структуру та життєвий цикл організації щодо третіх сторін. Внутрішні аудитори повинні використовувати судження для розуміння нюансів ризиків третіх сторін залежно від конкретних галузей, організацій та тем завдань. Відповідно до Стандарту 5.1 Використання інформації, внутрішні аудитори повинні знати і дотримуватися всіх політик і процедур, пов'язаних з інформацією щодо третіх сторін, до якої вони можуть отримати доступ.

Ця Тематична Вимога застосовується, коли функція внутрішнього аудиту виконує завдання з надання впевненості щодо третіх сторін та/або до будь-яких субпідрядних відносин, включаючи відносини з четвертими та наступними сторонами, дозволені контрактом або угодою третьої сторони з основною організацією. Внутрішні аудитори повинні визначати пріоритетність перевірки третіх і наступних сторін на основі ризиків, як описано в розділі "Управління ризиками" нижче. Внутрішні аудитори повинні застосовувати всі вимоги, визначені за результатами оцінки ризиків, а винятки повинні бути задокументовані.

Тематична Вимога щодо Третьої Сторони та Посібник Користувача стосуються етапів відносин організації з третіми сторонами, також відомих як етапи життєвого циклу: відбір, укладання контракту, початок співпраці, моніторинг діяльності та закінчення співпраці. Ці етапи будуть використовуватися для цілей Тематичної Вимоги щодо Третьої Сторони та посібника користувача, незважаючи на те, що в деяких галузях існують власні версії життєвого циклу. Етапи наступні:

- Відбір: включає процеси визначення потреби в третій стороні, планування її залучення та належної перевірки для відбору. Крім того, відбір має включати оцінку ризиків потенційних та залучених третіх сторін.
- Укладання договорів: включає в себе процеси юридичної перевірки для складання, узгодження, затвердження та укладання юридичної угоди з третьою стороною.
- Початок співпраці: починається з моменту підписання контракту щодо початку співпраці і створює основу для виконання третіми сторонами умов контракту або угоди.
- Моніторинг: включає в себе процеси управління "в процесі життя" та постійний моніторинг третьої сторони після укладення та затвердження контракту. Підхід, як правило, є систематичним і заснованим на оцінці ризиків, а також повинен передбачати постійне вдосконалення. Моніторинг включає в себе поновлення поточних контрактів або угод з третіми сторонами, коли це необхідно.
- Припинення співпраці: включає процеси завершення контрактів та угод, розробку стратегії виходу для третіх сторін, які були визначені пріоритетними на основі ризиків, а також припинення відносин у разі необхідності. Процеси, як правило, використовують підхід, заснований на оцінці ризиків, і можуть включати офіційний план виходу.

Основна організація несе відповідальність за ризики, пов'язані з досягненням своїх цілей, навіть якщо вона залучає третю сторону для допомоги в досягненні однієї або декількох цілей. Залучення третіх сторін може зменшити деякі з витрат організації на виконання

процесів. Однак це може спричинити операційні ризики, оскільки основна організація має менше інформації про процеси контролю третьої сторони та менше повноважень щодо них. Якщо третя сторона не виконує контрактні зобов'язання, бере участь у неетичних практиках або зазнає збоїв у бізнесі, основна організація може постраждати від наслідків цих подій.

Основна організація повинна виявляти, оцінювати та управляти ризиками за допомогою відповідних процесів управління, ризик-менеджменту та контролю. Категорії та приклади ризиків, пов'язаних з третіми сторонами, включають:

- Стратегічні, такі як здатність виконувати місію організації та/або цілі високого рівня або управляти наслідками злиття і поглинань.
- Репутаційні, такі як шкода, завдана навколишньому середовищу або стосункам і довірі основної організації з клієнтами, споживачами та зацікавленими сторонами.
- Етичні, такі як порушення доброчесності, конфлікти інтересів, хабарництво та корупція.
- Операційні, такі як фізична та інформаційна безпека, інсайдерські ризики, перебої в обслуговуванні та недосягнення цілей.
- Фінансові, такі як неплатоспроможність третіх сторін та шахрайство.
- Відповідності застосовним місцевим, національним та міжнародним нормативним вимогам.
- Кібербезпекові та інші, пов’язані з захистом даних, наприклад, від компрометації та витоку конфіденційних даних.
- Інформаційних технологій, такі як відсутність сервісів для підтримки критично важливих операцій.
- Юридичні, такі як конфлікти інтересів, спори та судові процеси за порушення контрактів.
- Сталого розвитку, наприклад, екологічні, соціальні та управлінські. Приклади включають ризики, пов'язані з впливом організації на навколишнє середовище, та ризики, що стосуються взаємодії організації з громадами.
- Геополітичні, такі як торгові суперечки/санкції та політична нестабільність.

Внутрішні аудитори повинні враховувати кожну стадію життєвого циклу третьої сторони при оцінці вимог до процесів управління, ризик-менеджменту та контролю.

Вимоги, викладені в Тематичній Вимозі щодо Третьої Сторони, розділені на три розділи відповідно до Стандарту 9.1 Розуміння процесів управління, ризик-менеджменту та контролю:

- Управління - чітко визначені базові цілі та стратегії залучення третіх сторін для підтримки організаційних цілей, політик та процедур.
- Ризик-менеджмент - процеси виявлення, аналізу, управління та моніторингу ризиків залучення третіх сторін, включаючи процес оперативної ескалації інцидентів.

- Контроль - встановлені керівництвом, періодично оцінювані процеси контролю для зменшення ризиків при залученні третіх сторін.

На додаток до Тематичної Вимоги та цього Посібника, внутрішні аудитори можуть звернутися до додаткових професійних рекомендацій щодо третіх сторін, таких як Глобальні Настанови IPPF та галузеві ресурси.

Рекомендації щодо впровадження

Наступні рекомендації можуть допомогти внутрішнім аудиторам впровадити вимоги, викладені в Тематичній Вимозі щодо Третьої Сторони. Висловлювання в кожному розділі нижче повторюють або перефразовують відповідні вимоги Тематичної Вимоги. Ці необов'язкові рекомендації ілюструють приклади способів оцінки вимог. Внутрішні аудитори повинні застосовувати професійне судження при визначенні того, що включати в свої оцінки.

Рекомендації щодо управління

Щоб оцінити, як процеси управління, включаючи нагляд ради, застосовуються до третіх сторін, внутрішні аудитори можуть проаналізувати наступні докази:

A. Формалізований і задокументований підхід або стратегія, що базується на оцінці ризиків, для визначення необхідності залучення третьої сторони. Підхід періодично переглядається і включає:

- Чітко визначений і стандартизований процес впровадження підходу, затверджений для використання в організації.
- Ресурси закладені в бюджет на основі аналізу витрат і вигід для обґрунтування залучення третьої сторони, забезпечення стратегічного узгодження та ефективності використання ресурсів.
- Оцінку керівництвом ризиків і засобів контролю, в тому числі тих, що стосуються вирішення питань із третіми сторонами.
- Адекватні ресурси для укладання контрактів, управління та моніторингу ефективності роботи третіх сторін.
- Інтеграцію зворотного зв'язку від зацікавлених сторін у підхід або стратегію.

B. Політики, процедури та інша відповідна документація, що використовується для визначення, оцінки та управління відносинами з третіми сторонами протягом життєвого циклу. Політики та процедури можуть включати в себе:

- Стандартизовані інструменти та шаблони для полегшення ключових процесів управління, ризик-менеджменту та контролю.
- Процеси періодичної оцінки політик і процедур, визначення їхньої адекватності та оновлення за необхідності.
- Встановлені критерії відбору, укладання контрактів, початку співпраці, моніторингу та припинення співпраці з третіми сторонами.
- Визначення та періодичний перегляд застосовних регуляторних вимог для узгодження з політиками та процедурами.
- Проведення порівняльного аналізу для визначення та порівняння провідних практик управління стосунками з третіми сторонами.

C. Визначені ролі та обов'язки, які сприяють досягненню цілей взаємодії з третіми сторонами. Інші докази можуть включати:

- Процеси оцінки відповідності цінностей, етики та корпоративної соціальної відповідальності третьої сторони принципам основної організації. Процес повинен передбачати, як оперативно вирішувати потенційні конфлікти інтересів або неетичні практики.
- Регулярне навчання та оцінку компетенцій персоналу, який виконує управління стосунками з третіми сторонами.
- Процес оцінки того, чи було впроваджено навчання для підвищення обізнаності про третіх сторін в масштабах всієї організації.
- Ролі та обов'язки узгоджуються з моделлю «трьох ліній».

D. Своєчасна комунікація та залучення відповідних зацікавлених сторін протягом життєвого циклу взаємодії з третьою стороною (наприклад, рада, вище керівництво, закупівлі, операційна діяльність, управління ризиками, комплаєнс, юристи, інформаційні технології, інформаційна безпека, управління персоналом та інші), що включає в себе:

- Інформацію про ризики третіх сторін та відомі потенційні вразливості в протоколах зустрічей, звітах або електронних листах.
- Обмін інформацією про управління стосунками з третіми сторонами та сприяння співпраці (наприклад, через періодичні зустрічі між підрозділами).

Рекомендації щодо ризик-менеджменту

Щоб оцінити, як процеси управління ризиками застосовуються до цілей взаємодії з третіми сторонами, внутрішні аудитори можуть переглянути наступні докази:

A. Стандартизовані та деталізовані процеси управління ризиками для користувачів послуг третіх сторін включають визначені ролі та обов'язки, і в достатній мірі охоплюють ключові ризики, що стосуються організації:

- Процеси оцінки та управління ризиками третіх сторін включають те, як ключові ризики:
    - Виявляються та звітуються.
    - Аналізуються з метою оцінки їх впливу на здатність досягати цілі організації.
    - Пом'якшуються, включаючи плани дій для зниження ризику до прийнятного рівня.
    - Відстежуються, включаючи виявлення та реагування на ранні попередження, а також план постійного звітування до повного усунення загроз.
- Відстеження (моніторинг) охоплює дотримання процесів та впровадження коригувальних дій для будь-яких відхилень, щоб запобігти підриву довгострокових цілей або стратегії організації.

- Комітет з управління ризиками або інша група здійснює безпосередній нагляд за третіми сторонами та надає інформацію раді. Комітет має чітко визначену мету і регулярно проводить засідання. Доказами роботи можуть бути протоколи засідань.

B. Ризики, пов'язані з третіми сторонами протягом усього життєвого циклу, регулярно виявляються та оцінюються. Оцінка ризиків використовується для ранжування та визначення пріоритетності третіх сторін. Заходи реагування на ризики ранжуються та сортуються за пріоритетністю.

- При розробці оцінки ризиків третіх сторін основна організація враховує такі фактори, як її розмір, зрілість та кількість залучених третіх сторін.
- Оцінка ризиків документується та визначає притаманні та залишкові ризики.
- Організація дотримується процесу належної перевірки для перегляду та оновлення оцінки ризиків.
- Критерії встановлюються для ранжування та визначення пріоритетності третіх сторін відповідно до ризиків. Приклади таких критеріїв включають:
    - Послуги, що надаються, є критично важливими для діяльності організації.
    - Фінансова вартість угоди є суттєвою.
    - Відносини є новими, укладені швидко, та/або їхня тривалість є великою.
    - У цьому процесі беруть участь кілька зовнішніх сторін.
    - Третя сторона планує передати частину або всю роботу субпідряднику.
- Організація дотримується загальноприйнятих практик оцінки ризиків, включаючи те, що оцінка ризиків проводиться на якомога більш ранній стадії, як правило, коли пропозиція аналізується на етапі відбору, а також перед початком дії контракту.
- Постачальники заповнюють анкету для визначення їхнього рейтингу та пріоритетності на основі притаманних їм ризиків. Організація переконується, що анкети заповнюються відповідним персоналом і перевіряються для забезпечення точності.
- Організація отримує періодичну інформацію щодо управління ризиками третіх сторін від таких підрозділів як: інформаційні технології, закупівлі, управління ризиками, управління персоналом, юридичний, комплаєнс, операційний, бухгалтерській облік та фінансовий.

C. Реакції (відповіді) на ризики, такі як пом'якшення, прийняття, усунення та розподіл, визначені та співмірні з рейтингом ризиків.

- Реагування на ризики задокументоване і включає в себе врахування середовища контролю третіх сторін.

- Документація щодо відповідей на ризики, що перевищують ризик-апетит основної організації, перевіряється на відповідність, особливо коли ризики прийняті. Серед відповідей мають бути ті, що стосуються потенційних конфліктів інтересів з третіми сторонами.

D. Процеси управління та ескалації ризиків третіх сторін, включаючи те, як рівень загрози або ризику оцінюється, призначається та сортується за пріоритетністю. Огляд може включати в себе:

- Визначення та пояснення рівнів ризиків організації - таких як високий, помірний та низький - та процедури ескалації для кожної категорії ризиків.
- Перелік третіх сторін, відсортованих за пріоритетністю за виявленими ризиками, та статус зниження ризиків у разі їх виникнення.
- Застосовні правові, регуляторні та комплаєнс-вимоги.
- Вплив ризиків, як фінансових, так і нефінансових (наприклад, репутаційних).
- Процеси інформування керівництва та працівників про ризики, пов'язані з третіми сторонами, включаючи регулярне звітування про профіль ризиків перед радою (або іншим відповідним органом). Повідомлення повинні містити інформацію про усунення будь-яких виявлених проблем з пріоритетними третіми сторонами.
- Процеси переоцінки ранжування та визначення пріоритетності, коли змінюється апетит до ризику та рівень толерантності до ризику основної організації.

Рекомендації щодо процесу контролю

Для того, щоб оцінити, як процеси контролю застосовуються до взаємовідносин із третіми сторонами, внутрішні аудитори можуть здійснювати перевірку доказів того, що:

A. Існує надійний процес належної перевірки для пошуку та відбору третіх сторін із задокументованим та затвердженим бізнес-обґрунтуванням або іншою відповідною документацією, що описує та обґрунтовує необхідність та характер взаємовідносин із третьою стороною.

- В бізнес-обґрунтуванні також слід враховувати наступне:
    - Враховувати ризики щодо здатності третьої сторони відповідати очікуванням, а також потенційний вплив на організацію.
    - Містити детальний аналіз витрат і вигод.
- Дотримуються встановлені процедури відбору постачальників, такі як конкурсні торги, запити на пропозиції та єдиний постачальник. Ці процеси включають:
    - Критерії щодо важливих аспектів, зокрема: перевірка протоколів кібербезпеки, верифікація банківських реквізитів, проведення фінансової перевірки, дослідження організаційної структури третьої сторони, кримінального та юридичного бекграунду, водійських записів, політичної активності та зв’язків із кримінальною діяльністю.

- Чітко визначені критерії відбору, зокрема для оцінки попередньої діяльності, рекомендацій, репутації та вартості контракту.
- Проведення належної перевірки для забезпечення вибору постачальників, наприклад, шляхом формування міжфункціональних команд для розгляду пропозицій. Для зниження ризику упередженості, засоби контролю для груп експертів включають процедури формування таких груп та вимоги щодо розкриття потенційних конфліктів інтересів.
- Проведення належної перевірки контрольного середовища третьої сторони; наприклад, здійснення візиту на місце або перегляд таких документів третьої сторони:
  - Звіти про систему та організаційний контроль (SOC).
  - Фінансова стабільність.
  - Установчі документи або свідоцтво про належний правовий статус.
  - Прозорість у процесі прийняття рішень керівництвом та зацікавленими сторонами.
  - Організаційна структура.
  - Операційна стабільність.
  - Протоколи кібербезпеки.
  - Дотримання відповідних законів, нормативних актів і стандартів.
  - Етичні принципи.
  - Історія взаємодії з основною організацією.
  - Репутація.
- Наявність доказів того, що потенційні постачальники або підрядники переходять до укладання контракту на етапі життєвого циклу лише після проходження відповідних процедур належної перевірки та аналізу їх результатів.

B. Встановлено та дотримуються політики і процедури укладання контрактів.

- Контракти написані з використанням чітких і недвозначних формулювань.
- На етапі підготовки контракту враховуються ключові ризики та включаються відповідні положення. Питання, що потребують вирішення, обговорюються з третьою стороною також на цьому етапі.
- Істотні елементи контрактів визначаються відповідно до політик і процедур укладання контрактів організації та рівня пріоритетності третьої сторони. До таких елементів можуть належати:
  - Угоди про нерозголошення (конфіденційність).
  - Положення про припинення дії контракту та визначені параметри доступу до даних.

- Вимоги до кібербезпеки, включаючи вимоги щодо доступу та обміну всіма даними, а також звітування про інциденти або порушення протягом визначеного періоду.
- Вимоги до повідомлень про порушення, що впливають на дані основної організації.
- Стандартизований процес перевірки ідентифікації третьої сторони, включаючи повну юридичну назву, адресу, фізичне місцезнаходження та веб-сайт. Стандартною практикою є використання контрольного списку під час процесу ідентифікації та перевірка достовірності інформації.
- Чітко визначені угоди про рівень обслуговування (SLA), які встановлюють очікувані результати, права, обов'язки, штрафні санкції, винагороди та відповідальність кожної сторони, включаючи відповідальність за оплату праці (в тому числі субпідрядників нижчого рівня).
- Положення про право на аудит, яке охоплює субпідрядників нижчого рівня, або вимога щодо надання доказів того, що сторони пройшли аудит авторитетного незалежного постачальника послуг з надання впевненості. За відсутності положення про право на проведення аудиту здатність служби внутрішнього аудиту отримувати або надавати впевненість може бути обмеженою.

- Основна організація має доступ до звітів про оцінку контрольного середовища, підготовлених незалежними аудиторами, наприклад, щодо фінансової звітності, комплаєнсу та безпеки даних, таких як Міжнародні стандарти завдань з надання впевненості або звіти SOC.
  - У разі покладання на роботу зовнішніх постачальників послуг з надання впевненості третьої сторони, документи переглядаються для забезпечення їх надійності.
  - Звіти SOC використовуються для виявлення недоліків у процесах управління ризиками та управління змінами.

- Політики і процедури охоплюють будь-які компоненти, що є критично важливими для окремих організацій або типів контрактів:
  - Положення щодо екологічної та соціальної сталості.
  - Протоколи щодо повідомлення про порушення.
  - Вимоги щодо оцінки показників ефективності.
  - Протестований план безперервності бізнесу для третіх сторін.
  - Використання штучного інтелекту в наданні послуг.
  - Чітке визначення, розкриття, умови та обсяг будь-яких субпідрядних робіт нижчого рівня.
  - Процес управління змінами, який визначає порядок внесення змін до обсягу, умов або операційних вимог (наприклад, зміни в технологіях або нормативних актах) протягом строку дії контракту.

- Обмеження щодо кількості змін до замовлень або сум, які можуть бути виставлені до оплати.

- Політики та процедури передбачають формалізоване прийняття кінцевої продукції до здійснення оплати або звільнення від будь-яких утримань.
- Треті сторони зобов'язані надати свої політики етики або кодекс поведінки та/або дотримуватися політик основної організації.
- У випадках, коли контракт надається третьою стороною, основна організація проводить юридичну перевірку, розуміє ключові ризики та забезпечує їх належне управління за допомогою відповідної стратегії зниження ризиків.

C. Фіналізовані контракти або угоди підлягають перегляду та затвердженню відповідними зацікавленими сторонами, включаючи юридичний та комплаєнс-підрозділи, надійно зберігаються та закріплюються за відповідальним менеджером, або адміністратором контракту.

- Контракт або інший офіційний документ, що підтверджує відносини аутсорсингу та зобов'язання третьої сторони, а також докази проведення необхідних юридичних і комплаєнс-перевірок.

D. Ведеться точний, повний та актуальний перелік усіх відносин з третіми сторонами, наприклад, у централізованій системі управління контрактами.

- Процес додавання нових контрактів або угод із третіми сторонами до цього переліку чи системи.
- Процес внесення потенційних третіх сторін до системи постачальників та їх видалення, якщо контракт не затверджено.
- Процес видалення контрактів або угод із третіми сторонами з переліку чи системи.
- Система відстеження для документування проблем із конкретними підрядниками або постачальниками для подальшого використання.
- Процедура перевірки для визначення точності та повноти сукупності третіх сторін.

E. Встановлені та дотримуються задокументовані процеси початку співпраці для забезпечення виконання третіми сторонами умов контракту або угоди. Огляди можуть включати перевірку того, чи:

- Стандартизовані процедури початку співпраці гарантують, що вся необхідна документація, навчання та перевірка на відповідність вимогам буде виконана.
- Системи та процеси третьої сторони можуть легко інтегруватися з технологіями основної організації.
- Спільні системи сумісні та безпечні. Докази можуть включати додаткові засоби контролю суб'єкта користувача як частину звітності SOC.

- Основна організація оцінює плани безперервності бізнесу третьої сторони, які забезпечують безперервність надання послуг під час надзвичайних ситуацій. Плани на випадок непередбачуваних обставин враховують потенційні збої.

F. Впроваджено процеси постійного моніторингу результатів діяльності постачальників щодо цілей контракту або угоди, включаючи оцінку ключових показників ефективності.

- Процеси моніторингу надають інформацію про оцінку ризиків, пов'язаних із третіми сторонами, а виявлені недоліки контролю переглядаються, ескалюються та усуваються за потреби.
- Звіти або спостереження щодо процесів, технологій та інструментів впроваджені для управління процесом моніторингу у реальному часі.
- Встановлені процеси, що забезпечують здійснення платежів відповідно до умов контракту або угоди, зокрема дотримання строків виконання проєкту, проміжних етапів і вимог до комунікації. Платежі здійснюються лише затвердженим підрядникам, з якими почали співпрацю, і які внесені до системи оплати постачальникам. Якщо в контракті зазначені результати, остаточні платежі здійснюються лише після того, як ці результати будуть перевірені.
- Здійснюється моніторинг для контролю витрат, пов'язаних з угодами з третіми сторонами, для забезпечення цінності та визначення рентабельності інвестицій. Результати аналізу витрат і вигод використовуються для перегляду умов контракту.
- Існують процеси оцінки штрафних санкцій за невиконання умов контракту або угоди щодо рівня обслуговування. Штрафи нараховуються та стягуються в момент їх виникнення.
- Рейтинг пріоритезованих третіх сторін на основі оцінки ризиків періодично переглядається, коли в угоду вносяться зміни, а також коли контракт наближається до завершення терміну дії або автоматичного поновлення.
- Здійснюються перевірки пріоритезованих третіх сторін, наприклад, виїзні або щоквартальні бізнес-огляди, для підтвердження засобів контролю та операційної цілісності.
- Докази додаткового постійного моніторингу можуть включати:
    - Аналіз фінансової стабільності третьої сторони.
    - Оцінку скарг на третіх сторін.
    - Аналіз керівництвом звітів незалежного аудитора, підготовлених за Міжнародним стандартом завдань з надання впевненості, Положенням про стандарти завдань з підтвердження достовірності інформації, фінансової, аудиторської звітності, звітності про дотримання вимог та безпеку даних, наданих третіми сторонами; сертифікація за стандартом ISO.
    - Аналіз керівництвом тестів на стійкість бізнесу, проведених третьою стороною, включаючи будь-які виявлені суттєві проблеми.

- Умови та обмеження щодо залучення субпідрядників або сторін нижчого рівня.
- Оцінку етичних цінностей, культури та поведінки третіх сторін.
- Відповіді на запити ЗМІ.
- Оцінку протоколів конфіденційності та кібербезпеки для захисту зберігання та передачі даних та інформації основної організації, включаючи використання сучасних технологій, таких як штучний інтелект.
- Виявлення організацією можливостей для постійного покращення результатів діяльності та досягнення цілей контракту або угоди.
- Перегляд розподілу обов'язків.

G. Впроваджено протоколи для ініціювання коригувальних дій щодо виявлених інцидентів у разі невиконання третьою стороною вимог контракту або угоди, або якщо дії третьої сторони підвищують ризик для основної організації.

- Впроваджено протоколи ескалації інцидентів на основі серйозності інциденту та пріоритетності третьої сторони.
- Аналіз інциденту після його усунення, включаючи аналіз першопричин.

H. Процеси для надання сповіщень про контракти та угоди, термін дії яких наближається до завершення або автоматичного поновлення. Процеси автоматичного поновлення включають перегляд:

- Ефективності третьої сторони.
- Умов контракту або угоди та будь-яких доповнень.
- Факторів ризику.

I. Впроваджено та дотримується формалізований план закінчення співпраці для забезпечення належного виконання вимог контракту щодо строків і очікувань, у тому числі для субпідрядників нижчого рівня.

- Контрольні списки або інтерв'ю з ключовими зацікавленими сторонами, щоб переконатися, що заходи безпеки є ефективними.
- Організаційна інформація або дані, що перебувають у володінні третьої сторони, були повернуті або знищені.
- Доступ третьої сторони до даних, систем, приміщень та інших об’єктів організації було відкликано.
- Активи первинної організації, такі як пристрої, ліцензії на програмне забезпечення, інтелектуальна власність та документація, були повернуті.
- У разі розірвання контракту з третьою стороною з обґрунтованої причини, обставини або ризики, що виникли, ідентифікуються та ескалюються до вищого керівництва та/або ради.

- У разі розірвання контракту з пріоритезованою третьою стороною, заміна здійснюється на основі тієї ж оцінки ризиків, допоки контракт буде завершено або він більше не буде потрібен.

Додаток А. Приклади практичного застосування

Наступні приклади описують сценарії, в яких може застосовуватися Тематична Вимога щодо Третьої Сторони:

Приклад 1: Завдання з внутрішнього аудиту в плані внутрішнього аудиту включає послугу або результат виконаних робіт, які наразі надаються третьою стороною.

Коли служба внутрішнього аудиту завершує процес планування на основі оцінки ризиків і включає до плану внутрішнього аудиту одне або декілька завдань стосовно надання послуг або виконання робіт, які наразі надаються третіми сторонами за контрактом або угодою, то Тематична Вимога є обов'язковою для виконання.

Не кожна вимога в Тематичній Вимозі може бути застосована до кожного аудиторського завдання. Коли внутрішні аудитори застосовують професійне судження і визначають, що одна або більше вимог Тематичної Вимоги щодо Третьої Сторони не застосовуються і тому повинні бути виключені із аудиторського завдання, внутрішні аудитори повинні задокументувати і зберігати обґрунтування для виключення цих вимог. Наприклад, обґрунтуванням для виключення певних вимог може бути те, що служба внутрішнього аудиту встановила, що залежність організації від третіх сторін у наданні критично важливих для місії послуг є низькою, або що це усталені відносини з низьким фінансовим впливом.

Приклад 2: Ризики, пов'язані з третіми сторонами, визначаються під час виконання завдання з надання впевненості на тему, що не стосується третіх сторін або управління контрактами.

Внутрішні аудитори можуть виявити значний ризик третіх сторін під час оцінки процесу, який спочатку не був пов'язаний з третіми сторонами або управлінням контрактами. Наприклад, плануючи аудиторське завдання з оцінки зберігання даних, внутрішні аудитори дізнаються, що хмарні сервіси розміщуються в третьої сторони. Під час інтерв'ю з керівництвом третьої сторони, яка надає послуги, внутрішні аудитори виявляють ризики кібербезпеки, пов'язані з третьою стороною.

Після виявлення відповідних ризиків внутрішні аудитори повинні переглянути Тематичну Вимогу щодо Третьої Сторони та Тематичну Вимогу з Кібербезпеки і визначити, які з них застосовні. Аудитори можуть виключити процес управління або ризик-менеджменту щодо взаємодії з третьою стороною з обсягу аудиторських завдань і зосередитися на контролях такої взаємодії за послугами, що перевіряються в рамках аудиту. Таке ж професійне судження застосовується і до застосування Тематичної Вимоги з Кібербезпеки. Аудитори повинні задокументувати в робочих документах аудиторського завдання обґрунтування виключення будь-яких вимог Тематичної Вимоги щодо Третьої Сторони або Тематичної Вимоги з Кібербезпеки та зберігати цю документацію.

Приклад 3: Потреба в аудиторському завданні щодо третьої сторони, яке не було спочатку включене до плану внутрішнього аудиту.

В організації виникає проблема, пов'язана з пріоритетною третьою стороною, яка потребує негайної уваги з боку служби внутрішнього аудиту. Проблема мала відношення до збою контролю. Керівник служби внутрішнього аудиту повинен спілкуватися з радою про зміну пріоритетів плану аудиту та ресурсів служби внутрішнього аудиту, щоб задовольнити цю потребу. Аудитор повинен залучити відповідне керівництво, щоб розробити цілі аудиторського завдання для оцінки ситуації та надати рекомендації для запобігання подібним випадкам у майбутньому. Керівник служби внутрішнього аудиту повинен проаналізувати Тематичну Вимогу для визначення обсягу аудиторського завдання, визначити, які вимоги застосовуються, та задокументувати будь-які винятки відповідним чином.

Додаток Б. Додатковий інструмент документування

Очікується, що внутрішні аудитори застосовуватимуть професійне судження при визначенні застосовності вимог на основі оцінки ризиків та належним чином документуватимуть винятки з певних вимог. Тематична Вимога може бути задокументована в плані внутрішнього аудиту або в робочих документах завдання на основі професійного судження аудитора. Одне або декілька аудиторських завдань можуть покривати вимоги. Крім того, не всі вимоги можуть бути застосовані. Наведена нижче форма для друку надає один з варіантів документування відповідності Тематичній Вимозі щодо Третьої Сторони, але її використання не є обов'язковим.

Треті Сторони - Управління

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
A. Встановлюється, впроваджується та періодично переглядається формальний підхід для визначення того, чи варто залучати третю сторону. Такий підхід включає відповідні критерії для визначення та оцінки необхідних і наявних ресурсів для досягнення цілей шляхом надання продукту або послуги.		
B. Політики та процедури встановлюються для визначення, оцінки та управління відносинами та ризиками з третіми сторонами протягом усього життєвого циклу взаємодії з третьою стороною. Політики та процедури узгоджуються з чинними нормативно-правовими вимогами та періодично переглядаються й оновлюються з метою посилення контрольного середовища.		

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
C. Визначено ролі та обов'язки організації щодо управління взаємодією з третіми сторонами, де детально описано, хто обирає, спрямовує, управляє, здійснює комунікації та контролює відносини з третіми сторонами, а також, хто має бути проінформований про діяльність третіх сторін. Існує процес, який забезпечує наявність відповідних компетенцій у осіб, призначених для виконання ролей та обов'язків у сфері управління третіми сторонами.		
D. Визначено протоколи комунікації з відповідними зацікавленими сторонами, які передбачають своєчасне звітування про стан виконання, ризики та дотримання вимог (зокрема, порушення законів та нормативних актів) пріоритетними третіми сторонами. Пріоритетність третіх сторін визначається на основі ризику. До відповідних зацікавлених сторін можуть належати: рада, вище керівництво, а також наступні підрозділи: закупівлі, операційна діяльність, управління ризиками, комплаєнс, юридичний, інформаційні технології, інформаційна безпека, управління персоналом та інші.		

Треті Сторони - Ризик-менеджмент

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
A. Процеси управління ризиками третіх сторін та їхніх послуг є стандартизованими та комплексними, включають визначені ролі та обов'язки, а також достатньою мірою враховують ключові ризики, що стосуються організації (такі як стратегічні, репутаційні, етичні, операційні, фінансові, комплаєнс, кібербезпекові, інформаційно-технологічні, юридичні, сталого розвитку та геополітичні). Дотримання процесів відслідковується, а за будь-яких відхилень впроваджуються коригувальні дії.		
B. Ризики, пов'язані з третіми сторонами протягом усього життєвого циклу, регулярно виявляються та оцінюються. Оцінка ризиків використовується для ранжування та визначення пріоритетності третіх сторін, у тому числі їх субпідрядників нижчого рівня. Також ранжуються та сортуються за пріоритетністю заходи реагування на ризики. Оцінка ризиків періодично переглядається та оновлюється.		
C. Заходи реагування на ризики є адекватними і точними, відповідно до рейтингу. Заходи реагування впроваджуються, переглядаються, затверджуються, контролюються, оцінюються та коригуються за потреби.		

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
D. Існують процеси для управління та ескалації, за необхідності, питань, які виникають з боку третіх сторін, що забезпечує відповідальність за результати та підвищує ймовірність виконання умов контрактів або інших угод. Якщо третя сторона не реагує на ескальоване питання, існують процеси, що дозволяють керівництву оцінити ризики поточних ділових відносин і вжити подальші заходи, виправлення ситуації або розірвання відносин, якщо це виправдано.		

Треті Сторони – Процеси Контролю

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
A. Існує надійний процес належної перевірки для пошуку та відбору третіх сторін із задокументованим та затвердженим бізнес-обґрунтуванням або іншим відповідним документом, що описує та обґрунтовує необхідність та характер відносин з третьою стороною.		
B. Процеси укладення контрактів та їх затвердження здійснюються відповідно до політик і процедур управління ризиками третіх сторін, прийнятих в організації, та передбачають співпрацю між відповідними підрозділами організації.		

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
C. Остаточні контракти або угоди переглядаються та затверджуються всіма відповідними зацікавленими сторонами, включаючи юридичний підрозділ та підрозділ комплаєнсу, підписуються уповноваженими особами з обох сторін та надійно зберігаються. За кожним контрактом закріплена відповідальна особа — менеджер або адміністратор.		
D. Ведеться точний, повний та актуальний перелік усіх відносин з третіми сторонами, наприклад, у централізованій системі управління контрактами.		
E. Задокументовані процеси початку співпраці встановлюються і дотримуються, щоб створити основу для виконання третіми сторонами умов контракту або угоди.		
F. Існують процеси постійного моніторингу, які дозволяють оцінити, чи виконують треті сторони умови контракту або угоди протягом усього життєвого циклу співпраці, а також чи виконують вони свої договірні зобов'язання. Процеси включають перевірку достовірності наданої інформації та періодичну переоцінку результатів діяльності, зокрема у випадках змін умов контракту.		
G. Протоколи встановлюються для ініціювання коригувальних дій, якщо третя сторона не відповідає очікуванням або становить підвищений чи неочікуваний ризик. Протоколи передбачають ескалацію інцидентів за ступенем серйозності, проведення аналізу після інцидентів та аналіз першопричин інцидентів.		

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
H. Відстежуються дати закінчення та поновлення контрактів, і за необхідності, вживаються заходи щодо їх поновлення.		
I. Впроваджується і дотримується формалізований план завершення співпраці, щоб забезпечити належне виконання вимог контракту щодо термінів та очікувань. Процеси включають дії щодо: • Припинення співпраці з третьою стороною. • Заміни третьої сторони у разі потреби. • Перепризначення обов'язків зі зберігання, повернення або знищення конфіденційних даних організації, що зберігаються у третьої сторони. • Відкликання доступу третьої сторони до систем, інструментів, приміщень та інших об'єктів організації.		

Про Інститут внутрішніх аудиторів

Інститут Внутрішніх Аудиторів (**The Institute of Internal Auditors, IIA**) - це міжнародна професійна асоціація, яка обслуговує понад 265 000 членів по всьому світу і яка видала понад 200 000 сертифікатів Certified Internal Auditor® (CIA®) по всьому світу. Заснований в 1941 році, Глобальний Інститут Внутрішніх Аудиторів визнаний в усьому світі як лідер у сфері стандартів, сертифікації, освіти, досліджень і технічного керівництва в галузі внутрішнього аудиту. Для отримання додаткової інформації відвідайте theiia.org.

Відмова від відповідальності

IIA публікує цей документ з інформаційною та освітньою метою. Цей матеріал не має на меті дати вичерпні відповіді на конкретні індивідуальні обставини і тому може бути використаний лише як орієнтир. IIA рекомендує звертатися за порадою до незалежних експертів, які мають безпосереднє відношення до будь-якої конкретної ситуації. IIA не несе відповідальності за те, що хтось покладається виключно на цей матеріал.

Авторське право

Вересень 2025 року

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