Взаимоотношения с третьими сторонами

Тематические требования

Руководство пользователя

Topical Requirement

The Institute of
Internal Auditors

Содержание

Обзор Тематических требований

Тематические требования являются важнейшим компонентом Международных основ профессиональной практики (The International Professional Practices Framework®), наряду с Международными стандартами внутреннего аудита (Global Internal Audit Standards™) и Международным руководством. Международный институт внутренних аудиторов (The Institute of Internal Auditors, IIA) требует, чтобы Тематические требования использовались в сочетании со Стандартами, которые являются надежной основой требуемой практики. Ссылки на Стандарты приводятся в этом руководстве в качестве источника более подробной информации.

Тематические требования определяют то, как внутренние аудиторы рассматривают распространенные области риска, и тем самым способствуют систематизации и повышению качества услуг внутреннего аудита. Тематические требования устанавливают минимальный уровень требований и предоставляют соответствующие критерии для оказания услуг по обеспечению уверенности, относящихся к предмету Тематических требований (Стандарт 13.4 «Критерии оценки»). Соответствие Тематическим требованиям является обязательным при оказании услуг по обеспечению уверенности и рекомендуемым для осуществления оценки при оказании консультационных услуг. Тематические требования не охватывают все потенциальные аспекты, которые следует учитывать при выполнении аудиторских заданий по обеспечению уверенности, а предоставляют минимальный набор требований для проведения надежной оценки в соответствующей области.

Тематические требования прямо связаны с Моделью трех линий (IIA) и Международными стандартами внутреннего аудита. Процессы руководства организацией, управления рисками и внутреннего контроля являются основными компонентами Тематических требований, соответствующих Стандарту 9.1 "Понимание процессов руководства организацией, управления рисками и внутреннего контроля". В соответствии с Моделью трех линий, процесс руководства организацией связан с Советом/ наблюдательным органом, управление рисками – со второй линией, а внутренний контроль или процессы контроля – с первой линией. Менеджмент представлен на первой и второй линиях, а функция внутреннего аудита находится на третьей линии как независимая и объективная сторона, предоставляющая уверенность, подотчетная Совету/ наблюдательному органу (Принцип 8 "Осуществление надзора со стороны Совета").

Применимость, риск и профессиональное суждение

Тематические требования должны применяться, когда функции внутреннего аудита выполняют задания по обеспечению уверенности в области Тематических требования или когда аспекты Тематических требований выявлены в рамках других аудиторских заданий по обеспечению уверенности.

Как описано в Стандартах, оценка рисков является важной частью планирования, выполняемого руководителем внутреннего аудита. Для определения заданий по обеспечению уверенности, которые должны быть включены в план работы внутреннего аудита, необходимо не реже одного раза в год проводить оценку стратегий, целей и рисков организации (Стандарт 9.4 «План внутреннего аудита»). При планировании отдельных аудиторских заданий по обеспечению уверенности внутренние аудиторы должны оценить риски, относящиеся к заданию (Стандарт 13.2 «Оценка рисков в рамках аудиторского задания»).

Если область Тематических требований определена в процессе риск ориентированного планирования и включена в план аудита, то требования, изложенные в Тематических требованиях, должны быть использованы для оценки данной области в рамках соответствующих аудиторских заданий. Кроме того, когда внутренние аудиторы выполняют аудиторское задание (включенное или не включенное в план) и выявляют аспекты Тематических требований, должна быть проведена оценка применимости Тематических требований в рамках выполнения аудиторского задания. Если имеется запрос на выполнение аудиторского задания, которое изначально не было включено в план и которое содержит область Тематических требований, то необходимо оценить применимость Тематических требований для его выполнения.

Профессиональное суждение играет ключевую роль в применении Тематических требований. Оценка рисков определяет решения руководителей внутреннего аудита в отношении того, какие аудиторские задания включить в план внутреннего аудита (Стандарт 9.4). Кроме того, внутренние аудиторы используют профессиональное суждение, чтобы определить, какие аспекты будут охвачены в рамках каждого аудиторского задания (Стандарты 13.3 "Цели и объем аудиторского задания", 13.4 "Критерии оценки" и 13.6 " Программа задания").

.Необходимо сохранить доказательства того, что все требования Тематических требований были оценены на предмет применимости, включая обоснование исключения каких-либо требований. Соответствие Тематическим требованиям должно документироваться с использованием профессионального суждения аудитора, как описано в Стандарте 14.6 "Документация аудиторского задания".

В то время как Тематические требованиям предоставляют минимальный требуемый набор процессов контроля, которые необходимо рассмотреть, организациям, оценивающим риски в области взаимоотношений с третьими сторонами как очень высокие, может потребоваться оценка дополнительных аспектов.

Если функция внутреннего аудита не обладает необходимыми компетенциями для выполнения аудиторских заданий в области Тематических требований, руководитель внутреннего аудита должен определить, как получить необходимые ресурсы, и своевременно сообщить Совету и высшему исполнительному руководству о влиянии ограничений и о том, как будет решаться проблема нехватки ресурсов. Руководитель внутреннего аудита несет полную ответственность за обеспечение соответствия функции внутреннего аудита Тематическим требованиям, независимо от того, каким образом были получены ресурсы (Стандарты 3.1 «Компетентность», 7.2 «Квалификация руководителя внутреннего аудита», 8.2 «Ресурсы», 10.2 «Управление кадровыми ресурсами»).

Выполнение, документирование и подготовка отчетности

Применяя Тематические требования, внутренние аудиторы также должны соответствовать Стандартам, проводя свою работу в соответствии с Разделом V: Предоставление услуг внутреннего аудита. В стандартах Раздела V описаны процессы планирования аудиторских заданий (Принцип 13 "Осуществляйте эффективное планирование аудиторских заданий"), выполнения аудиторских заданий (Принцип 14 "Выполняйте аудиторское задание") и информирования о результатах аудиторского задания (Принцип 15 "Информируйте о результатах аудиторского задания и осуществляйте мониторинг планов мероприятий").

Тематические требования разработаны для поддержки последовательной и качественной практики внутреннего аудита. Местные законы, нормативные акты, требования надзорных органов и другие профессионально признанные концепции могут устанавливать дополнительные или более детальные требования. Внутренние аудиторы должны понимать и соблюдать законы и/или нормативные акты, относящиеся к отрасли и юрисдикции, в которой работает организация, включая раскрытие информации в соответствии с требованиями Стандарта 1.3 "Правовые вопросы и этическое поведение". Внутренние аудиторы, возможно, уже включили эти дополнительные требования в программы аудита и процедуры тестирования и должны сопоставить их с Тематическими требованиями, чтобы обеспечить достаточный охват.

Охват Тематических требований может документироваться либо в плане внутреннего аудита, либо в рабочей документации аудиторского задания на основе профессионального суждения аудиторов. Одно или несколько аудиторских заданий могут обеспечивать охват всех требований. Кроме того, не все требования могут быть применимы. Необходимо сохранить доказательства того, что Тематические требования были оценены на предмет применимости, включая обоснования, объясняющие любые исключения.

Обеспечение качества

Согласно Стандартам руководитель внутреннего аудита должен разработать, внедрить и поддерживать программу обеспечения и повышения качества, охватывающую все аспекты функции внутреннего аудита (Стандарт 8.3 "Качество"). Результаты должны быть доведены до сведения Совета и высшего исполнительного руководства. В этих сообщениях должны содержаться сведения о соответствии функции внутреннего аудита Стандартам и достижении целевых параметров деятельности.

Соответствие Тематическим требованиям будет оцениваться при проведении оценок качества.

Третьи стороны

Третья сторона – это внешнее лицо, группа или организация, с которой организация ("основная организация") устанавливает деловые взаимоотношения для получения продуктов или услуг. Отношения могут быть оформлены договором, соглашением или другими способами для обеспечения основной организации продуктами, услугами, рабочей силой, производственными возможностями или решениями в области информационных технологий, таких как хранение, обработка и обслуживание данных.

> Примечание
>
> В Тематических требованиях используется общая терминология внутреннего аудита, определенная в Международных стандартах внутреннего аудита. Читателям следует обратиться к терминам и определениям, приведенным в глоссарии Стандартов.

Термин "третья сторона" может использоваться по-разному в зависимости от отрасли или других обстоятельств. Каждая функция внутреннего аудита имеет возможность действовать гибко, используя свое суждение при применении Тематических требований в зависимости от того, как основная организация (организация, заключающая соглашение с третьей стороной) определяет третьи стороны. В Тематических требованиях "Взаимоотношения с третьими сторонами" и руководстве пользователя термин "третья сторона" используется для обозначения поставщиков, подрядчиков, субподрядчиков, аутсорсинговых поставщиков услуг, других организаций и консультантов. Термин "третья сторона" охватывает все подобные договоренности, включая договоренности между третьей стороной и ее субподрядчиками, часто называемыми "последующими" субподрядчиками или "четвертыми сторонами", "пятыми сторонами" или "Н-ыми сторонами".

Данные Тематические требования не предназначены для рассмотрения сторонних взаимоотношений, интересов или связей основной организации с регулирующими органами, представителями организации (агентами), брокерами, инвесторами, попечителями/членами Совета, государственными службами и представителями общественности, или внутренних взаимоотношений с сотрудниками основной организации или поставщиками услуг внутри группы.

Термин "третья сторона" может определяться и использоваться по-разному в зависимости от отрасли или других обстоятельств. Внутренние аудиторы могут действовать гибко и полагаться на свое профессиональное суждение, адаптируя Тематические требования к определению третьей стороны, принятому в основной организации.

Эффективность процессов организации по управлению взаимоотношениями с третьими сторонами может быть оценена в рамках всей организации и/или на уровне одного или нескольких отдельных договоров, соглашений. Внутренним аудиторам следует использовать подход "сверху вниз", чтобы получить представление о политике, процедурах, процессах, моделях/ концепциях и жизненном цикле взаимоотношений с третьими сторонами. Внутренним аудиторам следует использовать суждение, чтобы понять нюансы рисков третьих сторон в зависимости от отрасли, организации и темы аудиторского задания. В соответствии со Стандартом 5.1 "Использование информации", внутренние аудиторы должны знать и соблюдать все политики и процедуры, связанные с информацией третьих сторон, к которой они могут получить доступ.

Тематические требования применяются, когда функция внутреннего аудита выполняет аудиторские задания по обеспечению уверенности в отношении взаимодействия с третьими сторонами и/или любыми субподрядными взаимоотношениями, включая четвертые или последующие, разрешенными договором или соглашением основной организации и третьей стороны. Внутренним аудиторам следует приоритизировать третьи и “последующие стороны” (субподрядчиков) на основе оценки рисков, как описано в разделе "Управление рисками" ниже. Внутренние аудиторы должны применять все требования в соответствии с результатами оценки рисков, а исключения должны быть документироваться.

Тематические требования "Взаимоотношения с третьими сторонами" и руководство пользователя относятся к этапам взаимоотношений организации с третьими сторонами, также известным как этапы жизненного цикла: выбор подрядчика, заключение договора, адаптация , мониторинг и прекращение работы с подрядчиком. Эти этапы будут использоваться для целей Тематических требований «Взаимоотношения с третьими сторонами» и руководства пользователя, даже если в некоторых отраслях существуют свои собственные версии жизненного цикла. Этапы:

- Выбор подрядчика: включает процесс определения потребности в третьей стороне, план по ее привлечению и применение принципа должной осмотрительности (due diligence) при выборе. Кроме того, выбор должен включать оценку рисков потенциальных и привлеченных третьих сторон.
- Заключение договора: включает в себя применение принципа должной осмотрительности (due diligence) для составления проекта договора, ведения переговоров, утверждения и реализации юридического соглашения с третьей стороной.
- Адаптация: начинается с момента подписания договора, что дает старт взаимоотношениям и закладывает основу для выполнения третьими сторонами условий договора или соглашения.
- Мониторинг: включает в себя процессы управления в течение всего периода взаимоотношений и постоянного мониторинга третьей стороны основной организацией после согласования договора. Подход обычно является систематическим, основанным на оценке рисков и должен предусматривать постоянное совершенствование. Мониторинг включает в себя продление текущих договоров или соглашений с третьими сторонами, когда это необходимо.
- Прекращение работы: включает в себя процессы завершения исполнения договоров и соглашений, определения стратегии отказа от работы с третьими сторонами, которые были приоритизированы с учетом риска, и прекращение взаимоотношений в случае необходимости. В этих процессах обычно используется подход, основанный на оценке рисков, и может быть предусмотрен формализованный регламент отказа от работы с третьей стороной.

Основная организация сохраняет за собой ответственность за риски, связанные с достижением ее целей, даже если она привлекает третью сторону для помощи в достижении одной или нескольких целей. Привлечение третьих сторон может снизить некоторые затраты организации на выполнение процессов. Однако это может привести к возникновению операционных рисков, поскольку

основная организация в меньшей степени осведомлена и обладает меньшими полномочиями в отношении процессов контроля третьей стороны . Если третья сторона не выполняет условия договора, участвует в неэтичных действиях или испытывает сбои в своей деятельности, это может привести к последствиям для основной организации.

Основная организация должна выявлять, оценивать риски и управлять ими с помощью соответствующих процессов руководства организацией, управления рисками и внутреннего контроля. Категории и примеры рисков, связанных с третьими сторонами, включают:

- Стратегические, такие как способность основной организации выполнять свою миссию и/или достигать верхнеуровневых целей или управлять последствиями слияний и поглощений.
- Репутационные, такие как ущерб, нанесенный окружающей среде или отношениям и доверию основной организации с клиентами, заказчиками и заинтересованными сторонами.
- Этические, такие как нарушения приверженности этическим принципам, конфликты интересов, коммерческие подкупы (откаты) и коррупция.
- Операционные, такие как физическая и информационная безопасность, инсайдерский риск, сбои в работе сервисов и недостижение поставленных целей.
- Финансовые, такие как неплатежеспособность третьих сторон и мошенничество.
- Риски комплаенс - несоблюдение применимых местных, национальных и международных нормативных требований.
- Риски кибербезопасности и других видов защиты данных, таких как компрометация и утечка конфиденциальных данных.
- Риски информационных технологий, например, отсутствие сервисов для поддержки критически важных операций.
- Юридические, такие как конфликты интересов, споры и судебные разбирательства в связи с нарушением договоров.
- Риски устойчивого развития, такие как ESG риски. Примерами могут служить риски, связанные с воздействием организации на окружающую среду, и риски, касающиеся взаимодействия организации с сообществами.
- Геополитические, такие как торговые споры/санкции и политическая нестабильность.

Внутренним аудиторам следует учитывать каждый этап жизненного цикла взаимоотношений с третьей стороны при оценке требований к процессам руководства организацией, управления рисками и внутреннего контроля.

Требования, содержащиеся в Тематических требованиях «Взаимоотношения с третьими сторонами», разделены на три раздела в соответствии со Стандартом 9.1 "Понимание процессов руководства организацией, управления рисками и внутреннего контроля":

- Руководство организацией - четко определенные базовые цели и стратегии использования третьих сторон для поддержки целей, политики и процедур основной организации.
- Управление рисками - процессы выявления, анализа, управления и мониторинга рисков, связанных с использованием третьих сторон, включая процесс оперативной передачи инцидентов на более высокий уровень рассмотрения.
- Внутренний контроль - установленные менеджментом и периодически оцениваемые процессы контроля для снижения рисков при использовании третьих сторон.

В дополнение к Тематическим требованиям и данному руководству пользователя внутренние аудиторы могут обратиться к дополнительным профессиональным рекомендациям по взаимоотношениям с третьими сторонами, таким как Международное руководство Международных основ профессиональной практики и ресурсы, посвященные конкретной отрасли.

Рекомендации

Следующие рекомендации могут помочь внутренним аудиторам в реализации норм, содержащихся в Тематических требованиях «Взаимоотношения с третьими сторонами». Буквенные обозначения в каждом разделе ниже повторяют или перефразируют соответствующие нормы Тематических требований. Эти необязательные рекомендации носят иллюстративный характер и служат примером того, как можно оценить требования. Внутренним аудиторам следует применять профессиональное суждение при определении того, что включать в свои аудиторские задания.

Рекомендации по оценке процесса руководства организацией

Для оценки того, как процессы руководства организацией, включая надзор со стороны Совета, применяются для достижения целей взаимоотношений с третьими сторонами, внутренние аудиторы могут изучить доказательства:

A. Формализованного и документированного подхода или стратегии, основанных на оценке рисков, для определения необходимости использования третьей стороны. Подход периодически пересматривается и включает в себя:
   - Четко определенный, стандартизированный и утвержденный организацией процесс его внедрения.
   - Бюджетирование ресурсов на основе анализа затрат и выгод для обоснования привлечения третьей стороны, обеспечения стратегической согласованности и эффективности использования ресурсов.
   - Оценки менеджментом рисков и средств внутреннего контроля, включая те, которые касаются вопросов взаимодействия с третьими сторонами.
   - Наличие достаточных ресурсов для заключения договоров, управления и мониторинга работы третьих сторон.
   - Интеграцию в используемый подход или стратегию обратной связи от заинтересованных сторон.

B. Политик, процедур и другой соответствующей документации, используемой для выбора, оценки и управления взаимоотношениями с третьими сторонами на протяжении всего их жизненного цикла. Политики и процедуры могут включать в себя:
   - Стандартизированные инструменты и шаблоны для поддержания ключевых процессов руководства организацией, внутреннего контроля и управления рисками.
   - Процессы периодической оценки политик и процедур, определения их адекватности и обновления по мере необходимости.
   - Установление критериев выбора третьих сторон, заключения с ними договоров, адаптации, мониторинга и прекращения работы с третьими сторонами.

- Определение и периодический анализ применимых нормативных требований на предмет соответствия политикам и процедурам.
- Проведение бенчмаркинга для выявления ведущих практик управления взаимоотношениями с третьими сторонами.

C. Определение ролей и обязанностей, способствующих достижению целей взаимоотношений с третьими сторонами. Дополнительные подтверждения могут включать:

- Процессы оценки соответствия ценностей, этики и корпоративной социальной ответственности третьей стороны принципам основной организации. Процессы, которые должны предусматривать оперативное устранение потенциальных конфликтов интересов или неэтичной практики.
- Регулярное обучение персонала, выполняющего функции управления взаимоотношениями с третьими сторонами, и периодическую оценку его компетентности.
- Процесс оценки того, проводилось ли обучение для повышения осведомленности всей организации о взаимодействии с третьими сторонами.
- Роли и обязанности приведены в соответствие с принципами Модели трех линий.

D. Своевременная коммуникация и взаимодействие с соответствующими заинтересованными сторонами (например, Советом, высшим исполнительным руководством, отделом закупок, операционными подразделениями, отделом управления рисками, отделом комплаенс, юридической службой, отделом ИТ, отделом информационной безопасности, отделом кадров и другими) на протяжении всего жизненного цикла взаимоотношений с третьими сторонами, что включает:

- Информацию о рисках третьих сторон и известных потенциальных уязвимостях, которая отражена в протоколах совещаний, отчетах или электронных письмах.
- Обмен информацией о взаимоотношениях с третьими сторонами и поощрение сотрудничества (например, путем проведения периодических межфункциональных встреч).

Рекомендации по оценке управления рисками

Для оценки того, как процессы управления рисками применяются для достижения целей взаимоотношений с третьими сторонами, внутренние аудиторы могут изучить доказательства того, что:

A. Стандартизированные и комплексные процессы управления рисками для пользователей услуг третьих сторон включают в себя определенные роли и обязанности и в достаточной степени учитывают ключевые риски, относящиеся к основной организации:

- Процессы оценки и управления рисками взаимоотношений с третьими сторонами включают в себя то, как ключевые риски:
  - Изначально выявляются и отражаются в отчетности

- Анализируются для оценки их влияния на способность достигать целей основной организации
- Снижаются, включая планы действий по снижению риска до приемлемого уровня.
- Мониторятся, включая обнаружение и реагирование на ранние предупреждения, а также план постоянной отчетности до полного устранения угроз.

- Мониторинг осуществляется на предмет соблюдения процессов и выполнения корректирующих действий при любых отклонениях, чтобы не допустить неисполнения долгосрочных целей или стратегии основной организации.
- Комитет по управлению рисками или другая группа осуществляет прямой надзор за рисками, связанными с третьими сторонами, и предоставляет информацию Совету. У комитета определены цели, и он регулярно проводит свои заседания. В качестве доказательств можно использовать протоколы заседаний.

B. Риски, связанные с третьими сторонами, на протяжении всего жизненного цикла регулярно выявляются и оцениваются. В ходе оценки рисков третьи стороны ранжируются и приоритизируются. Меры реагирования на риски ранжируются и приоритизируются.

- При оценке рисков третьих сторон основная организация учитывает такие факторы, как размер, степень зрелости и количество привлеченных третьих сторон.
- Оценка рисков определяет присущие и остаточные риски и документируется.
- Организация применяет принцип должной осмотрительности (due diligence) для пересмотра и обновления результатов оценки рисков.
- Устанавливаются критерии для ранжирования и приоритизирования третьих сторон в соответствии с рисками. Примеры таких критериев включают:
  - Предоставляемые услуги имеют критически важное значение для деятельности организации.
  - Финансовая стоимость соглашения является существенной.
  - Отношения новые, возникли быстро, и/или их продолжительность велика.
  - В процессе участвуют несколько сторонних организаций.
  - Третья сторона планирует передать часть или всю работу на субподряд.
- Организация придерживается общепринятой практики оценки рисков, включая оценку рисков на самом раннем этапе, как правило при анализе предложения на этапе отбора, и перед адаптацией.
- Поставщики заполняют анкету, чтобы определить их рейтинг и приоритетность на основе присущих рисков. Организация обеспечивает, что анкеты заполняются соответствующим персоналом и проверяются на предмет точности.
- Организация периодически получает информацию об управлении рисками, связанными с третьими сторонами, от функциональных подразделений, таких как отдел ИТ, отдел закупок, отдел управления рисками, отдел кадров, юридический

отдел, отдел комплаенс, операционные подразделения, бухгалтерия и финансовый отдел.

C. Определяются меры реагирования на риск, такие как снижение, принятие, устранение и передача, которые соответствуют рейтингу риска.

- Ответы на риски документируются и включают рассмотрение контрольной среды третьей стороны.
- Документация, подтверждающая, что реакция на риски, превышающие допустимый уровень риска основной организации, проверяется на предмет целесообразности, особенно если риски принимаются. Выявляются ситуации, которые касаются потенциального конфликта интересов во взаимоотношениях с третьими сторонами.

D. Процессы управления и передачи на более высокий уровень рассмотрения рисков, связанных с третьими сторонами, включая то, как оценивается, назначается и приоритизируется уровень угрозы или риска. Оценка может включать определение/идентификацию:

- Определения и объяснения уровней риска организации - например, высокого, умеренного и низкого - и процедуры передачи на более высокий уровень рассмотрения для каждой категории риска.
- Списка третьих сторон, приоритизированных на основе выявленных рисков, и статус снижения последствий любых событий, связанных с рисками.
- Применимых юридических и нормативных требований.
- Последствий рисков, как финансовых, так и нефинансовых (например, репутация).
- Процессов информирования руководства и сотрудников о рисках третьих лиц, включая регулярное представление результатов оценки рисков Совету (или другому соответствующему органу). Информационных сообщений, включающих обновленную информацию об устранении любых проблемных вопросов, отмеченных в отношении приоритетных третьих сторон.
- Процессов переоценки ранжирования и приоритизирования при изменении риск-аппетита и уровня допустимого риска основной организации.

Рекомендации по оценке внутреннего контроля

Для оценки того, как процессы внутреннего контроля применяются к взаимоотношениям с третьими сторонами, внутренние аудиторы могут изучить подтверждения того, что:

A. При поиске и выборе третьих сторон применяется принцип должной осмотрительности (due diligence) с подготовкой документированного и утвержденного экономического обоснования или другого соответствующего документа, обосновывающего необходимость и характер отношений с третьей стороной.

- Экономическое обоснование также может включать:

- Рассмотрение рисков, связанных со способностью третьей стороны оправдать ожидания, и потенциальные последствия для основной организации.
- Подробный анализ затрат и выгод.

- Соблюдение установленных процессов поиска поставщиков, таких как конкурсные торги, запросы предложений и выбор единственного поставщика. Эти процессы включают:
  - Критерии для таких важных аспектов, как проверка протоколов кибербезопасности, проверка банковских реквизитов, проверка финансового прошлого, изучение организационной структуры, криминального и юридического прошлого, водительского стажа, политической деятельности и связей с криминальными структурами третьей стороны.
  - Четко сформулированные критерии отбора, в том числе для оценки прошлой работы, рекомендаций, репутации и стоимости договора.
  - Использование принципа должной осмотрительности (due diligence) для обеспечения надлежащего выбора поставщиков, например, формирование кросс-функциональных групп для рассмотрения предложений. Для снижения риска предвзятости контроль над группами оценки третьих сторон включает процедуры создания групп и требования по раскрытию информации о потенциальном конфликте интересов.
  - Использование принципа должной осмотрительности (due diligence) при оценке контрольной среды третьей стороны; например, посещение объекта или изучение и оценка:
    - Отчетов о системных и организационных контролях, в том числе для сервисных организаций (System and Organization Control, SOC).
    - Финансовой стабильности.
    - Учредительных документов или свидетельств о юридическом статусе.
    - Степени прозрачности в принятии решений ключевыми руководителями и заинтересованными сторонами.
    - Организационной структура.
    - Стабильности работы.
    - Протоколов кибербезопасности.
    - Соблюдения соответствующих законов, правил и стандартов.
    - Соблюдения этики.
    - Истории работы с основной организацией.
    - Репутации.
  - Доказательства того, что потенциальные поставщики или подрядчики переходят к этапу заключения договора только после проведения соответствующих процедур в соответствии с принципом должной осмотрительности (due diligence) и анализа результатов.

B. Разработка и соблюдение политики и процедур заключения договоров.

- Договоры составляются с учетом ясно изложенных условий.
- Ключевые риски учитываются на этапе составления договора, и в него включаются соответствующие пункты. На этом этапе с третьей стороной обсуждаются вопросы, требующие решения.
- Основные элементы договоров определяются на основе политики и процедур основной организации по заключению договоров и уровня приоритетности третьей стороны. Элементы могут включать:
  - Соглашения о неразглашении (конфиденциальности).
  - Оговорки о прекращении действия и определенные параметры доступа к данным.
  - Требования к кибербезопасности, включая требования к доступу и обмену всеми данными, а также к сообщению об инцидентах или нарушениях в течение определенного периода времени.
  - Требования к уведомлениям о нарушении, затрагивающем данные основной организации.
  - Стандартизированный процесс проверки идентификации третьей стороны, включая полное юридическое имя, адрес, физическое(ие) место(а) и веб-сайт. Стандартной практикой является использование контрольного списка в процессе идентификации и проверка точности информации.
  - Четко сформулированные соглашения об уровне обслуживания (SLA) с указанием ожидаемых результатов и прав, обязанностей, штрафов, поощрений и ответственности каждой стороны, включая ответственность за оплату труда (в том числе субподрядчиков).
  - Оговорку о праве на аудит, распространяющаяся на субподрядчиков, или требование подтвердить, что аудит третьих и “последующих” сторон проводил независимый поставщик услуг. Без оговорки о праве на аудит возможности функции внутреннего аудита по проведению оценки с целью обеспечения уверенности могут быть ограничены.
- Основная организация имеет доступ к отчетам независимых аудиторов об оценке внутреннего контроля третьей стороны; например, к заключению по вопросам финансовой отчетности, отчетности по соблюдению нормативных требований и безопасности данных, таким как отчеты по Международному стандарту по обеспечению гарантийных обязательств или отчеты SOC.
  - Если функция внутреннего аудита полагается на работу внешних сторон, предоставляющих уверенность , документы проверяются на предмет достоверности.
  - Отчеты SOC используются для выявления несоответствующих процессов управления рисками и изменениями.

- Политики и процедуры регламентируют вопросы, касающиеся конкретных организаций или типов договоров:
  - Положения (пункты) об охране окружающей среды и устойчивом развитии.
  - Порядок действий по итогам сообщений (от информаторов) о неправомерных действиях.
  - Требования к оценке показателей эффективности.
  - Проверенный план обеспечения бесперебойного функционирования для третьих сторон.
  - Использование искусственного интеллекта в сфере предоставления услуг.
  - Четкая идентификация, раскрытие информации, условия и объем любых субподрядных работ.
  - Процесс управления изменениями, описывающий, как обрабатывать изменения в объеме, условиях или операционных требованиях (например, изменения в технологии или нормативные обновления) в течение срока действия договора.
  - Ограничения на изменение количества заказов или суммы заказа, которые могут быть выставлены на оплату.
- Политика и процедуры требуют официальной приемки конечных продуктов (товаров, услуг и проч.) до осуществления оплаты или каких-либо удержаний в пользу третьих сторон.
- Третьи стороны обязаны предоставить свою политику этики или кодекс поведения и/или придерживаться политики основной организации.
- Если договор заключает третья сторона, основная организация проводит юридическую проверку, а ключевые риски понятны и подкрепляются соответствующей стратегией снижения рисков.

C. Окончательно оформленные договоры или соглашения рассматриваются и утверждаются соответствующими заинтересованными сторонами, включая юридические и комплаенс-службы, надежно хранятся и назначается менеджер или администратор, ответственный за их исполнение.
   - Договор или другой официальный документ, подтверждающий отношения с третьей стороной и обязательства третьей стороны, а также свидетельство проведения необходимых юридических и нормативных проверок.

D. Ведется точный, полный и актуальный перечень всех взаимоотношений с третьими сторонами, например, в централизованной системе управления договорами (CCMS).
   - Процесс добавления новых договоров или соглашений с третьими сторонами в систему.
   - Процесс внесения потенциальных третьих сторон в систему поставщиков и их удаления в случае несогласования договора.
   - Процесс удаления договоров или соглашений с третьими сторонами из системы.

- Система отслеживания для документирования проблем с конкретными подрядчиками или поставщиками для последующего использования.
- Процесс анализа, позволяющий определить, является ли перечень третьих сторон точным и полным.

E. Для того, чтобы третьи стороны могли выполнять условия договора или соглашения, устанавливаются и соблюдаются процессы адаптации поставщиков. Оценки могут включать в себя проверку того, что:

- Стандартизированные процедуры адаптации обеспечивают, что вся необходимая документация, обучение и проверка на соответствие нормативным требованиям будут выполнены.
- Системы и процессы третьей стороны могут легко интегрироваться с технологиями основной организации.
- Общие системы совместимы и безопасны. Подтверждения могут включать дополнительные средства контроля в рамках отчетности SOC.
- Основная организация оценивает планы третьей стороны по обеспечению непрерывности бизнеса, которые гарантируют продолжение обслуживания в чрезвычайных ситуациях. Для устранения возможных сбоев в работе предусмотрены планы действий в чрезвычайных ситуациях.

F. Процессы постоянного мониторинга эффективности работы поставщиков относительно целей договора или соглашения, включая оценку ключевых показателей эффективности.

- Процессы мониторинга используются для оценки рисков третьих сторон, а выявленные недостатки контроля анализируются, передаются на рассмотрение на более высокий уровень и устраняются по мере необходимости.
- Отчеты или наблюдения о процессах, технологиях и инструментах, создаются для мониторинга в режиме реального времени.
- Процессы, обеспечивающие осуществление платежей в соответствии с условиями договора или соглашения, например, при соблюдении сроков проекта, этапов и требований к коммуникации. Платежи осуществляются только утвержденным подрядчикам, которые прошли этап адаптации и были внесены в систему оплаты поставщиков. Если в договоре оговорены ожидаемые результаты, окончательные платежи производятся только после подтверждения результатов.
- Мониторинг для контроля затрат, связанных с соглашениями с третьими сторонами, в целях обеспечения ценности и определения окупаемости инвестиций. Результаты анализа затрат и выгод используются для пересмотра договоров.
- Процессы начисления штрафов за несоблюдение любых соглашений об уровне обслуживания (SLA) отражаются в договоре или соглашении. Штрафы рассчитываются и начисляются по мере их возникновения.

- Ранжирование третьих сторон, основанное на оценке рисков, периодически пересматривается, когда в соглашение вносятся изменения, а также когда срок действия договора близок к истечению или автоматическому продлению.
- Проверки приоритетных третьих сторон, такие как выездные или ежеквартальные проверки бизнеса, проводятся для оценки эффективности контроля и операционной надежности.
- Свидетельства дополнительного непрерывного мониторинга могут включать:
    - Анализ финансовой устойчивости третьей стороны.
    - Оценки жалоб на третьи стороны.
    - Анализ руководством отчетов независимых аудиторов по таким направлениям как финансовая отчетность, отчетность по соблюдению нормативных требований и отчетность по безопасности данных, сертификация по системе менеджмента качества (ISO).
    - Анализ руководством оценок устойчивости бизнеса, проведенных третьей стороной, включая все выявленные существенные проблемы.
    - Условия и ограничения на использование субподрядчиков или нижестоящих организаций.
    - Оценки этических ценностей, культуры и поведения третьих сторон.
    - Ответы на запросы СМИ.
    - Оценки протоколов конфиденциальности и кибербезопасности для защищенного хранения и передачи данных и информации основной организации, включая использование передовых технологий, таких как искусственный интеллект.
    - Выявление организацией возможностей для постоянного улучшения работы и достижения целей договора или соглашения.
    - Результаты анализа разграничения обязанностей (SoD).

G. Порядок действий по осуществлению корректирующих мероприятий по выявленным инцидентам, когда третья сторона не выполняет требования договора или соглашения или если действия третьей стороны повышают риск для основной организации.

- Порядок действий по передаче инцидентов на более высокий уровень рассмотрения в зависимости от степени серьезности инцидента и приоритетности третьей стороны.
- Анализ ситуации после инцидента, включая анализ корневых причин.

H. Процессы, обеспечивающие оповещение о договорах и соглашениях, срок действия которых истекает или автоматически продлевается. Процессы автоматического продления включают в себя проверку:

- Результата работ третьей стороны.
- Условий договора или соглашения и любых дополнений к ним.
- Факторов риска.

I. Внедрен и соблюдается формализованный регламент прекращения работы с поставщиками, чтобы обеспечить адекватное выполнение требований договоров, включая сроки и условия, в том числе для всех “последующих” субподрядчиков.

- Чек-листы или интервью с ключевыми заинтересованными сторонами для оценки эффективности мер безопасности.
- Информация или данные основной организации, находящиеся на хранении у третьей стороны, были возвращены или уничтожены.
- Доступ третьей стороны к данным, системам или оборудованию организации был аннулирован.
- Активы основной организации, такие как устройства, лицензии на программное обеспечение, интеллектуальная собственность и документация, были возвращены.
- Если происходит прекращение взаимоотношений с третьей стороной, то причины, и риски, доводятся до сведения высшего исполнительного руководства и/или Совета.
- При расторжении договора с приоритетной третьей стороной ее заменяют на основе той же оценки рисков, если только договор не завершен или в нем больше нет необходимости.

Приложение **A.** Примеры практического применения

В следующих примерах описаны сценарии, в которых может быть применимы Тематические требования «Взаимоотношения с третьими сторонами»:

Пример **1:** Аудиторское задание, включенное в план внутреннего аудита, включает услугу или продукт, который в настоящее время предоставляется третьей стороной.

Если функция внутреннего аудита завершает процесс планирования с учетом рисков и включает в план внутреннего аудита одно или несколько заданий, связанных с услугами или результатами, которые в настоящее время предоставляются третьими сторонами по договору или соглашению, соблюдение Тематических требований является обязательным.

Не каждая норма Тематических требований может применяться в каждом аудиторском задании. Если внутренние аудиторы применяют профессиональное суждение и определяют, что одна или несколько норм Тематических требований к третьим сторонам неприменимы и поэтому должны быть исключены из аудиторского задания, внутренние аудиторы должны документировать обоснование исключения этих норм. Например, основанием для исключения определенных требований может быть то, что функция внутреннего аудита определила, что зависимость организации от третьих сторон в отношении критически важных услуг невелика, или это устоявшиеся отношения, которые имеют несущественное воздействие на финансовый результат.

Пример **2:** Риски третьих сторон выявляются в ходе аудиторского задания по обеспечению уверенности по теме, отличной от темы третьих сторон или управления договорной деятельностью.

Внутренние аудиторы могут выявить значительный риск, связанный с третьими сторонами, при оценке процесса, который изначально не был определен как связанный с третьими сторонами или управлением договорной деятельностью. Например, при планировании аудиторского задания по оценке хранения данных внутренние аудиторы узнают, что облачные сервисы размещаются у третьей стороны. В ходе интервью с руководством подрядных организаций (третьих сторон), предоставляющих услуги, внутренние аудиторы выявляют риски кибербезопасности, связанные с третьей стороной.

После выявления соответствующих рисков внутренние аудиторы должны проанализировать Тематические требования «Взаимоотношения с третьими сторонами» и «Кибербезопасность» и определить, какие из них применимы. Аудиторы могут исключить из области охвата аудита взаимоотношений с третьей стороной процесс руководства организацией или процесс управления рисками и сосредоточиться на области внутреннего контроля. Такое же профессиональное суждение применимо и Тематическим требованиям «Кибербезопасность». Аудиторы должны

отразить в рабочих документах обоснование исключения любых норм Тематических требований «Взаимоотношения с третьими сторонами» или «Кибербезопасность»

Пример **3:** Возникла необходимость в выполнении аудиторского задания по оценке взаимоотношений с третьими сторонами**,** которое не было включено в план внутреннего аудита**.**

В организации возникает проблема, связанная с приоритетной третьей стороной, которая требует немедленного внимания со стороны функции внутреннего аудита. Проблема была связана со сбоем во внутреннем контроле. Руководителю внутреннего аудита следует обсудить с Советом вопрос о пересмотре приоритетов плана и ресурсов функции внутреннего аудита с учетом возникшей необходимости. Аудитор должен взаимодействовать с руководством компании, на которую повлияла данная ситуация, для оценки ситуации и выработки рекомендаций по предотвращению подобных ситуаций в будущем. Руководитель внутреннего аудита должен изучить Тематические требования с целью определить объем аудиторского задания, понять, какие требования применимы; любые исключения должны документироваться соответствующим образом.

Приложение **B.** Инструмент для документирования (опционально)

Внутренние аудиторы должны применять профессиональное суждение при определении применимости требований на основе оценки рисков и надлежащим образом документировать исключение отдельных требований. Тематические требования могут быть отражены в плане внутреннего аудита или в рабочих документах на основании профессионального суждения аудитора. Одно или несколько заданий по внутреннему аудиту могут охватывать все требования. Кроме того, не все требования могут быть применимы. Приведенная ниже печатная форма предоставляет один из вариантов документального подтверждения соответствия Тематическим требованиям «Взаимоотношения с третьими сторонами», но ее использование не является обязательным.

Процесс руководства организацией

Требование	Выполнение или обоснование исключения	Ссылка на документ
A. Разработан, внедрен и периодически пересматривается подход к определению необходимости заключения договора с третьей стороной. Подход включает в себя соответствующие критерии для определения и оценки ресурсов, необходимых и доступных для достижения целей посредством получения продукта или услуги.		
B. Разработаны политики и процедуры для определения, оценки и управления взаимоотношениями и рисками третьих сторон на протяжении всего жизненного цикла взаимодействия с ними. Политика и процедуры приведены в соответствие с применимыми нормативными требованиями и периодически пересматриваются и обновляются с целью усиления контрольной среды.		

Требование	Выполнение или обоснование исключения	Ссылка на документ
C. Определены роли и обязанности в основной организации по управлению взаимоотношениями с третьими сторонами, подробно указано, кто выбирает, управляет, взаимодействует с третьими сторонами и контролирует их деятельность, а также кто должен быть проинформирован о деятельности третьих сторон. Существует процесс, позволяющий убедиться в том, что лица, на которых возложены функции и обязанности третьих сторон, обладают соответствующей компетенцией.		
D. Определен порядок общения с соответствующими заинтересованными сторонами, включающий своевременное информирование о текущем состоянии, рисках и вопросах комплаенса (в частности, о нарушениях законов и нормативных актов) приоритетных третьих сторон. Третьи стороны приоритизируются, исходя из степени риска. К соответствующим заинтересованным сторонам могут относиться Совет, высшее исполнительное руководство, отдел закупок, операционные подразделения, отдел управление рисками, комплаенс, юридическая служба, отдел ИТ, отдел информационной безопасности, отдел кадров и другие.		

Управление рисками

Требование	Выполнение или обоснование исключения	Ссылка на документ
A. Процессы управления рисками, связанными с третьими сторонами и их услугами, являются стандартизированными и полными , включают в себя определенные роли и обязанности и в достаточной степени учитывают ключевые риски, имеющие отношение к организации (такие как стратегические, репутационные, этические, операционные, финансовые, комплаенс, кибербезопасность, информационные технологии, правовые, риски устойчивого развития и геополитические). Соблюдение процессов контролируется, и при любых отклонениях выполняются корректирующие действия.		
B. Риски, связанные с третьими сторонами, на протяжении всего жизненного цикла регулярно выявляются и оцениваются. Оценка рисков используется для ранжирования и приоритизирования третьих сторон, в том числе субподрядчиков. Меры реагирования на риски также ранжируются и приоритизируются. Оценка рисков периодически пересматривается и обновляется.		
C. Меры реагирования на риски адекватны и точны, соответствуют рейтингу. Реагирование на риски осуществляется, пересматривается, утверждается, контролируется, оценивается и корректируется по мере необходимости.		

Требование	Выполнение или обоснование исключения	Ссылка на документ
D. Существуют процедуры решения и, при необходимости, передачи на более высокий уровень рассмотрения проблемных вопросов, связанных с третьими сторонами, что обеспечивает ответственность за результаты и повышает вероятность выполнения условий договоров и других соглашений. Если третья сторона не реагирует на поднятые организацией проблемные вопросы, менеджмент оценивает риски, связанные с продолжением деловых отношений, и предпринимает дальнейшие действия по исправлению ситуации или прекращению взаимоотношений с третьими сторонами , если это необходимо.		

Внутренний контроль

Требование	Выполнение или обоснование исключения	Ссылка на документ
A. При поиске и выборе третьих сторон применяется принцип должной осмотрительности с документированным и утвержденным экономическим обоснованием или другим соответствующим документом, описывающим и обосновывающим необходимость и характер отношений с третьей стороной.		
B. Заключение и утверждение договоров осуществляются в соответствии с политикой и процедурами организации по управлению рисками в отношении третьих сторон и включают в себя сотрудничество между соответствующими подразделениями основной организации.		

Требование	Выполнение или обоснование исключения	Ссылка на документ
C. Итоговые версии договоров или соглашений рассматриваются и утверждаются всеми заинтересованными сторонами, включая юридический отдел и отдел комплаенс, подписываются уполномоченными лицами с обеих сторон и надежно хранятся. За каждым договором с третьей стороной закреплен ответственный менеджер или администратор.		
D. Ведется точный, полный и актуальный перечень всех взаимоотношений с третьими сторонами, например, в централизованной системе управления договорной деятельностью (CCMS).		
E. Установлены и соблюдаются процессы, создающие основу для выполнения третьими сторонами условий договора или соглашения.		
F. Существуют процессы постоянного мониторинга для оценки того, выполняют ли третьи стороны условия договора или соглашения в течение всего жизненного цикла работы с третьими сторонами и выполняют ли третьи стороны свои договорные обязательства. Эти процессы включают в себя проверку достоверности предоставленной информации и периодическую переоценку результатов работы, например при изменении условий соглашения.		
G. Установлен порядок осуществления корректирующих действий, если третья сторона не оправдывает ожиданий или представляет повышенный или непредвиденный риск. Порядок включает передачу инцидентов на более высокий уровень рассмотрения в зависимости от степени их серьезности, изучение инцидентов и анализ их корневых причин.		

Требование	Выполнение или обоснование исключения	Ссылка на документ
H. Отслеживаются даты истечения и продления договоров и при необходимости принимаются меры по их продлению.		
I. Внедрен и соблюдается формализованный регламент прекращения работы с подрядчиками, чтобы обеспечить адекватное выполнение требований договоров, включая сроки и условия. Определено, каким образом: • Расторгнуть договор с третьей стороной. • Заменить третью сторону в случае необходимости. • Перераспределить полномочия по хранению, вернуть или удалить конфиденциальные данные организации, хранящиеся у третьей стороны. • Аннулировать доступ третьей стороны к системам, инструментам и оборудованию.		

О Международном институте внутренних аудиторов

Международный институт внутренних аудиторов (IIA) - международная профессиональная ассоциация, обслуживающая более 265 000 членов из различных стран мира и предоставившая 200 000 сертификатов «Дипломированный внутренний аудитор» Certified Internal Auditor® (CIA®) по всему миру. Основанный в 1941 году, Международный институт внутренних аудиторов является всемирно признанным лидером в области стандартизации, сертификации, обучения, проведения исследований и разработки технических руководств в области внутреннего аудита. Дополнительную информацию можно получить на сайте theiia.org.

Отказ от ответственности

Авторское право

Сентябрь 2025 года

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