



Повышение устойчивости управления рисками третьих сторон (TPRM)

Результаты глобального
исследования KPMG

—

2026



По мере усиления зависимости организаций от подрядчиков, поставщиков, сервис-провайдеров и технологических партнёров управление рисками третьих сторон (Third Party Risk Management, TPRM) становится одним из ключевых элементов операционной устойчивости и корпоративного управления.

Цифровизация, усложнение глобальных цепочек поставок, рост регуляторных требований и эскалация киберугроз существенно трансформировали ландшафт TPRM. От организаций ожидается не только идентификация и оценка рисков, но и их непрерывный мониторинг, своевременное реагирование и адаптация на протяжении всего жизненного цикла взаимодействия с третьими сторонами. При этом многие компании отмечают, что их ресурсы по-прежнему непропорционально направлены на оценку низкорисковых контрагентов, тогда как наиболее значимые риски не всегда получают достаточное внимание.

Стремительная цифровая трансформация, расширение глобальных цепочек поставок, ужесточение регуляторных требований и рост киберугроз существенно изменили ландшафт TPRM. В настоящее время от организаций ожидается не только выявление и оценка рисков, но и их постоянный мониторинг, своевременное реагирование и адаптация к возникающим вызовам на протяжении всего жизненного цикла взаимодействия с третьими сторонами. Тем не менее, большинство клиентов отмечают, что им не всегда удаётся делать это эффективно, поскольку ресурсы часто перегружены оценкой третьих сторон с низким уровнем риска, вместо того чтобы сосредоточиться на тех партнёрах, которые действительно представляют существенный риск.

На этом фоне наш опрос изучает последние тенденции, практики и вызовы в области управления рисками третьих сторон. Он предоставляет понимание того, как организации трансформируют свои системы TPRM, внедряют новые технологии, привлекают внешних провайдеров, интегрируют функции управления рисками и реагируют на регуляторные и операционные требования. В отчёте также представлены стратегические рекомендации по управлению рисками третьих сторон с фокусом на повышение устойчивости и создание дополнительной ценности.



**Александр
Гешонник**

Глобальный руководитель
направления Форензик



Рой Валигора

Глобальный
руководитель
направления управления
рисками третьих сторон

Эффективное управление рисками третьих сторон становится одновременно критически важным и всё более сложным в условиях современной взаимосвязанной бизнес среды.

Глобальное исследование KPMG в области TPRM формирует практическую «дорожную карту» перехода от реактивных, фрагментированных, подходов к проактивной, масштабируемой и ориентированной на будущее модели управления рисками третьих сторон.

В центре внимания остаются регуляторные и киберриски как наиболее значимые и срочные угрозы.

Данное исследование указывает на существенный потенциал для:

- углубления интеграции TPRM с ERM,
- масштабирования операционных моделей,
- более осмысленного использования ИИ,
- повышения качества и надёжности данных.

Краткое резюме

Управление рисками третьих сторон (TPRM) находится в переломной точке. На протяжении многих лет руководители признавали растущую значимость экосистемы третьих сторон, и сегодня появляется возможность сократить разрыв между осознанием важности этой темы и практическими действиями за счёт внедрения современных возможностей и подходов.

Наш глобальный опрос по TPRM, в котором приняли участие 851 специалист из различных отраслей и регионов, выявил чёткую возможность для развития: несмотря на то что руководители осознают высокую значимость рисков, сохраняется потенциал для повышения эффективности реализации мер управления. Преимущества проактивного подхода очевидны: **за последние три года треть организаций понесли финансовые потери или репутационный ущерб, а 28% столкнулись с нарушениями в цепочках поставок.**

Краткое резюме

В мире, характеризующемся постоянными изменениями и сбоями, переход от формального подхода, основанного на чек-листах, к формированию подлинной, проактивной устойчивости является ключевым направлением развития. Полученные данные указывают на возможности для совершенствования и наращивания текущих усилий. Ниже приведены некоторые из ключевых выводов опроса:



Регуляторное соответствие / киберриски

И регуляторное соответствие, и киберриски являются критическими и неотложными угрозами. Это центр внимания CRO, что указывает на возможность для программ развить проактивные компетенции, позволяющие «заглядывать за горизонт» и управлять следующей волной рисков до того, как они реализуются.



Интеграция

При том что лишь 53% программ по управлению рисками третьих сторон (TPRM) в какой-то мере интегрированы с управлением корпоративными рисками (ERM), и только 71% — полностью интегрированы, сохраняется значительный потенциал для формирования единого, общеорганизационного взгляда на риски.



Масштабируемость

По-настоящему масштабируемые и стратегические операционные модели TPRM становятся зарождающимся трендом: многие организации передают на аутсорсинг отдельные высокообъемные задачи, формируя путь к end-to-end управляемым сервисам, которые на сегодняшний день внедрены лишь в 5% организаций.



Использование ИИ

Более половины организаций изучают возможности использования искусственного интеллекта (AI), и с учётом того, что 22% оценивают его как «очень эффективный», становится очевидной возможность более эффективно трансформировать технологические инвестиции в измеримую бизнес-ценность.



Качество данных

Поскольку лишь 15% руководителей выражают высокую уверенность в данных, лежащих в основе их программ, **повышение качества данных — это базовый шаг для усиления эффективности TPRM** на фундаментальном уровне.



Горячая линия / Whistleblowing

Горячая линия является важным инструментом системы комплаенса и управления рисками, обеспечивая безопасный и конфиденциальный канал для сообщения о возможных нарушениях, включая мошенничество, коррупцию, конфликты интересов и нарушения деловой этики. Интеграция горячей линии в процессы комплаенса и управления рисками позволяет организациям своевременно выявлять потенциальные нарушения, усиливать систему внутреннего контроля и получать дополнительный источник информации для мониторинга рисков, включая риски, связанные с третьими сторонами (TPRM).

Наши выводы служат чётким сигналом о ценности смелого движения вперёд в модернизации и развитии программ TPRM. Устойчивость — это не цель, которой однажды достигают, а мышца, которую необходимо постоянно развивать. Это требует встраивания управления рисками в самую основу стратегии, операционной деятельности и корпоративной культуры через интегрированные системы, умные технологии и распределённую ответственность по всему бизнесу.

Настоящий отчёт отсекает информационный шум, сводя результаты нашего опроса к пяти ключевым темам и предлагая практические рекомендации, необходимые руководителям по рискам, комплаенсу и технологиям для построения TPRM-программы, готовой к будущим вызовам.

Методология

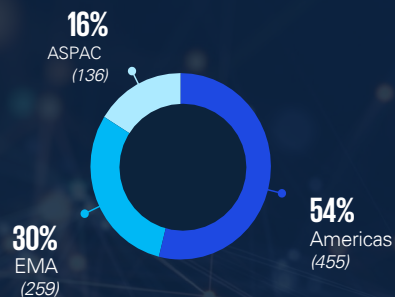
В 2025 году KPMG провела онлайн-опрос 851 респондента из различных отраслей и регионов (Америка, Европа, Азиатско-Тихоокеанский регион). В исследовании приняли участие руководители и специалисты, непосредственно вовлечённые в управление рисками третьих сторон, корпоративное управление рисками, комплаенс, ИБ и операционную деятельность.

Оценивались:

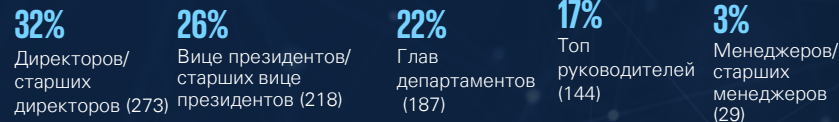
- зрелость программ TPRM,
- используемые системы и инструменты,
- подходы к оценке и мониторингу рисков,
- управление жизненным циклом третьих сторон,
- уровень устойчивости, качество данных и применение технологий.

Обзор респондентов

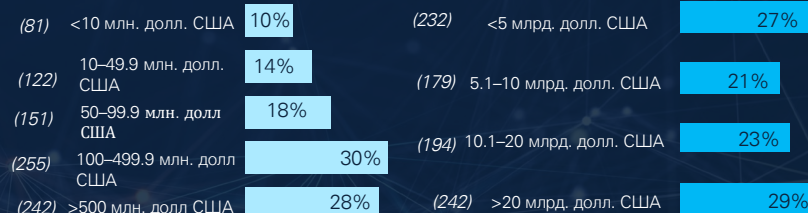
География организаций



Текущая позиция



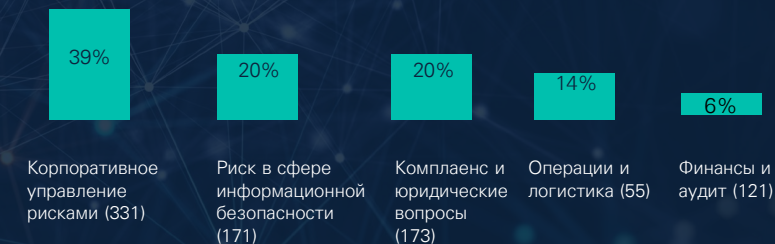
Годовые расходы на третьих лиц — Годовой доход



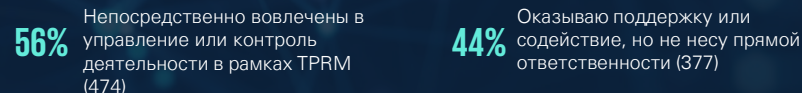
Сектор



Функции



Уровень вовлеченности в TPRM



Ключевые темы, выявленные на основе результатов опроса



Комплаенс и кибербезопасность: два ключевых столпа стратегии управления рисками третьих сторон (TPRM)

Комплаенс риски и киберриски остаются двумя доминирующими столпами стратегии TPRM. Для большинства организаций текущий подход носит преимущественно защитный характер, что отражает обоснованные опасения по поводу быстрого распространения уязвимостей третьих сторон на всю организацию.

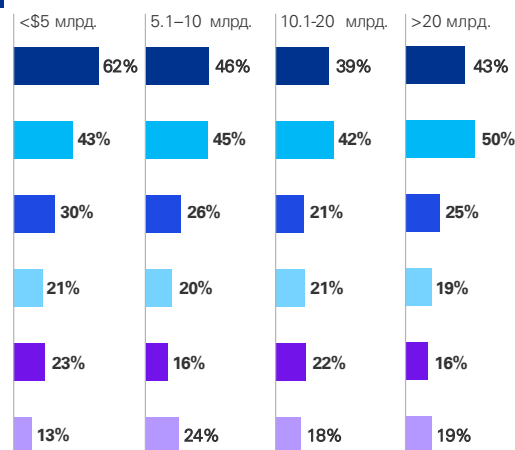
Приоритеты в инвестициях соответствуют этим опасениям, однако зачастую не приводят к формированию целостной и зрелой системы управления рисками третьих сторон.

Рисунок 1. Киберриски и регуляторные риски доминируют в стратегии управления рисками третьих сторон (TPRM)

Какие риски приобрели наибольшую значимость в рамках TPRM за последние несколько лет



По выручке (долл. США)



По сектору



Киберриски / информационная безопасность

Регуляторные и комплаенс-риски

Риски обеспечения непрерывности бизнеса

Технологические инновации

Юридические риски

Источник: TPRM опрос, 2025
Примечание: значения могут не суммироваться до 100 % из-за округления.

Киберриски приобретают особую важность для небольших организаций, согласно результатам опроса. Обладая более ограниченными ресурсами, малые компании часто рассматривают функцию кибербезопасности как основную защиту от угроз. В то же время крупные, хорошо финансируемые, организации имеют возможности развивать корпоративные подходы к управлению рисками более комплексно, снижая общий уровень уязвимости. Особенности отдельных секторов также влияют на приоритеты стратегии управления рисками третьих сторон (TPRM) и распределение расходов. Например, компании финансового сектора руководствуются строгими нормативными требованиями, тогда как организации сферы здравоохранения сталкиваются со сложными обязательствами по соблюдению требований, связанными с разнообразными отношениями с третьими сторонами.

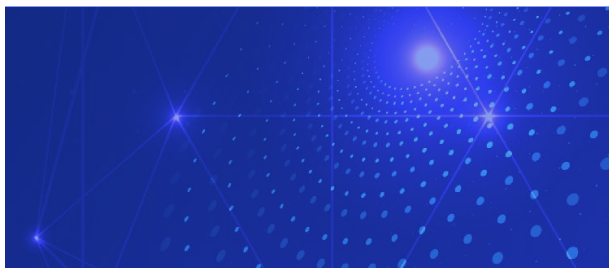
Производственные компании всё чаще включают в свои TPRM-фреймворки такие элементы, как факторы экологической, социальной и корпоративной ответственности (ESG), права человека и устойчивое развитие. Во многих секторах понимание происхождения деталей и материалов имеет решающее значение для соблюдения тарифных и торговых требований, а также для соответствия нормативным требованиям по стандартам поставок.

Широкий спектр рисков, связанных с третьими сторонами, а также многочисленные и разнообразные приоритеты программ TPRM отражают сложность и масштаб задач. Независимо от отрасли, количество рисков, связанных с третьими сторонами, значительно растёт по мере того, как экосистемы партнеров становятся более взаимосвязанными, что делает особенно актуальной необходимость подходов, адаптированных к уровню риска. Современные компании сильно зависят от партнерств с третьими сторонами для создания ценности и стимулирования инноваций, однако их количество растёт быстрее, чем организации успевают управлять рисками.

¹ "Accelerate growth and innovation with the right partner ecosystem," KPMG LLP, 2025.

Согласно исследованию KPMG, 83% руководителей планируют расширять свои партнерские сети в течение одного-трех лет, но 71% признают, что им сложно добиться согласования целей с партнерами.

В нашем опыте проектирования и управления программами TPRM для клиентов мы наблюдаем компании с десятками тысяч поставщиков, пытающиеся проверять всех подряд, тогда как только меньшая часть — примерно 10–20% — представляет повышенный риск и требует более глубокого анализа. Это огромная возможность сосредоточить усилия там, где они действительно важны. Еще одним ключевым направлением является развитие осведомленности о «Nth-party» — то есть анализ не только непосредственных третьих сторон, но и их собственных поставщиков. Видимость «Nth-party» — единственный способ выявить и управлять концентрационным риском, например, чрезмерной зависимостью от поставщиков в конкретном регионе. Многие компании не имеют такой прозрачности, но она необходима для принятия обоснованных решений по уровню риска, таких как продолжение сотрудничества с поставщиком, разработка планов действий в чрезвычайных ситуациях или прекращение отношений.



Стратегические рекомендации по управлению расширяющейся экосистемой рисков третьих сторон с обеспечением устойчивости:

Рост и усложнение экосистем третьих сторон приводит к экспоненциальному увеличению количества рисков. Во многих организациях наблюдается ситуация, когда десятки тысяч поставщиков проходят формальную проверку, в то время как лишь 10–20% из них фактически представляют повышенный риск и требуют углублённого анализа.

Отдельного внимания требует развитие видимости рисков на уровне Nth party, включая концентрационные риски и скрытую зависимость от отдельных регионов или поставщиков.

Регуляторные требования и уровень надзорного контроля растут

Соединенные Штаты

- Телеком – Безопасность цепочки поставок по стандартам FCC
- Исполнительный указ 14028 – Безопасность цепочки поставок программного обеспечения
- Финансовые услуги – Межведомственные рекомендации по управлению рисками третьих сторон
- Биомедицина – Управление по контролю за продуктами и лекарствами США
- Конфиденциальность – Центральный орган защиты прав потребителей
- Здравоохранение – Закон о технологиях обработки медицинской информации для экономической и клинической сферы
- Энергетика – Защита критической инфраструктуры по стандартам NERC CIP
- Межотраслевые требования – Обновленные рекомендации Минюста США по корпоративным программам комплаенса

Канада

- Конфиденциальность – Закон о защите персональной информации и электронных документах
- Финансовые услуги – Руководство OSFI B-10 (OSFI Guideline B-10)

Европа

- Телеком – Руководство по безопасности 5G
- Финансовые услуги – DORA, Руководящие принципы EBA по аутсорсингу
- Критическая информационная инфраструктура – NIS2
- Здравоохранение – Требования Европейского агентства по лекарственным средствам к TPRM
- Конфиденциальность – Общий регламент по защите данных (GDPR)

Казахстан

- Закон «Об информатизации»
- Закон «О персональных данных и их защите»
- Правила НБ РК № 48 и 188
- AFSA Guidelines for the Risk Management Policy
- AIFC General Rules

Сингапур

- Финансовые услуги – Уведомление MAS по аутсорсингу
- Критическая информационная инфраструктура – Закон о кибербезопасности

Япония

- Конфиденциальность – Закон о защите персональной информации
- Финансовые услуги – Вопросы регулирования и надзора, связанные с аутсорсингом

Индия

Финансовые услуги – Руководство RBI по управлению рисками третьих сторон

Австралия

- CII – Security of Critical Infrastructure
- Financial Services – Australian Prudential Regulatory Authority - CPS 230, 231 and 234
- Telecommunication - Telecommunications Sector Security Reforms

Соединенное Королевство

- Telecommunication - Telecommunication Security Act
- Financial Services – PRA, FCA, BoE - Operational Resilience SS1/21 / SS2/21



Проблемы интеграции: несмотря на декларируемую интеграцию, TPRM и ERM во многих организациях по-прежнему функционируют в разных управленческих и операционных логиках

Управление корпоративными рисками (Enterprise Risk Management, ERM) фокусируется на стратегических угрозах высокого уровня, тогда как управление рисками третьих сторон (TPRM) чаще связано с ежедневной работой с данными поставщиков, и это создаёт разрыв. Несмотря на широкое признание необходимости целостного подхода к управлению рисками, интеграция между TPRM и ERM остаётся фрагментированной. 78 % организаций сообщают, что их программы «во многом интегрированы», и 71 % утверждают, что достигли полной интеграции. Тем не менее организации продолжают сталкиваться с устойчивой проблемой: выравнивание TPRM с функциями управления рисками таким образом, чтобы это было одновременно стратегически и операционно согласованно.

На практике «частичная интеграция» часто сводится к передаче агрегированных данных TPRM в отчётность ERM без глубокой связки процессов, систем и принятия решений. Распределённая ответственность между функциями (закупки, ИБ, комплаенс, операции) дополнительно усложняет формирование единого взгляда на риски. ERM сосредоточено на ключевых рисках, которые могут препятствовать реализации стратегии, тогда как TPRM чаще носит транзакционный характер и оперирует большим объёмом данных о третьих сторонах. Кроме того, ответственность за TPRM распределена между многими подразделениями — либо «комитетом», либо отдельными командами, такими как закупки, цепочка поставок, кибербезопасность и TPRM, вместо размещения под более широкой функцией управления рисками. Такая структурная разделённость приводит к различным терминам, приоритетам и отсутствию единой точки зрения на риски.

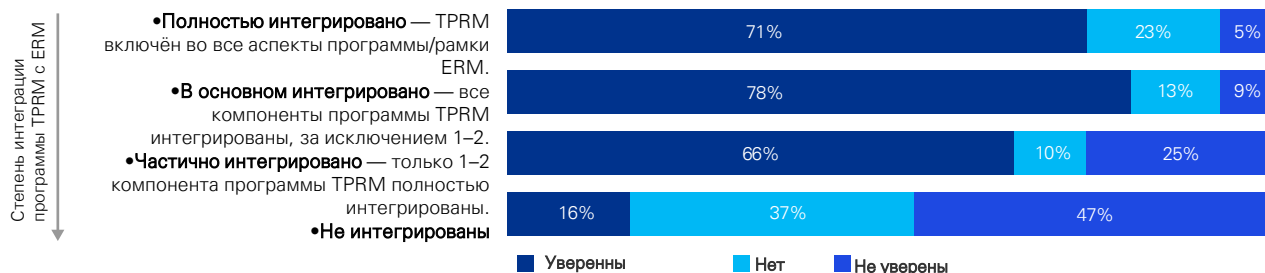
«В условиях роста числа инцидентов, связанных с поставщиками сервисов, и усиления требований регуляторов, управление рисками третьих сторон становится критически важным для компаний в Казахстане. Организациям необходимо уделять больше внимания оценке рисков, связанных с их подрядчиками и партнёрами, для обеспечения устойчивости и соблюдения регуляторных норм.»

Константин Аушев

Партнер, Руководитель
Технологической практики
KPMG Кавказ
и Центральная Азия



Рисунок 2. Существует потенциал для улучшения интеграции программ TPRM и ERM
Уровень интеграции программ TPRM/ERM и планы по дальнейшей интеграции



Источник: TPRM Исследование, 2025

Примечание: Цифры могут не суммироваться до 100 процентов из-за округления

Разделение также имеет философский характер. На TPRM часто смотрят через две призмы: со стороны комплаенса, где внимание сосредоточено на рисках причинения вреда (например, финансовые преступления, киберугрозы, взяточничество, соблюдение требований), и со стороны закупок/ цепочек поставок/ финансов, где стремятся выполнять операции быстрее, качественнее и дешевле. Без общего понимания рисков между этими доменами интеграция буксует.

Чтобы преодолеть этот разрыв, передовые организации внедряют TPRM в свои бизнес-процессы (например, «от выбора поставщика до оплаты») и выравнивают его с корпоративной стратегией и архитектурой программы управления рисками. Этот переход требует не только согласованности политик — он предполагает технологическую интеграцию, общие таксономии и межфункциональное управление. Например, модель TPRM от KPMG помогает организациям оценить текущий уровень зрелости и выстроить путь к оптимальной интеграции, опираясь на автоматизацию и операционные модели, охватывающие заинтересованных сторон из подразделений кибербезопасности, комплаенса, финансов и операционной деятельности.

Технологии также играют ключевую роль. Хотя 71 процент организаций планируют дальнейшую интеграцию в течение следующих трёх лет, лишь 17 процентов считают свои данные TPRM полностью надёжными. Этот разрыв в качестве данных подрывает усилия по консолидации отчётности, проведению интегрированных оценок рисков или взаимному использованию результатов работы.

Стратегические рекомендации по интеграции TPRM и ERM:

Проясните цели интеграции: Определите, как выглядит полная интеграция — не только в виде дашбордов, но и через общие контроли, унифицированные оценки и совместное принятие решений.

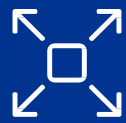
- **Устраняйте организационные барьеры:** Создайте межфункциональные структуры управления, которые выстраивают согласованность TPRM с ERM, комплаенсом, кибербезопасностью, закупками, цепочкой поставок, операционной деятельностью и информационными технологиями.
- **Инвестируйте в качество данных:** Ставьте в приоритет полноту и точность данных, чтобы обеспечить надёжную отчётность о рисках и аналитические возможности.
- **Внедряйте технологии осознанно:** Используйте автоматизацию и ИИ для оптимизации рабочих процессов, но убедитесь, что инструменты встроены в более широкую архитектуру управления рисками.
- **Согласуйте TPRM с бизнес-процессами:** Интегрируйте TPRM в процессы закупок и финансов, чтобы управление рисками было стратегическим, а не только реактивным.

“Когда речь идёт о рисках, связанных с третьими сторонами, компании одновременно стремятся к эффективности, результативности и качественному опыту. Задача состоит в том, чтобы не просто ставить галочки для соблюдения требований, а выстроить процесс, который будет устойчивым, масштабируемым и приносить реальную ценность как для бизнеса, так и для ваших поставщиков и партнёров.”



– Джон Джъенго

Руководитель по управлению рисками сторонних организаций в США, KPMG



Управляемые сервисы и аутсорсинг: масштабирование TPRM с помощью внешней поддержки

Более 80 процентов организаций сообщают, что используют управляемые сервисы, аутсорсинг или и то и другое для выполнения основных задач TPRM — от проверки и онбординга до мониторинга и устранения нарушений. Это распространяется не только на профессиональные услуги, но и на технологические решения в сфере рисков и инструменты аналитики.

Однако внедрение таких моделей не является всеобъемлющим: лишь около 5 процентов организаций используют полностью сквозные (end-to-end) управляемые сервисы. Вместо этого большинство выбирают частичные модели, привлекая внешних провайдеров для наиболее трудоёмких этапов — например, для выполнения большого объёма оценок в рамках жизненного цикла, а не для полной передачи процесса.

Например, 44 процента участников опроса используют управляемые сервисы для постоянного мониторинга, а 27 процентов передают на аутсорсинг проведение должной проверки. Это позволяет им эффективнее управлять большим количеством третьих сторон и повышать результативность и эффективность процессов управления рисками.

Опасения по поводу потери контроля и необходимости делиться конфиденциальными данными остаются серьёзными барьерами для более широкого использования аутсорсинга, косорсинга и управляемых сервисов.

Некоторые организации рассматривают свою экосистему третьих сторон как конкурентное преимущество и не спешат раскрывать эту информацию.

По мере того как развивается подход «управление рисками как сервис» (risk-management-as-a-service), готовность к аутсорсингу растёт, однако организации продолжают с осторожностью относиться к передаче функций, которые считают ключевыми для своего бизнеса.

Большинство организаций используют аутсорсинг, косорсинг или управляемые сервисы для отдельных этапов TPRM, прежде всего для высокообъёмных и трудоёмких процессов.

Во-первых, развитие ИИ стимулирует компании переходить к партнёрским моделям оказания услуг в области управления рисками третьих сторон. Несмотря на то что организации всё активнее внедряют ИИ для ускорения отдельных задач TPRM, многие делают это без целостной стратегии оптимизации, что приводит к фрагментированному «лоскутному» набору инструментов, затрудняющему сквозную эффективность.

Используя провайдера управляемых сервисов, организации могут заменить разрозненный внутренний набор инструментов единой, предварительно интегрированной платформой, оптимизированной для всего жизненного цикла TPRM.

Рисунок 3. Программы TPRM в значительной степени опираются на управляемые сервисы, особенно в области управления контрактами и онбординга. Какие конкретные аспекты вашей программы TPRM вы передаёте на аутсорсинг или используете для них управляемые сервисы?

Планирование и идентификация третьих сторон



Оценка контрагента и риск-решение



Управление контактами и онбординг



Постоянный мониторинг



Офбординг



■ Аутсорс ■ Управляемый сервис ■ Никакой ■ Оба

Примечания: (a) Категория "Другое" не включена в диаграмму из-за малого количества ответов, (b) Результат может не суммироваться до 100 процентов из-за округления

Источник: TPRM Survey, 2025

Благодаря достижениям в области ИИ модель предоставления услуг TPRM смещается от подхода, основанного на количестве часов, к подходу, ориентированному на результаты. Провайдеры управляемых услуг находятся на переднем крае этой эволюции, предлагая технологически поддерживаемые, масштабируемые модели, разработанные для достижения измеримых результатов — таких как повышение эффективности и снижение рисков — вместо простой фиксации отработанных часов.

В конечном счёте, хотя использование полноформатных управляемых услуг пока не стало нормой, оно, по-видимому, будет расти по мере того, как организации совершенствуют свои процессы TPRM и ищут масштабируемые, экономически эффективные решения и надёжных партнёров.

По мере того как организации внедряют аутсорсинг, косорсинг и управляемые сервисы, эффективный контроль становится обязательным. Чтобы добиться успеха, организациям необходимо иметь компетентных специалистов, способных управлять отношениями с провайдером, разрабатывать программу, соответствующую их конкретным потребностям, а также постоянно анализировать и оспаривать результаты. Сильное управление проектами и хорошие технологии критически важны для сохранения контроля и обеспечения того, что управляемая услуга выполняет свои обещания.

Готовность переходить к новым моделям предоставления услуг во многом зависит от отрасли. Например, компании финансового сектора, имеющие масштабные программы по идентификации клиентов (KYC) и зрелые функции управления рисками, более привычны к аутсорсингу отдельных частей ключевых процессов для их усиления сторонними провайдерами.



В отличие от них, корпоративные организации из других отраслей могут не обладать достаточным уровнем внутренней зрелости или ресурсами, чтобы в полной мере извлечь выгоду от управляемых сервисов. Многие всё ещё находятся в процессе определения и стандартизации своих TPRM-процессов, прежде чем смогут уверенно передавать их на аутсорсинг. Организации должны обеспечить соответствие внешних провайдеров внутреннему аппетиту к риску и целям в области устойчивости. Передовые практики включают создание чётких договорных рамок с соглашениями об уровне обслуживания (SLA) и ключевыми показателями эффективности (KPI), а также выбор провайдеров, которые сочетают техническую экспертизу с ярко выраженной ориентацией на клиента. Эффективные провайдеры учитывают профиль рисков организации, сосредотачиваются на наиболее рискованных областях и помогают оптимизировать процессы оценок, чтобы не перегружать внутренние команды.

Передовые предложения в сфере управляемых услуг всё чаще опираются на технологии: используют ИИ для обработки больших объёмов данных при скрининге и чат-ботов для ускоренного решения запросов низкого уровня риска. Эти инструменты обеспечивают последовательность и эффективность предоставления услуг, одновременно улучшая клиентский опыт. Такие решения продолжают совершенствоваться благодаря квалифицированным командам экспертов как на локальных, так и на зарубежных площадках, которые играют ключевую роль в обеспечении комплексной поддержки там, где уровень зрелости процессов это позволяет.

Стратегические рекомендации по масштабированию TPRM с помощью управляемых сервисов и аутсорсинга:

Определите и развивайте внутренние процессы до аутсорсинга: Стандартизируйте и документируйте рабочие процессы TPRM, чтобы обеспечить готовность к внедрению управляемых сервисов

Создайте сильную систему управления: четкие SLA и KPI, а также способность организации управлять провайдером как продолжением собственной стратегии управления рисками становится ключевым фактором успеха

Выбирайте провайдеров, обладающих как экспертизой, так и клиентоориентированностью: Выбирайте партнёров, которые понимают регуляторные требования, учитывают ваш профиль рисков и могут адаптировать свои услуги, уделяя приоритетное внимание областям с высоким уровнем риска.

Оценивайте культурную готовность и управляйте изменениями: Инвестируйте в управление изменениями, чтобы сформировать доверие к внешним провайдерам и модели аутсорсинга.

Планируйте масштабируемость: По мере развития потребностей TPRM убедитесь, что ваша модель управляемых сервисов способна масштабироваться для поддержки более широких или более сложных областей рисков без ущерба для контроля или качества.

«Мы видим, что многие организации говорят, что используют управляемые сервисы для TPRM, но на самом деле лишь немногие делают это комплексно, от начала до конца. Большинство просто отдаёт на аутсорсинг отдельные элементы. Настоящая возможность — преодолеть этот разрыв: когда вы определяете и оптимизируете свои процессы и настраиваете фундаментальные вещи перед масштабированием, вы получаете выгоду в виде более быстрого и эффективного TPRM.»



– Рой Валегора

Партнёр и глобальный руководитель направления TPRM
KPMG Великобритания



Технологии и искусственный интеллект: раскрывая зрелость TPRM и создавая ценность

Искусственный интеллект и автоматизация открывают значительный потенциал для повышения эффективности TPRM, однако на практике внедрение часто носит фрагментированный характер.

Большинство организаций используют от одной до пяти систем для поддержки TPRM, и интеграция с другими платформами является главным источником боли. Автоматизация обычно применяется к отдельным задачам — таким как должная проверка или присвоение рейтингов рисков, — но не охватывает весь жизненный цикл. В результате формируется мозаика разрозненных систем, которая создаёт больше сложности, а не уменьшает её.

Внедрение ИИ растёт, особенно в области отчётности и визуализации данных. Однако эффективность ИИ тоже неоднозначна. Хотя 50–58 процентов участников опросов утверждают, что используют ИИ, только 22 процента считают его «очень эффективным», а 40 процентов говорят, что он «в какой-то степени эффективен». Разрыв в эффективности часто связан с уровнем доверия и качеством оркестрации. **Организации, добивающиеся наибольшей отдачи от ИИ, фокусируются не на отдельных сценариях, а на оркестрации сквозных процессов, чётком распределении ответственности и качестве исходных данных.**

Изолированные, одношаговые агенты значительно менее эффективны, чем связанный, оркестрованный процесс.

Самые мощные приложения ИИ объединяют глубокие исследования, приобретённые аналитические данные из специализированных баз данных и информацию, собранную непосредственно от третьей стороны, формируя более полную картину рисков. Это позволяет организациям оценивать не только текущие реальные события, но и моделировать различные сценарии, готовясь как к «настоящему», так и к «следующему». Будущее TPRM заключается в такой сквозной оркестрации, которая обеспечивает более глубокую оценку поставщиков и даёт компаниям возможность не только реагировать на происходящее сейчас, но и предвидеть то, что будет дальше. Смотри вперёд, от 39 до 47 процентов организаций ожидают умеренного использования ИИ в ключевых задачах TPRM в течение ближайших трёх лет. Возможность очевидна: ИИ может ускорить сквозные операции, улучшить выявление рисков и обеспечить более интеллектуальное принятие решений в режиме реального времени. Однако для реализации этого потенциала необходимы целевые инвестиции, межфункциональное взаимодействие и чёткая дорожная карта перехода от пилотных проектов к решениям корпоративного масштаба.

Рисунок 4. Большинство программ TPRM используют лишь умеренный уровень автоматизации, и лишь немногие применяют продвинутое формы автоматизации.

Уровень автоматизации программы TPRM и аспекты, в которых используется автоматизация

Мы не используем ИИ ни в одном процессе



Принять решение о прекращении сотрудничества с третьей



Оценить потенциальные риски



Обеспечивать мониторинг



24/7 консультант TPRM через FAQ-чатбот



Проверка контракта на наличие соответствующих положений



Проверка ответов поставщика в анкете и выявление проблем



Определение требований к должной проверке (due diligence)



■ **Продвинутая стадия:** полностью автоматизированные, интегрированные системы

■ **Средняя стадия:** оптимизированные процессы, частичная автоматизация

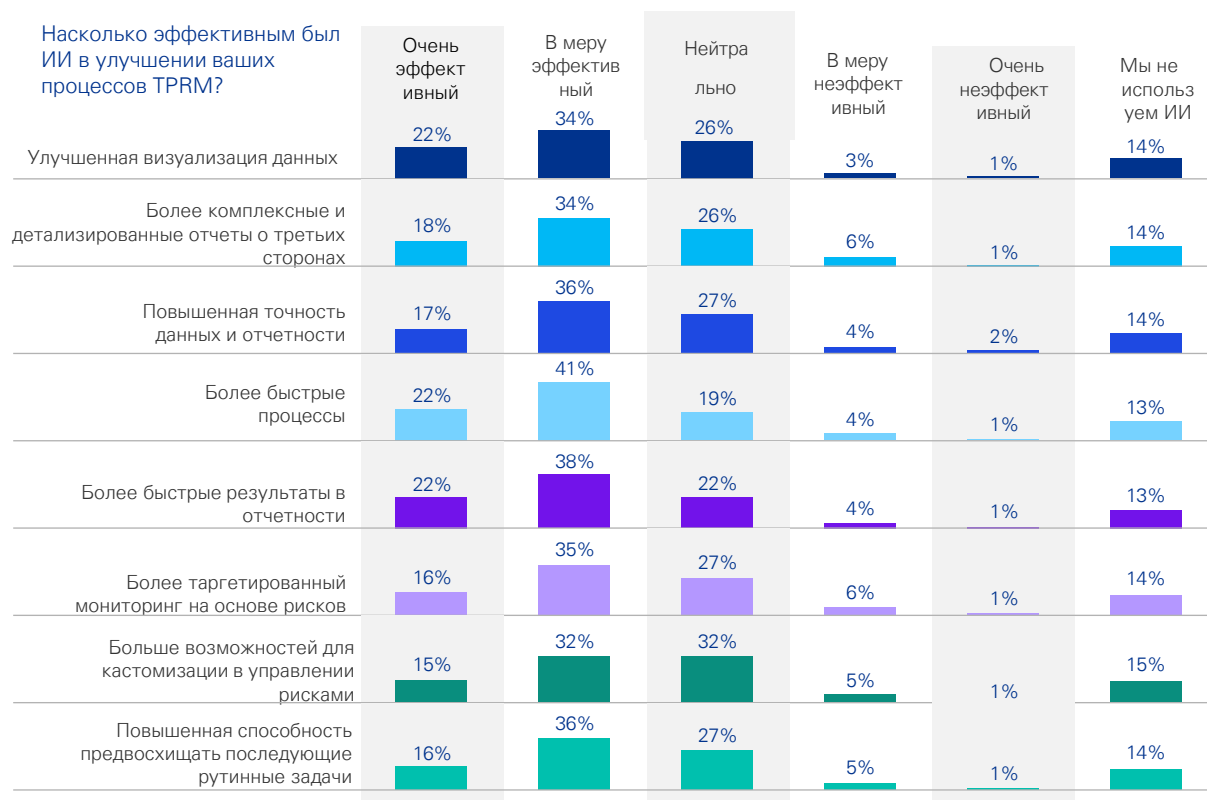
■ **Начальная стадия:** базовые инструменты, частичное ручное участие

■ **Базовая стадия:** минимальная автоматизация, в основном ручные процессы

Примечания: (а) Для наглядности выбраны восемь самых распространённых вариантов. (б) Итоги могут не суммироваться до 100 процентов из-за округления.

Источник: опрос TPRM, 2025 год

Рисунок 5. Эффективность ИИ в улучшении процессов TPRM варьируется от организации к организации.



Примечания: (а) Категория "Другое" не включена в диаграмму из-за малого количества ответов, (б) Результат может не суммироваться до 100 процентов из-за округления

Source: TPRM Survey, 2025

Стратегические рекомендации по развитию ИИ и автоматизации в TPRM:

- Внедряйте ИИ в сквозные рабочие процессы:** перейдите от отдельных сценариев использования к интеграции ИИ на всех этапах жизненного цикла TPRM — от онбординга до офбординга.
- **Сочетайте автоматизацию с экспертизой человека:** комбинируйте инструменты ИИ с командами управляемых сервисов, чтобы решения по рискам были информированными, контекстными и согласованными с целями бизнеса.
 - **Отдавайте приоритет интеграции систем:** устраняйте фрагментацию платформ, чтобы обеспечить бесшовный поток данных и максимизировать ценность ИИ и автоматизации.
 - **Фокусируйтесь на высокоэффективных сценариях:** начинайте с таких областей, как массовый скрининг, скоринг рисков и обработка запросов с помощью чатботов, чтобы быстро продемонстрировать результаты.
 - **Инвестируйте в готовность к ИИ:** обеспечьте качество данных, надлежащее управление ими и зрелость процессов для эффективного внедрения ИИ.



Качество данных и уровень доверия: Основа надёжного управления рисками третьих сторон (TPRM)

Уверенность в эффективности TPRM зависит от надёжных данных. Наш опрос выявил резкий контраст: лидеры, располагающие качественными данными, уверены в своём управлении рисками. Лидеры с плохими данными — нет. Всё предельно просто. Среди респондентов, обладающих высококачественными данными, 52 процента заявили, что “очень уверены” в своих решениях в области TPRM, тогда как 40 процентов участников с недостаточным качеством данных сказали, что они “не уверены”.

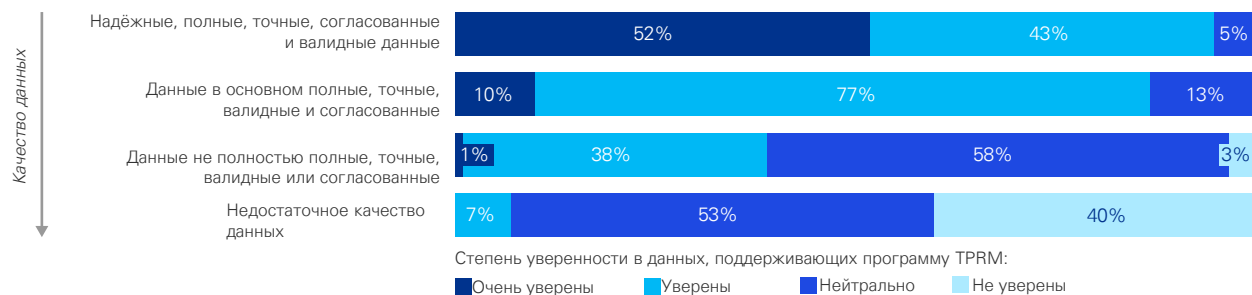
Качество данных является фундаментом надёжного TPRM. Исследование выявляет прямую зависимость между качеством данных и уверенностью руководства в принимаемых решениях.

Фрагментация систем, несогласованные таксономии и отсутствие единого источника данных существенно ограничивают возможности аналитики, автоматизации и интеграции с ERM.



Рисунок 6. Уверенность в процессах TPRM зависит от качества данных

Качество данных, используемых в отчётности TPRM, и уверенность в данных, поддерживающих общую программу TPRM



Источник: Опрос TPRM, 2025

Примечание: Суммарные значения могут не составлять 100 %, поскольку выполнено округление

Плохое качество данных не только вызывает сомнения, но и активно подрывает ваши стратегические инвестиции. Качество данных является одним из основных барьеров для эффективного внедрения ИИ и управляемых сервисов. Фактически, результаты опроса по качеству данных противоречат широко распространённым заявлениям респондентов о внедрении ИИ и управляемых сервисов, что говорит о том, что многие организации применяют эти инструменты лишь к отдельным процессам, а не ко всему жизненному циклу TPRM. Без надёжных данных даже самые продвинутые инструменты не способны обеспечить значимые инсайты или автоматизацию.

Организациям необходимо инвестировать в управление данными, стандартизованную отчётность и постоянную валидацию. Однако эта задача может казаться слишком сложной, особенно из-за множества систем и функциональных команд, вовлечённых в процесс. Многие компании испытывают трудности с определением точки начала. Практичным подходом является старт с малого — сосредоточиться на очистке и проверке данных для ограниченного круга наиболее важных поставщиков (например, критически значимых третьих сторон или отдельных географий). Структурированные, поэтапные улучшения могут обеспечить измеримые результаты с точки зрения затрат и ценности, а также создать импульс для более широких инициатив по управлению данными.

Стратегические рекомендации по повышению качества данных и уровня доверия в рамках TPRM

Начните с критически важных третьих сторон: сосредоточьте первоначальные усилия по очистке данных на наиболее значимых поставщиках, чтобы добиться ранних результатов и продемонстрировать ценность.

Применяйте поэтапный подход к исправлению данных: разбивайте инициативы по повышению качества данных на управляемые шаги, которые дают соотношение затрат и выгоды на каждом этапе, вместо того чтобы пытаться провести полную перестройку сразу.

Инвестируйте в управление данными и стандартизацию: установите чёткое распределение ответственности, единообразные определения и стандартную отчётность между бизнес-подразделениями и географиями.

Интегрируйте системы закупок и управления рисками: работайте над созданием единого представления данных о сторонних поставщиках по всем глобальным операциям, чтобы повысить прозрачность и качество оценки рисков.

Согласуйте инициативы по повышению качества данных с целями в области ИИ и управляемых сервисов: обеспечьте, чтобы фундаментальные улучшения данных поддерживали более широкие стратегии автоматизации и аутсорсинга..

«Построение фундамента из достоверных данных — самый эффективный способ укрепить уверенность и раскрыть полный потенциал TPRM. Тот факт, что только 17 процентов руководителей сообщают о наличии высококачественных данных, указывает на очевидный путь вперёд. Сфокусировавшись на целостности данных, организации смогут получить больше ценности от своих технологических инвестиций, таких как ИИ, и создать по-настоящему устойчивую программу TPRM, которая обеспечивает более качественное и быстрое принятие решений.»



– Гэвин Розеттенстайн
Партнёр, KPMG Австралия

Свод рекомендаций: создание устойчивой, готовой к будущему программы TPRM

Путь к программе TPRM, готовой к будущему, — это не серия небольших корректировок; он требует смелых, стратегических действий. Чтобы перейти от реактивной, основанной на соблюдении требований функции к проактивному, создающему ценность двигателю устойчивости, организациям необходимо принять новое мышление. Следующие шаги обобщают ключевые выводы нашего исследования и предлагают чёткую дорожную карту, которая позволит не только защитить вашу организацию, но и укрепить её конкурентные преимущества.



Сфокусируйте ресурсы на действительно значимых рисках, отказавшись от формального охвата всей экосистемы



Устраните организационные и технологические разрывы между TPRM и ERM



Рассматривайте данные как стратегический актив, а не побочный продукт процессов



Переходите от «AI театра» к осознанной автоматизации сквозных процессов



Расширьте периметр управления рисками за пределы прямых поставщиков



Передавайте на аутсорсинг результаты, но не ответственность за риск

Как KPMG может помочь

В этом отчёте представлена дорожная карта по трансформации TPRM – от защитной необходимости к стратегическому преимуществу. KPMG обладает опытом, технологиями и глобальными ресурсами, чтобы помочь вам реализовать эту стратегию и добиться успеха. Мы работаем вместе с вами над созданием устойчивости, повышением эффективности и раскрытием стратегической ценности ваших отношений с третьими сторонами. Наша глобальная команда по TPRM структурирована таким образом, чтобы предоставлять комплексную поддержку — сочетая глубокую отраслевую экспертизу, передовые технологии и развитую модель управляемых сервисов, которая выгодно выделяет нас на рынке.

Глобальная команда

Наши специалисты по TPRM работают через сеть глобальных центров доставки, обеспечивая круглосуточный доступ к квалифицированным ресурсам в ключевых мировых хабах. Такая структура позволяет гибко масштабировать команды в зависимости от потребностей клиента, обеспечивать поддержку в разных часовых поясах и на различных языках, а также гарантировать единое, высокое качество услуг в разных юрисдикциях.

Мультидисциплинарный подход

KPMG использует мультидисциплинарный подход, объединяя экспертов по рискам, закупкам, комплаенсу, технологиям, кибербезопасности и ESG для разработки, внедрения и постоянного совершенствования TPRM-программ. Такая кросс-функциональная модель управления помогает обеспечить охват всех аспектов программы управления рисками третьих сторон — с чётко определёнными зонами ответственности и подотчётности.

Современные управляемые сервисы

Предложение KPMG в формате Managed Service для TPRM — это двигатель непрерывной трансформации, объединяющий автоматизацию, ИИ и специализированную экспертизу по запросу. Наш модульный сервис на основе подписки разработан для повышения эффективности за счёт использования передовых технологий, автоматизации и офшорных ресурсов. В отличие от традиционного аутсорсинга, наши комплексные управляемые сервисы охватывают весь жизненный цикл TPRM — от онбординга и due diligence до постоянного мониторинга, управления инцидентами и офбординга.



Наши TPRM-решения обеспечивают измеримую ценность:

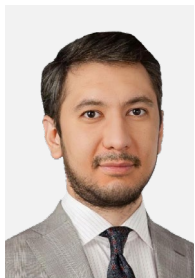
Повышение эффективности: Снижение административной нагрузки и ускорение онбординга третьих сторон благодаря автоматизации и оптимизированным процессам.

Снижение рисков: Наши управляемые сервисы помогают клиентам проактивно выявлять, оценивать и смягчать риски на всех этапах жизненного цикла поставщика, улучшая общий уровень безопасности и соответствия требованиям.

Стратегическая аналитика: Продвинутая аналитика и отчётность обеспечивают прикладные инсайты, позволяющие принимать более информированные решения и поддерживать непрерывное совершенствование.

Операционная устойчивость: Интегрируя TPRM с ERM и используя глобальные ресурсы, KPMG помогает организациям укреплять устойчивость к сбоям, изменениям нормативных требований и внешним потрясениям.

Контакты



Фаррух Абдуллаханов

Партнер, Руководитель практики Форензик
KPMG в Узбекистане

E: FAbdullakhanov@kpmg.com



Берик Бекниязов

Директор практики Форензик
KPMG Кавказ и Центральная Азия

E: bbekniyazov@kpmg.com



Константин Аушев

Партнер, Руководитель
Технологической практики
KPMG Кавказ и Центральная Азия

E: kaushev@kpmg.kz



Габит Мусрепов

Партнер, руководитель практики корпоративного
управления и устойчивого развития
KPMG Кавказ и Центральная Азия

E: GMusrepov@kpmg.kz



Дамир Еркин

Директор Технологической практики
KPMG Кавказ и Центральная Азия

E: damirerkin@kpmg.com



Роман Ким

Заместитель директора практики корпоративного управления
KPMG Кавказ и Центральная Азия

E: romankim@kpmg.kz