УПРАВЛЕНИЕ РИСКАМИ ПРИ РАБОТЕ С КОНТРАГЕНТАМИ

Багамаев Ш.Г.,
Финансовый университет при Правительстве Российской Федерации

Аннотация: многие компании в какой-то степени полагаются на третьих лиц. У некоторых тысячи сторонних отношений. Они помогают компаниям сократить расходы, повысить скорость обслуживания и обеспечить глобальный доступ. Они также позволяют компаниям быть более гибкими и конкурентоспособными. Но контрагенты могут создавать большие риски, от репутационного и брендового характера до риска серьезного финансового ущерба. Управление сторонним риском обычно получает наибольшее внимание, когда компания находится в строго регулируемой отрасли – например, финансовые услуги или фармацевтика, либо, когда компания столкнулась с проблемами Закона о коррупции за рубежом (FCPA), и регулирующие органы требуют надежных программ соблюдения и мониторинга в рамках мирового соглашения. Использование контрагентов является частью бизнес среды. Третьи лица предоставляют компаниям много преимуществ, но также они несут неизбежные риски. Поэтому наличие эффективной и действенной программы управления сторонними рисками имеет решающее значение. В этой статье рассматриваются рынок взаимодействия с контрагентами и риски, связанными с ними. Проанализированы многочисленные взаимосвязи и деловые отношения между компаниями касательно рисков в этой сфере. Также рассмотрены возможные меры по минимизированию рисков.

Ключевые слова: контрагенты, безопасность, оценка риска, управление рисками

Любая предпринимательская деятельность связана с какой-либо рисковой составляющей, характеризующейся вероятностью недостижения цели, которая стоит перед хозяйствующим субъектом. Наличие подобной составляющей обусловлено действием значительного количества факторов, в т. ч. факторов внешней среды, контрагентов и лиц, поведение которых не всегда можно предсказать с приемлемой точностью, оказывающих влияние на конечный результат деятельности.

Контрагент – это любое физическое лицо, компания, клиент, подрядчик, поставщик, агент или дистрибьютор, который взаимодействует с компанией или от ее имени. Контрагенты предоставляют все виды услуг, от обработки платежных ведомостей до работы центров обработки данных.

Общие зоны риска при использовании контрагентов:

- Отмывание денег
- Конфиденциальность
- Охрана окружающей среды
- Торговля, санкции, экспортный контроль
- Мошенничество
- Здоровье и безопасность
- Откаты
- Непрерывность и устойчивость бизнеса
- Кибербезопасность
- Антимонопольное законодательство
- Спорные территории
- Торговля людьми, рабский и детский труд
- Кража интеллектуальной собственности
- Технологии
- Взяточничество

Факторы рисков, связанные с контрагентами, можно отнести к внешней зоне возникновения, так как для предприятия сложно оказывать достаточное влияние на вероятность неисполнения контрагентом своих обязательств, ведь на это оказывает влияние фактор внутренней среды предприятия-контрагента, его подверженность изменениям внешней среды. В связи с этим предприятию необходимо сместить свой фокус оценки и сделать главной задачей выявление факторов, которые могут способствовать увеличению степени подверженности рискам контрагентов и минимизации потенциальных потерь.

Препятствия для понимания сторонних рисков:

- Нет данных обо всех контрагентах, с которыми сотрудничает компания
- Недостаточное понимание того, что делают третьи лица
- Неполная оценка того, как работают контрагенты
- Процесс выбора контрагентов имеет недостатки
- Высокая стоимость
- Требуется время, которое компания может не иметь, когда бизнес пытается быстро реагировать

Факторы оценки рисков контрагентов

- *Кибербезопасность и конфиденциальность данных.* Кибербезопасность и защита данных являются главной заботой и проблемой третьих лиц. Компании все больше полагаются на интернет вещей, облачные вычисления и анализ

данных. Многие используют сторонних поставщиков для таких технологий. Но часто компании не знают, какие контрагенты имеют доступ к конфиденциальным данным. Контрагенты часто являются мишенями из-за их доступа к данным, в то время как другие имеют небезопасные точки входа. Кроме того, существуют законы о конфиденциальности, которые необходимо соблюдать. Например, Общие положения Европейского союза о защите данных (GDPR) вступили в силу 25 мая 2018 года. Коммерческие компании могут быть оштрафованы на сумму до 24 миллионов долларов, или 4% от общего дохода (в зависимости от того, что больше) за нарушения GDPR.

• *Соблюдение действующих норм.* Необходимо соблюдать законы о конфиденциальности данных. Существуют законы о борьбе с отмыванием денег, а также законы о защите прав потребителей и работников. Имеются также строгие отраслевые требования для определенных секторов, например, для медицинских устройств.

• *Соблюдение этических норм и охрана окружающей среды.* Массовое субподрядное соглашение означает, что компании передают производство на аутсорсинг фабрикам и сетевым поставщикам по всему миру, где затраты ниже. Это очень затрудняет отслеживание полной цепочки поставок компании. Данная практика довольно часто становится источником возникновения этических и социальных риски, а также судебных процессов или негативной огласки. В 2016 году организация Amnesty International обнаружила использование детского труда в цепочках поставок некоторых крупных технологических и автомобильных компаний. Производители продуктов питания также подверглись критике за использование детского труда в бедных странах. Более 152 миллионов детей во всем мире в возрасте от 5 до 17 лет становятся жертвами детского труда. А в сфере розничной торговли по-прежнему существуют потогонные фабрики, где необходимо быстро производить более дешевые продукты.

• *Бренд и репутация.* Потребители все чаще хотят понять суть бизнеса, с которым они взаимодействуют. В наши дни неэтичные действия контрагентов могут очень быстро распространиться и сильно повлиять на состояние компании.

• *Уязвимость.* Стихийное бедствие или какая-либо форма ограничения трансграничной торговли (например, Brexit), которая нарушает цепочку поставок, может затруднить работу компании. Это главным образом относится к тем случаям, когда альтернативные источники не всегда доступны.

• *Существенность.* То, сколько компания тратит на контрагента всегда будет частью расчета риска. Но объем расходов не является единственным критерием. Контрагент, представляющий относительно незначительные расходы, может представлять более значительный риск в зависимости от характера его услуг. Здесь стоит вспомнить ИТ-индустрию.

Процесс управления рисками предполагает, что будут использоваться различные мер, которые позволят в какой-то степени спрогнозировать наступление того или иного рискового события, а также принять целенаправленные действия для снижения степени риска. Избежать риска в предпринимательской деятельности практически невозможно, но, зная источник возникновения рисков, предприниматель способен снизить их уровень, уменьшив действие неблагоприятных факторов.

Учитывая огромное количество контрагентов, которых используют компании, важно оценивать и управлять соответствующими рисками. Совет директоров может играть важную роль в поощрении компаний к созданию эффективных программ управления рисками третьих сторон. Благодаря эффективному управлению рисками руководство компании может оперативно принимать решения и снизить затраты. В идеале программа должна предоставлять руководству текущий перечень контрагентов и их уровень риска, а также предоставлять информацию о том, насколько эффективно устраняются риски. По результатам опроса компанией PwC в 2018 году, только 35% компаний имеют полный перечень всех третьих лиц, которым они передают конфиденциальную информацию. Крайне важно, чтобы генеральный директор поддерживал решение вопросов, связанных со сторонними рисками, и чтобы на их решение выделялись необходимые ресурсы и внимание.

Как создать эффективную программу по контролю сторонних рисков

1. Определить третьих лиц
2. Установить политику и процедуру проверки
3. Оценить отдельных третьих лиц
4. Упростить базу поставщиков
5. Внедрить технологии
6. Понять, с чего начать

Управлять рисками, связанными с контрагентами, довольно сложно, так как этот процесс имеет динамический характер и требует постоянного внимания субъекта управления, а также использования оригинальных подходов и усложненных методик. Большинство компаний используют сочетание выездных инспекций и заполнение анкет

третьими лицами. Частота этих видов мониторинга будет зависеть от уровня риска. Особенность управления рисками контрагентов состоит в том, что необходимо учитывать фактор внешнего характера источников рисков контрагентов. Одним из способов устранения сторонних рисков является включение условий контракта, которые устанавливают стандарты и уровень соответствия, которого ожидает компания. Например, некоторые компании устанавливают экологические, социальные или трудовые стандарты для своих сторонних поставщиков.

Использование контрагентов, деловых партнеров и аутсорсинга является частью бизнес среды. Третьи лица предоставляют компаниям много преимуществ, но также они несут неизбежные риски. А огромное количество сторонних отношений у компании, затрудняет наблюдение за рисками, которые они приносят. Вот почему наличие эффективной и действенной программы управления сторонними рисками имеет решающее значение - и совету директоров необходимо знать, адекватно ли устраняются риски.

Литература

1. Ермолаев Д.Н. Методологические основы управления рисками контрагентов // Дискуссия. 2011. № 9. URL: https://cyberleninka.ru/article/n/metodologicheskie-osnovy-upravleniya-riskami-kontragentov (дата обращения: 02.08.2020)

2. Управление комплаенс-рисками при работе с контрагентами. 2016. № 22. С. 2 – 13 [Электронный ресурс] // URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/finance/russian/compliance_risk_managemen_working_with_counterparties_2017.pdf (дата обращения: 03.08.2020)

3. Understanding third-party risk [Электронный ресурс]. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-on-the-boards-agenda.pdf (data obrashhenija: 3.08.2020)

References

1. Ermolaev D.N. Metodologicheskie osnovy upravleniya riskami kontragentov. Diskussiya. 2011. № 9. URL: https://cyberleninka.ru/article/n/metodologicheskie-osnovy-upravleniya-riskami-kontragentov (data obrashcheniya: 02.08.2020)

2. Upravlenie komplaens-riskami pri rabote s kontragentami. 2016. № 22. S. 2 – 13 [Elektron-nyj resurs]. URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/finance/russian/compliance_risk_managemen_working_with_counterparties_2017.pdf (data obrashcheniya: 03.08.2020)

3. Understanding third-party risk [Elektronnyj resurs]. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-on-the-boards-agenda.pdf (data obrashhenija: 3.08.2020)

RISK MANAGEMENT AT WORKING WITH CONTERAGENTS

Bagamaev Sh.G.,
Financial University under the Government of the Russian Federation

Abstract: many companies rely on third parties to some extent. Some have thousands of outside relations. They help companies reduce costs, improve service speeds, and provide global access. They also allow companies to be more flexible and competitive. But counterparties can also be the cause of, ranging from reputation and branding to the risk of serious financial damage. Managing third-party risk usually gets the most attention when: a company is in a highly regulated industry - such as financial services or pharmaceuticals, or when the company has run into Foreign Corrupt Practices Act (FCPA) issues, and regulators require robust compliance and monitoring programs within amicable agreement. Cooperation with contractors and business partners, as well as the use of outsourcing is part of the business environment. Third parties provide many benefits to companies, but they also carry inevitable risks. Therefore, having an effective and efficient third party risk management program is critical. This article examines the market of cooperation with counterparties and the risks associated with them. Numerous relationships and business relationships between companies regarding risks in this area were analyzed. Possible measures to minimize risks are also considered.

Keywords: counterparties, security, risk assessment, risk management