МЕЖДУНАРОДНЫЙ СТАНДАРТ

ИСО 31000

2-е издание
2018-02

Менеджмент риска – Руководство

Risk management - Guidelines

Регистрационный номер
ISO 31000:2018(E)

Перевод АНО ДПО "ИСАР"

Оглавление

Предисловие

Международная организация по стандартизации (ИСО) является всемирной федерацией национальных организаций по стандартизации (комитетов - членов ИСО). Разработка международных стандартов обычно осуществляется техническими комитетами ИСО. Каждый член ИСО, заинтересованный в деятельности соответствующего технического комитета, имеет право быть представленным в этом комитете. Международные организации, как правительственные, так и неправительственные также принимают участие в данной работе в сотрудничестве с ИСО. ИСО тесно сотрудничает с Международной электротехнической комиссией (МЭК) по всем вопросам электротехнической стандартизации.

Процедуры, использованные при разработке этого документа и предназначенные для дальнейшей поддержки, описаны в Директивах ИСО/МЭК, Часть 1. В частности, должны быть указаны различные критерии утверждения, необходимые для различных типов документов ИСО. Настоящий документ был разработан в соответствии с правилами, изложенными в Директивах ИСО/МЭК, Часть 2 (см. www.iso.org/diretives).

Особое внимание уделено тому, что некоторые элементы данного документа могут являться предметом патентных прав. ИСО и МЭК не должны нести ответственность за идентификацию какого-либо или всех подобных патентных прав. Детали, касающиеся любых патентных прав, установленные в ходе разработки документа, должны быть указаны в разделе Введение и/или в листе полученных патентных деклараций ISO (см. www.iso.org/patts).

Все торговые марки, упомянутые в настоящем документе, приведены для удобства пользователей, а не в качестве рекомендаций или выражения публичной поддержки.

Для разъяснения значений используемых ИСО специфических терминов и выражений, связанных с оценкой соответствия, равно как и для информации о соблюдении ИСО принципов соглашения ВТО по техническим барьерам в торговле см. ссылку www.iso.org/iso/foreword.html.

Настоящий документ разработан Техническим комитетом ИСО (ТК) № 262 «Менеджмент риска».

Представленное второе издание стандарта отменяет и вводится взамен технически пересмотренного первого издания (ИСО 31000:2009).

Ниже указаны основные изменения относительно первого издания:

- пересмотрены принципы риск-менеджмента, соответствие которым обеспечивает успешность его внедрения;

- особо выделены лидерская роль высшего руководства и интеграция менеджмента риска, начиная с уровня управления организацией;

- сделан больший акцент на итеративный характер риск-менеджмента, также отмечено, что получение нового опыта, знаний и результатов анализа может потребовать пересмотра элементов процесса, действий и средств контроля на каждом этапе процесса;

- упорядочено содержание документа с целью обеспечения универсальности и применимости его положений к различным потребностям и ситуациям.

Введение

Настоящий документ предназначен для лиц, которые создают и защищают стоимость в организации, путем управления рисками, принятия решений, постановки и достижения целей, а также повышения производительности.

Организации всех типов и размеров сталкиваются с внешними и внутренними факторами и воздействиями, которые порождают неопределенность в отношении того, достигнут ли они своих целей.

Риск-менеджмент является итеративным процессом и помогает организациям определять стратегию, достигать цели и принимать обоснованные решения.

Риск-менеджмент является частью корпоративного управления и лидерства и оказывает значительное воздействие на то, как осуществляется управление организацией на всех уровнях. Риск-менеджмент способствует совершенствованию систем управления.

Риск-менеджмент применяется ко всем видам деятельности, связанным с организацией, и включает взаимодействие с заинтересованными сторонами.

Риск-менеджмент рассматривает факторы внешней и внутренней среды (контекста) организации, включая поведенческие и культурные факторы.

Риск-менеджмент основан на принципах, структуре и процессе, описанных в настоящем документе, как проиллюстрировано на рисунке 1. Данные компоненты в некотором виде (полностью или частично) могут уже существовать в организации, однако, возможно, их потребуется адаптировать или улучшить для того, чтобы риск-менеджмент был эффективным, результативным и последовательным.

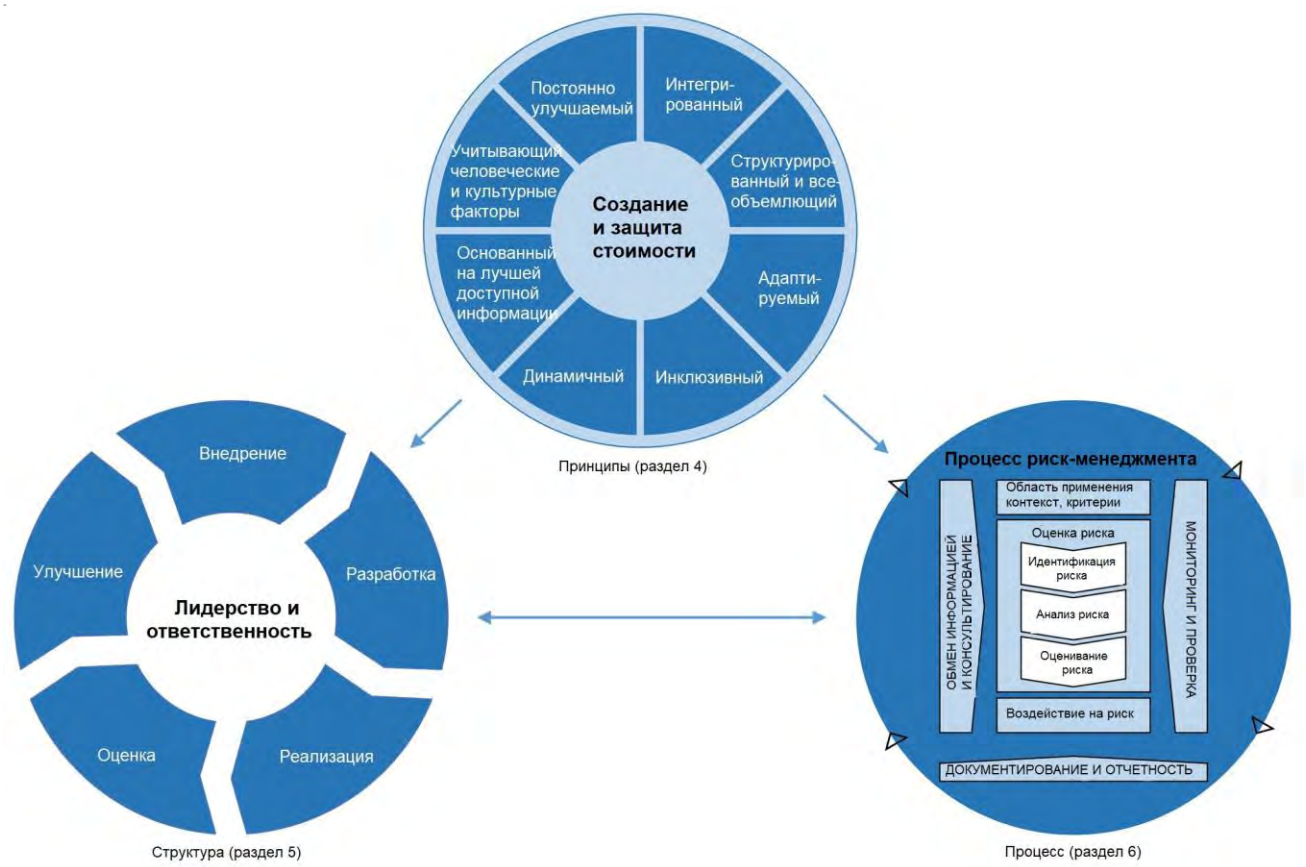

Рисунок 1 — Принципы, структура и процесс

Менеджмент риска — Руководство

1 Область применения

Настоящий документ предоставляет рекомендации по управлению рисками, с которыми сталкиваются организации. Порядок применения данных рекомендаций может быть адаптирован для любой организации и ее контекста.

Настоящий стандарт содержит общий подход к управлению любыми рисками и не является узкоспециальным или отраслевым.

Настоящий стандарт может применяться в течение всего жизненного цикла организации и для любой деятельности, включая принятие решений на всех уровнях.

2 Нормативные ссылки

Настоящий документ не содержит нормативных ссылок.

3 Термины и определения

Для целей настоящего документа применяются следующие термины и определения.

ИСО и МЭК ведут терминологические базы для использования в стандартизации по следующим ссылкам:

— Онлайн платформа ИСО: доступна по адресу http://www.iso.org/obp

— Международный электротехнический словарь МЭК: доступен по адресу http://www.electropedia.org

3.1
Риск (risk)
Влияние неопределенности на цели

Примечание 1: Влияние – это отклонение от того, что ожидается. Оно может быть положительным и/или отрицательным, и может способствовать реализации возможностей и устранению угроз, создавать или приводить к возникновению возможностей и угроз.

Примечание 2: Цели могут иметь различные аспекты и категории и могут применяться на различных уровнях.

Примечание 3: Риск обычно определяется в терминах ***источников риска*** (3.4). потенциальных ***событий*** (3.5). ***последствий*** этих событий (3.6) и их ***вероятности*** (3.7).

3.2
Менеджмент риска, риск-менеджмент (risk-management)
Скоординированные действия по управлению организацией с учетом ***риска*** (3.1)

3.3
Заинтересованная сторона (stakeholder)
Лицо или организация, которые могут воздействовать, или подвергаться воздействию, или которые считают, что подвергаются воздействию какого-либо решения или деятельности.

Примечание: Термин «Стейкхолдер» может использоваться в качестве синонима термина «Заинтересованная сторона».

3.4
Источник риска (risk source)
Элемент, который по отдельности или в сочетании с другими может приводить к возникновению ***риска*** (3.1)

3.5
Событие (event)
Возникновение или изменение ряда определенных обстоятельств

Примечание 1: Событие может иметь одно или несколько происхождений и может иметь несколько причин и несколько ***последствий*** (3.6).

Примечание 2: Событие также может заключаться в том, что не происходит что-то ожидаемое или происходит что-то непредвиденное.

Примечание 3: Событие может являться ***источником риска*** (3.4).

3.6
Последствие (consequence)
Результат события (3.5), влияющий на цели

Примечание 1: Последствие может быть определенным или неопределенным и иметь положительное или отрицательное влияние на цели.

Примечание 2: Последствия могут быть выражены качественно или количественно.

Примечание 3: Любые последствия могут обостряться в силу эффекта каскада и кумулятивных эффектов.

3.7
Вероятность, возможность (likelihood)
Шанс того, что что-то может произойти

Примечание 1: В терминологии риск-менеджмента (3.2) термин «вероятность» или «возможность» означает шанс того, что что-то может произойти, независимо от того, установлено ли это, измерено или определено объективно или субъективно, качественно или количественно, и описывается ли с помощью общих понятий или математически (например, как вероятность или частота за данный период времени).

Примечание 2: Английский термин «likelihood» не имеет прямого перевода на некоторые языки: вместо этого часто используется перевод слова «probability». Однако в английском языке термин «probability» часто понимают в узком математическом смысле. Поэтому в терминологии риск-менеджмента термин «likelihood» используется с той целью, чтобы придать ему настолько же широкий смысл, какой имеет слово «probability» во многих языках, кроме английского.

3.8
Контроль риска (control)
Мера, которая сдерживает и/или модифицирует (изменяет) ***риск*** (3.1)

Примечание 1: Контроль риска может включать любой процесс, политику, методику, практику или другие условия и/или действия, сдерживающие и/или модифицирующие (изменяющие) риск (но не ограничивается перечисленным).

Примечание 2: Контроль риска может не всегда приводить к желаемому или ожидаемому эффекту.

4 Принципы

Целью риск-менеджмента является создание и защита стоимости. Риск-менеджмент улучшает производительность, стимулирует инновации и способствует достижению целей.

Принципы, представленные на рисунке 2, устанавливают характеристики эффективного и результативного риск-менеджмента, отражая его ценность и объясняя его назначение и цель. Эти принципы являются основой риск-менеджмента и должны учитываться при создании структуры и процессов риск-менеджмента организации. Эти принципы должны позволить организации управлять влиянием неопределенности на ее цели.

Рисунок 2 — Принципы

Эффективный риск-менеджмент должен соответствовать характеристикам, представленным на рисунке 2, которые могут быть дополнительно объяснены следующим образом:

а) Интегрированный

Риск-менеджмент является неотъемлемой частью деятельности организации.

б) Структурированный и всеобъемлющий

Структурированный и комплексный подход к риск-менеджменту приводит к согласующимся и сопоставимым результатам.

в) Адаптируемый

Структура и процесс риск-менеджмента соотносятся и настраиваются с учетом внешнего и внутреннего контекста организации, связанного с ее задачами.

г) Инклюзивный

Соответствующее и своевременное вовлечение заинтересованных сторон позволяет учитывать их знания, взгляды и мнения. Это приводит к повышению осведомленности и обоснованности риск-менеджмента.

д) Динамичный

Риски могут возникать, меняться или исчезать по мере изменения внешнего и внутреннего контекста организации. Риск-менеджмент предвосхищает, обнаруживает, признает и реагирует на эти изменения и события соответствующим образом и своевременно.

е) Основанный на наилучшей доступной информации

В качестве входных данных для процесса риск-менеджмента применяются исторические и фактические данные, а также прогнозные ожидания. Риск-менеджмент явно учитывает любые ограничения и неопределенности, связанные с имеющимися данными и ожиданиями. Используемая информация должна быть актуальной, ясной и доступной для заинтересованных сторон.

ж) Учитывающий человеческие и культурные факторы

Человеческое поведение и культура существенно влияют на все аспекты риск-менеджмента на каждом уровне и этапе.

з) Постоянно улучшаемый

Риск-менеджмент постоянно совершенствуется благодаря обучению и накоплению опыта.

5 Структура

5.1 Общие положения

Целью структуры риск-менеджмента является оказание содействия организации во внедрении риск-менеджмента во все сферы ее деятельности и функции. Эффективность риск-менеджмента будет зависеть от его интеграции в систему управления организацией, включая процесс принятия решений. Это требует поддержки со стороны заинтересованных сторон, особенно высшего руководства.

Разработка структуры включает в себя внедрение (интеграцию), разработку, реализацию, оценку и улучшение риск-менеджмента в организации. На рисунке 3 показаны компоненты структуры.

Рисунок 3 – Структура

Организация должна оценить свои существующие методы и процессы риск-менеджмента, выявить любые пробелы в структуре и устранить их.

Компоненты структуры и их взаимодействие должны быть настроены под потребности организации.

5.2 Лидерство и ответственность

Высшему руководству и надзорным органам (в применимых случаях) следует обеспечивать интеграцию риск-менеджмента во все виды деятельности организации и демонстрировать лидерство и ответственность путем:

- адаптации и внедрения всех компонентов структуры;

- утверждения положения или политики, устанавливающих подход, план или порядок действий в части риск-менеджмента;

- обеспечения выделения необходимых ресурсов для риск-менеджмента;

- установления полномочий, ответственности и подотчетности на соответствующих уровнях организации.

Это поможет организации:

- согласовать риск-менеджмент с целями, стратегией и культурой организации;

- признавать и выполнять все свои обязательства, в том числе добровольные;

- установить величину и тип рисков, которые организация может или не может принять, для обеспечения разработки критериев риска, при условии, что соответствующая информация доведена до сведения заинтересованных сторон и внутри организации;

- доводить до сведения заинтересованных сторон информацию о ценности риск-менеджмента;

- стимулировать систематический мониторинг рисков;

- обеспечить соответствие структуры риск-менеджмента контексту организации.

Высшее руководство отвечает за управление рисками, в то время как надзорные органы отвечают за контроль над риск-менеджментом. От надзорных органов ожидается и требуется:

- обеспечение адекватного учета рисков при определении целей организации;

- понимание рисков, с которыми организация сталкивается при достижении своих целей;

- обеспечение внедрения и эффективного функционирования систем управления такими рисками;

- обеспечение соответствия таких рисков целям организации;

- обеспечение надлежащего обмена информацией о таких рисках и их управлении.

5.3 Интеграция

Интеграция риск-менеджмента основана на понимании организационных структур и контекста. Структуры различаются в зависимости от цели, задач и сложности организации. Управление рисками осуществляется в каждой части структуры организации. Каждый человек в организации несет ответственность за управление рисками.

Принципы корпоративного управления направляют деятельность организации, ее внешние и внутренние отношения, а также определяют правила, процессы и процедуры, необходимые для достижения цели организации. Структуры управления преобразуют принципы корпоративного управления в стратегию и связанные с ней цели, необходимые для достижения желаемых показателей устойчивости и долгосрочной жизнеспособности. Определение ролей, обеспечивающих подотчетность и контроль внутри организации, является неотъемлемой частью корпоративного управления.

Интеграция риск-менеджмента в организацию представляет собой динамичный и итеративный процесс, который должен учитывать потребности и культуру организации. Риск-менеджмент должен быть неотъемлемой частью целей организации, корпоративного управления, лидерства и ответственности, стратегии, задач и деятельности организации и не должен отделяться от них.

5.4 Разработка

5.4.1 Понимание организации и ее контекста

При разработке структуры риск-менеджмента организации следует изучить и понять ее внешний и внутренний контекст.

В процессе изучения внешнего контекста организации рассматриваются, в том числе, следующие факторы:

- социальные, культурные, политические, правовые, регулирующие, финансовые, технологические, экономические и экологические факторы на международном, национальном, региональном или местном уровнях;

- основные движущие силы и тренды, влияющие на цели организации;

- взаимосвязи с внешними заинтересованными сторонами, их восприятия, ценности, потребности и ожидания;

- контрактные отношения и обязательства;

- сложность цепочек связей и зависимостей.

В процессе изучения внутреннего контекста организации рассматриваются, в том числе, следующие факторы:

- видение, миссия и ценности организации;

- управление, организационная структура, роли и обязанности;

- стратегия, цели и политики;

- культура организации;

- стандарты, руководства и модели, принятые организацией;

- потенциальные возможности, понимаемые как ресурсы и знания (например, капитал, время, люди, интеллектуальная собственность, процессы, системы и технологии);

- данные, информационные системы и информационные потоки;

- взаимосвязи с внутренними заинтересованными сторонами с учетом их восприятия и ценностей;

- контрактные отношения и обязательства;

- взаимозависимости и взаимосвязи.

5.4.2 Демонстрация приверженности управлению рисками

Высшему руководству и надзорным органам (в применимых случаях) следует демонтировать постоянную приверженность управлению рисками. Это может быть реализовано посредством политики, программного заявления или иным способом, четко отражающим цели и приверженность организации риск-менеджменту. Приверженность риск-менеджменту должна включать, но может не ограничиваться следующим:

- нацеленность организации на управление рисками и связи с ее целями и другими политиками;

- укрепление потребности в интеграции риск-менеджмента в общую культуру организации;

- проведение процедур интеграции риск-менеджмента в основные виды деятельности и процессы принятия решений;

- определение полномочий, ответственности и подотчетности;

- обеспечение доступа к необходимым ресурсам;

- способы решения конфликтных задач;

- измерение показателей эффективности организации и отчетность по ним;

- пересмотр и улучшение.

Приверженность риск-менеджменту следует подобающим образом распространять внутри организации и доводить до сведения заинтересованных сторон.

5.4.3 Определение организационных функций, полномочий, ответственности и подотчетности

Высшему руководству и надзорным органам (в применимых случаях) следует обеспечивать, чтобы полномочия, ответственность и подотчетность для соответствующих ролей в отношении управления рисками определялись и доводились до сведения соответствующих лиц на всех уровнях организации, а также необходимо:

- акцентировать внимание на том, что риск-менеджмент является основной обязанностью;

- определить лиц, подотчетных и имеющих полномочия по управлению рисками (владельцы рисков).

5.4.4 Распределение ресурсов

Высшему руководству и надзорным органам (в применимых случаях) следует распределять соответствующие ресурсы для управления рисками, которые могут включать, но не ограничиваются следующим:

- люди, навыки, опыт и компетентность;

- процессы, методы и инструменты организации, используемые для риск-менеджмента;

- документированные процессы и процедуры;

- системы управления информацией и знаниями;

- профессиональное развитие и обучение.

Организации следует учитывать возможности и ограничения существующих ресурсов.

5.4.5 Установление механизмов обмена информацией и консультирования

Организации следует установить согласованный подход к обмену информацией и консультированию для поддержки структуры и содействия эффективному применению риск-менеджмента. Коммуникация предполагает обмен информацией с целевой аудиторией. Консультирование также подразумевает получение обратной связи от участников этого процесса с целью ее учета при принятии решений и осуществлении других видов деятельности. Методы обмена информацией и консультирования, а также их содержимое должны, когда это уместно отражать ожидания заинтересованных сторон.

Обмен информацией и консультирование должны быть своевременными и обеспечивать, чтобы соответствующая информация была собрана, сопоставлена, обобщена и распределена соответствующим образом, а также, чтобы была предоставлена обратная связь и проведены улучшения.

5.5 Реализация

Организации следует реализовать структуру риск-менеджмента посредством:

- разработки соответствующего плана с определением сроков и ресурсов;

- определения того, где, когда, как и кем принимаются различные типы решений в организации;

- модификации (изменения) применимых процессов принятия решений (при необходимости);

- обеспечения понимания и правильного применения механизмов управления рисками организации.

Успешное внедрение структуры требует участия и осведомленности заинтересованных сторон. Это позволяет организациям прямо учитывать неопределенность при принятии решений, а также обеспечивать, чтобы любая новая или последующая неопределенность была принята во внимание по мере возникновения.

Надлежащим образом спроектированная и применяемая структура риск-менеджмента обеспечивает его внедрение во все виды деятельности организации, включая процесс принятия решений, а также надлежащий учет изменений во внешнем и внутреннем контексте.

5.6 Оценка

С целью оценки эффективности структуры риск-менеджмента, организации следует:

- проводить периодическую оценку эффективности структуры риск-менеджмента с точки зрения ее цели, планов реализации, показателей и предполагаемого поведения;

- определять, по-прежнему ли она содействует достижению целей организации.

5.7 Улучшение

5.7.1 Адаптация

Организации следует обеспечивать постоянный мониторинг и адаптацию структуры риск-менеджмента для реагирования на внешние и внутренние изменения. Действуя таким образом, организация может улучшить показатели своей стоимости.

5.7.2 Постоянное совершенствование

Организации следует постоянно улучшать соответствие, адекватность и эффективность структуры риск-менеджмента и совершенствовать способы интегрирования процесса риск-менеджмента в свою деятельность.

По мере выявления соответствующих недостатков или возможностей улучшения организации следует разрабатывать планы и задачи и поручать их выполнение ответственным за реализацию. После реализации эти улучшения должны способствовать совершенствованию риск-менеджмента.

6 Процесс

6.1 Общие положения

Процесс риск-менеджмента предполагает систематическое применение политик, процедур и практик для обеспечения обмена информацией и консультирования, определения контекста, а также оценки рисков, воздействия на риски, мониторинга, анализа и документирования рисков, а также ведения отчетности по рискам. Процесс риск-менеджмента показан на рисунке 4.

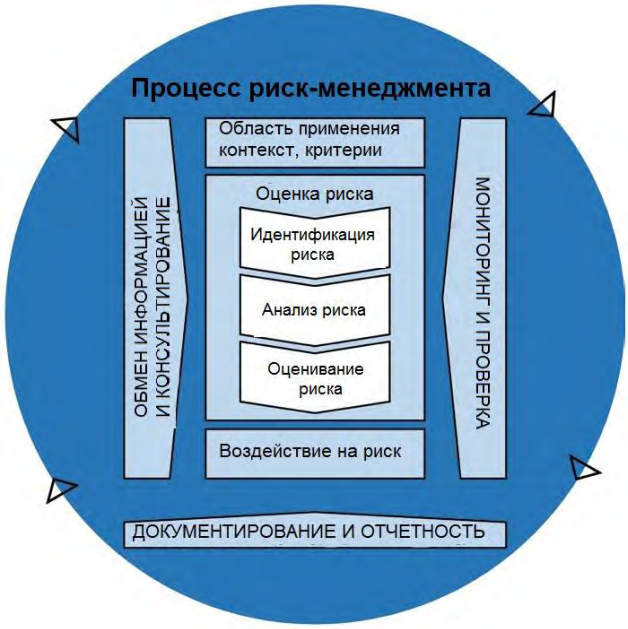

Рисунок 4 – Процесс

Процесс риск-менеджмента должен быть неотъемлемой частью процессов управления и принятия решений и должен быть интегрирован в структуру, деятельность и процессы организации. Он может применяться на стратегическом, операционном, программном или проектном уровнях.

В рамках организации процесс риск-менеджмента может иметь множество вариантов применения, адаптированных с учетом необходимости достижения целей организации, а также внешнего и внутреннего контекста.

На протяжении всего процесса риск-менеджмента следует учитывать динамичный и переменчивый характер поведения и культуры человека.

Хотя процесс управления рисками зачастую представляют последовательным, в действительности он является итеративным.

6.2 Обмен информацией и консультирование

Целью обмена информацией и консультирования является оказание заинтересованным сторонам содействия в понимании риска, предпосылок, на основании которых принимаются решения, и причин, по которым требуются определенные действия. Обмен информацией направлен на повышение осведомленности и обеспечение понимания риска, тогда как консультирование включает получение обратной связи и информации для обоснования принимаемых решений. Тесное взаимодействие этих двух процессов должно способствовать фактическому, своевременному, актуальному, точному и понятному обмену информацией с учетом конфиденциальности и целостности информации, а также прав частных лиц на неприкосновенность личной жизни.

Обмен информацией и консультирование с соответствующими внешними и внутренними заинтересованными сторонами должны проводиться на всех этапах процесса риск-менеджмента.

Обмен информацией и консультирование проводятся с целью:

- сведения разных областей экспертных знаний воедино для каждого этапа процесса риск-менеджмента;

- обеспечения надлежащего учета различных взглядов при определении критериев риска и оценке рисков;

- предоставления достаточной информации для облегчения контроля за рисками и принятия решений;

- создания чувства вовлеченности и причастности среди лиц, подвергшихся воздействию риска.

6.3 Область применения, контекст и критерии

6.3.1 Общие положения

Целью определения области применения, контекста и критериев является настройка процесса управления рисками для обеспечения эффективной оценки риска и соответствующего воздействия на него. Область применения, контекст и критерии подразумевают определение сферы охвата процесса и понимание внешнего и внутреннего контекста.

6.3.2 Определение области применения

Организации следует определить область применения своей деятельности по риск-менеджменту.

Поскольку процесс риск-менеджмента может применяться на разных уровнях (например, стратегическом, операционном, программном, проектном или др.), важно четко понимать затрагиваемую риск-менеджментом сферу охвата, соответствующие цели, которые необходимо учитывать, и их согласованность с целями организации.

При планировании подхода необходимо учитывать следующее:

- цели и решения, которые необходимо принять;

- ожидаемые результаты от шагов, предпринимаемых в рамках этого процесса;

- время, местоположение, определенные допущения и исключения;

- соответствующие инструменты и методы оценки рисков;

- требуемые ресурсы, зоны ответственности и документацию (отчетность);

- взаимное влияние с другими проектами, процессами и действиями.

6.3.3 Внешний и внутренний контекст

Внешний и внутренний контекст – это среда, в которой организация определяет свои цели и стремится их достичь.

Контекст процесса управления рисками должен определяться из понимания внешней и внутренней среды, в которой работает организация, и должен отражать определенную среду деятельности, к которой применяется процесс управления рисками.

Понимание контекста важно, поскольку:

- управление рисками происходит с учетом целей и деятельности организации;

- организационные факторы могут являться источниками риска;

- цель и область применения процесса управления рисками могут быть взаимосвязаны с целями организации в целом.

Организации следует устанавливать внешний и внутренний контекст процесса управления рисками путем рассмотрения факторов, упомянутых в п. 5.4.1.

6.3.4 Определение критериев риска

Организации следует уточнить величину и тип риска, который она может или не может принять с учетом поставленных целей. Также ей следует определить критерии оценки значимости риска и обосновать процесс принятия решений. Критерии риска должны быть согласованы со структурой риск-менеджмента и адаптированы под определенные цели и сферу охвата рассматриваемой деятельности. Критерии риска должны отражать ценности организации, ее цели и ресурсы и соответствовать политике управления рисками организации и ее положениям о риск-менеджменте. Критерии должны определяться с учетом обязательств организации и мнений заинтересованных сторон.

Хотя критерии риска следует устанавливать в начале процесса оценки риска, они являются динамичными и должны постоянно пересматриваться, и, в случае необходимости, корректироваться.

Чтобы установить критерии риска, следует учитывать следующее:

- характер и тип неопределенностей, которые могут повлиять на результаты и цели (как материальные, так и нематериальные);

- способ определения и измерения последствий (как положительных, так и отрицательных) и вероятности;

- факторы, связанные со временем;

- согласованность в использовании измерений;

- порядок определения уровня риска;

- метод учета комбинаций и последовательностей множественных рисков;

- потенциал организации.

6.4 Оценка риска

6.4.1 Общие положения

Оценка риска – это полный процесс идентификации, анализа и оценивания риска.

Оценку риска следует проводить систематически, итеративно и совместно, опираясь на знания и мнения заинтересованных сторон. При оценке необходимо использовать наилучшую доступную информацию, дополняя ее при необходимости данными дополнительных исследований.

6.4.2 Идентификация риска

Цель идентификации рисков заключается в поиске, определении и описании рисков, которые могут помочь или помешать организации в достижении ее целей. Для идентификации рисков важно использовать надлежащую, соответствующую и актуальную информацию.

Организация может использовать ряд методов для идентификации неопределенностей, которые могут повлиять на достижение ей одной или нескольких целей. При этом следует учитывать следующие факторы и взаимосвязь между ними:

- материальные и нематериальные источники риска;

- причины и события;

- угрозы и возможности;

- уязвимости и способности;

- изменения внешнего и внутреннего контекста;

- индикаторы возникающих рисков;

- характер и стоимость активов и ресурсов;

- последствия и их влияние на цели;

- ограниченность знаний и достоверности информации;

- факторы, связанные со временем;

- предубеждения, допущения и убеждения вовлеченных лиц.

Организации следует идентифицировать риски, независимо от того, находятся ли источники этих рисков под ее контролем. Следует учитывать возможность нескольких исходов, что может привести к множеству различных материальных или нематериальных последствий.

6.4.3 Анализ риска

Цель анализа рисков заключается в том, чтобы понять характер риска и его особенности, включая, когда это необходимо, уровень риска. Анализ рисков включает подробное рассмотрение неопределенностей, источников риска, последствий, вероятности, событий, сценариев, средств контроля и их эффективности. Событие может иметь различные причины и последствия и может влиять на различные цели.

Анализ риска может проводиться с различной степенью детализации и сложности, в зависимости от цели анализа, доступности и достоверности информации и располагаемых ресурсов. Методы анализа могут быть качественными, количественными или их комбинациями, в зависимости от конкретных обстоятельств и предполагаемого использования результатов.

Анализ риска следует проводить с учетом таких факторов, как:

- вероятность событий и последствий;

- характер и масштабы последствий;

- сложность и связность компонентов;

- факторы, связанные со временем, и волатильность;

- эффективность существующих средств контроля;

- чувствительность и достоверность.

На анализ рисков может влиять любое расхождение мнений, предвзятость, восприятие риска и суждения. Дополнительное влияние оказывают качество используемой информации, допущения и исключения, любые ограничения методов и способов их реализации. Эти факторы необходимо изучать, документировать и сообщать лицам, ответственным за принятие решений.

Определение количественной оценки событий с высокой неопределенностью может быть затруднительным, что может являться проблемой при анализе событий с серьезными последствиями. В таких случаях использование комбинации методов обычно обеспечивает более глубокое понимание.

Анализ риска обеспечивает вклад в общий процесс оценки риска и принятия решений относительно того, следует ли воздействовать на риск и как, а также какая стратегия и методы реагирования на риск будут наиболее подходящими. Результаты анализа позволяют понимать решения, которые предполагают выбор, а возможные варианты включают различные типы и уровни риска.

6.4.4 Оценивание риска

Целью оценивания риска является содействие принятию решений. Оценивание риска включает сравнение результатов анализа риска с установленными критериями риска для определения необходимости дополнительных действий. Этот процесс может привести к решению:

- более ничего не предпринимать;

- рассмотреть возможные варианты воздействия на риск;

- провести дальнейший анализ, чтобы лучше понять риск;

- поддерживать существующие средства контроля;

- пересмотреть цели.

Решения должны учитывать более широкий контекст и объективные и субъективные последствия для внешних и внутренних заинтересованных сторон.

Результаты оценки риска должны быть документированы, донесены до заинтересованных сторон, а затем проверены на соответствующих уровнях организации.

6.5 Воздействие на риск

6.5.1 Общие положения

Цель воздействия на риск заключается в выборе и применении вариантов реагирования на риск.

Воздействие на риск представляет собой итеративный процесс, включающий:

- определение и выбор вариантов воздействия на риск;

- планирование и выполнение воздействия на риск;

- оценка эффективности такого воздействия;

- принятие решения о приемлемости остаточного риска;

- в случае, если уровень остаточного риска не приемлем, проведение дальнейшего воздействия.

6.5.2 Выбор вариантов воздействия на риск

Выбор наиболее подходящего варианта или вариантов воздействия на риск предусматривает сопоставление выгод, ожидаемых от достижения целей воздействия на риск, с затратами, усилиями и недостатками реализации в ходе воздействия.

Варианты воздействия на риск не обязательно являются взаимоисключающими или подходящими при всех обстоятельствах. Воздействие на риск может осуществляться одним или несколькими из следующих вариантов:

- избежание риска посредством принятия решения не начинать или не продолжать деятельность, которая порождает риск;

- принятие или увеличение риска для использования благоприятной возможности;

- устранение источника риска;

- изменение вероятности;

- изменение последствий;

- разделение риска с другой стороной или сторонами (например, с помощью договоров, страхования);

- осознанное удержание риска.

Обоснование необходимости воздействия на риск выходит за рамки исключительно экономических соображений и должно учитывать все обязательства организации, добровольные обязательства и мнения

заинтересованных сторон. Выбор вариантов воздействия на риск должен производиться в соответствии с целями организации, критериями риска и доступными ресурсами.

При выборе вариантов воздействия на риск организация должна учитывать ценности, восприятие и потенциальное вовлечение заинтересованных сторон, а также наиболее подходящие способы обмена информацией и консультирования с ними. Некоторые варианты воздействия на риск могут быть более приемлемыми с точки зрения отдельных заинтересованных сторон, чем другие, являющиеся столь же эффективными.

Воздействие на риск, даже тщательно проработанное и осуществленное, может не дать ожидаемых результатов и может привести к непредвиденным последствиям. Мониторинг и пересмотр должны быть неотъемлемой частью реализации воздействия на риск для обеспечения гарантии, что различные формы воздействия станут и будут оставаться эффективными.

Воздействие на риск также может привести к возникновению новых рисков, которыми необходимо будет управлять.

Если нет доступных вариантов воздействия на риск или если варианты воздействия недостаточно модифицируют (изменяют) риск, такой риск следует документировать и держать под постоянным контролем.

Лица, принимающие решения, и другие заинтересованные стороны должны быть осведомлены о характере и степени остаточного риска после осуществления воздействия. Остаточный риск должен быть документирован и подвергнут мониторингу, обзору и, при необходимости, дальнейшему воздействию.

6.5.3 Подготовка и реализация планов воздействия на риск

Цель планов воздействия на риск заключается в том, чтобы определить порядок реализации выбранных вариантов воздействия, так, чтобы мероприятия были поняты участниками этого процесса и имелась возможность контролировать прогресс по исполнению плана. План воздействия должен четко определять порядок, в соответствии с которым следует осуществлять воздействие на риск.

Планы воздействия следует интегрировать в управленческие планы и процессы организации с учетом консультирования с соответствующими заинтересованными сторонами.

Информация, содержащаяся в плане воздействия, должна включать следующее:

- обоснование выбора вариантов воздействия, включая указание ожидаемых выгод;

- указание подотчетных и ответственных за утверждение и реализацию плана лиц;

- предлагаемые действия;

- требуемые ресурсы, включая непредвиденные расходы;

- показатели эффективности;

- ограничения;

- требования к отчетности и мониторингу;

- сроки реализации и выполнения действий.

6.6 Мониторинг и пересмотр

Цель мониторинга и пересмотра заключается в обеспечении и повышении качества и эффективности разработки, реализации и результатов процесса. Постоянный мониторинг и периодический пересмотр процесса управления рисками и его результатов должны быть запланированной частью процесса управления рисками, в отношении которой установлена четко определенная ответственность.

Мониторинг и пересмотр должны проводиться на всех этапах процесса. Мониторинг и пересмотр включают в себя планирование, сбор и анализ информации, документирование результатов и предоставление обратной связи.

Результаты мониторинга и пересмотр должны являться частью деятельности по общему управлению организацией, оценке эффективности, а также составлению отчетности.

6.7 Документирование и отчетность

Процесс риск-менеджмента и его результаты следует документировать и отображать в отчетности с помощью соответствующих механизмов. Документирование и отчетность направлены на:

- обмен информацией о мероприятиях и результатах риск-менеджмента в организации;

- предоставление информации для принятия решений;

- совершенствование деятельности по риск-менеджменту;

- содействие взаимодействию с заинтересованными сторонами, в том числе ответственными и подотчетными за деятельность риск-менеджменту.

Решения, касающиеся создания, хранения и обработки документированной информации, должны учитывать, помимо прочего, их использование, конфиденциальность информации, внешний и внутренний контекст.

Отчетность является неотъемлемой частью управления организацией и должна повышать качество диалога с заинтересованными сторонами и содействовать высшему руководству и надзорным органам в выполнении ими своих обязанностей. Факторы, которые следует учитывать для отчетности, включают, но не ограничиваются следующими:

- различия заинтересованных сторон, их специфических потребностей в информации и требований к ней;

- стоимость, периодичность и своевременность отчетности;

- метод отчетности;

- соответствие информации целям организации и ее релевантность для принятия решений.

Библиография

[1]IEC 31010, *Risk management — Risk assessment techniques* (*И*СО/МЭК 31010. Менеджмент риска. Методы оценки риска.)