МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO 31000

Вторая редакция
2018-02

Управление рисками - Руководство

Management du risque — Lignes directrices

Логотип ISO

Номер для ссылки
ISO 31000:2018

А. Горбунов
Ред. 20.04.2019

Содержание

Страница

Предисловие iv
Введение v
1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Принципы 2
5 Структура системы управления рисками 4
5.1 Общие положения 4
5.2 Лидерство и обязательства 5
5.3 Интеграция 5
5.4 Разработка 6
5.4.1 Понимание организации и ее контекста 6
5.4.2 Выражение приверженности управлению рисками 6
5.4.3 Назначение ролей, полномочий, ответственности за выполнение и результаты 7
5.4.4 Распределение ресурсов 7
5.4.5 Определение порядка коммуникаций и консультаций 7
5.5 Внедрение 8
5.6 Оценка 8
5.7 Улучшение 8
5.7.1 Адаптация 8
5.7.2 Постоянное улучшение 8
6 Процесс 9
6.1 Общие положения 9
6.2 Коммуникации и консультации 10
6.3 Область действия, контекст и критерии 10
6.3.1 Общие положения 10
6.3.2 Определение области действия 10
6.3.3 Внешний и внутренний контекст 11
6.3.4 Определение критериев риска 11
6.4 Оценка риска 11
6.4.1 Общие положения 11
6.4.2 Идентификация риска 12
6.4.3 Анализ риска 12
6.4.4 Оценка риска 13
6.5 Обработка риска 13
6.5.1 Общие положения 13
6.5.2 Выбор вариантов обработки риска 14
6.5.3 Подготовка и выполнение планов обработки рисков 14
6.6 Мониторинг и анализ 15
6.7 Регистрация результатов и отчетность 15
Библиография 17

Предисловие

ISO (International Organization for Standardization – Международная Организация по Стандартизации) является всемирной федерацией национальных органов по стандартизации (органов-членов ISO). Работа над подготовкой Международных Стандартов выполняется, как правило, техническим комитетом ISO. Каждый орган-член ISO, заинтересованный в цели, для которой был создан технический комитет, имеет право быть представленным в данном комитете. Международные организации, правительственные и неправительственные, поддерживающие связь с ISO, также принимают участие в работе. ISO также тесно сотрудничает с Международной Электротехнической Комиссией (IEC), ведется совместная работа по всем вопросам электротехнической стандартизации.

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

Особое внимание уделено тому, что некоторые элементы данного документа могут являться предметом патентных прав. ISO не должна 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 патентных деклараций ISO (см. www.iso.org/patents).

Все торговые марки, упомянутые в настоящем документе, приведены для удобства пользователей и не означают рекомендации (одобрения).

Для разъяснения значений, используемых ISO специфических терминов и выражений, связанных с оценкой соответствия, равно как и информации о соблюдении ISO принципов соглашения Всемирной Торговой Организации (ВТО) по техническим барьерам в торговле (ТБТ) см. по следующей ссылке: www.iso.org/iso/foreword.html.

Данный документ подготовлен Техническим Комитетом ISO/TC 262, *Риск-менеджмент*.

Эта вторая редакция отменяет и заменяет первую редакцию (ISO 31000:2009), которая была подвергнута техническому пересмотру.

Основные изменения по сравнению с предыдущей редакцией следующие:

- пересмотр принципов менеджмента рисков, которые являются ключевыми критериями его успеха;

- акцент на лидерство высшего руководства и встраивание риск-менеджмента, начиная с управления организацией;

- больший акцент на итеративный характер управления рисками, учитывая, что новый опыт, знания и анализ могут вести к пересмотру составных элементов процесса, задач и средств управления на каждой стадии процесса;

- оптимизация содержания с большим акцентом на поддержание модели открытых систем, чтобы соответствовать множественным потребностям и контекстам.

Введение

Данный документ предназначен для использования теми, кто создает и сохраняет ценности в организациях посредством управления рисками, принятия решений, постановкой и достижением целей и улучшением общего функционирования.

Организации всех типов и размеров сталкиваются с внешними и внутренними факторами и воздействиями, которые вносят неопределенность в достижение их целей.

Управление рисками является итеративным и помогает организациям в определении стратегии, достижении целей и принятии обоснованных решений.

Менеджмент риска является частью системы управления и элементом проявления лидерства и имеет основополагающее значение с точки зрения того, как организация управляется на всех уровнях. Он способствует совершенствованию систем менеджмента.

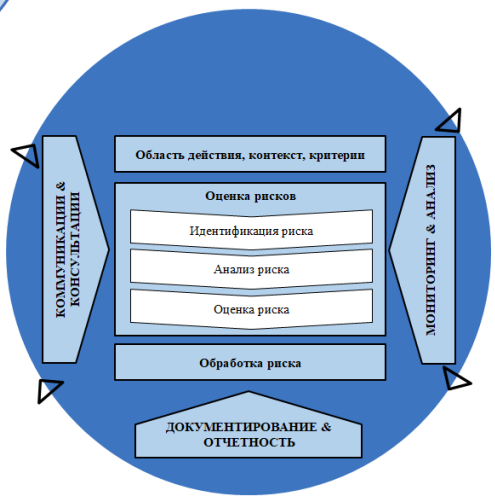
Менеджмент риска является частью всех действий, связанных с организацией, и включает взаимодействие с заинтересованными сторонами.

Менеджмент риска учитывает внешний и внутренний контекст организации, включая факторы, связанные с поведением людей и культурой.

Менеджмент риска основан на принципах, структуре и процессе, описанных в данном документе, как это показано на Рисунке 1. Указанные на нем компоненты могут уже иметься в организации полностью или частично, однако их, возможно, потребуется адаптировать или усовершенствовать с тем, чтобы управление рисками было эффективным, результативным и согласованным.

Принципы (раздел 4)

Структура (раздел 5)



Процесс (раздел 6)

Рисунок 1 - Принципы, структура и процесс

Управление рисками - Руководство

1 Область применения

Данный документ содержит руководство по управлению рисками, с которыми сталкиваются организации. Применение этих руководящих указаний может быть адаптировано для любой организации и ее контекста.

Данный документ предлагает общий подход к управлению любым типом риска и не является специфичным для какой-либо отрасли или сектора рынка.

Данный документ может использоваться на протяжении всего жизненного цикла организации и может применяться к любой деятельности, включая принятие решений на всех уровнях.

2 Нормативные ссылки

Данный документ не содержит нормативных ссылок

3 Термины и определения

Для целей настоящего документа применяются следующие термины и определения.

ISO и IEC поддерживают терминологическую базу данных для применения в сфере стандартизации по следующим адресам:

— платформа ISO Online browsing: доступна на http://www.iso.org/obp

— IEC Electropedia: доступна на http://www.electropedia.org/.

3.1

риск (risk)

влияние неопределенности на цели

Примечание 1 к определению: Влияние рассматривается как отклонение от ожидаемого. Оно может быть с позитивными или негативными последствиями, а также с теми, и другими, и может создавать или выступать в форме возможностей и угроз.

Примечание 2 к определению: Цели могут иметь различные аспекты, относиться к разным категориям и применяться на различных уровнях.

Примечание 3 к определению: Риск обычно определяется с точки зрения *источников риска* (3.4), возможных *событий* (3.5), их *последствий* (3.6) и их *вероятности* (3.7).

3.2

управление рисками[*] (risk management)

скоординированные действия для управления организацией в отношении *рисков* (3.1)

3.3

заинтересованная сторона (stakeholder)

лицо или организация, которые могут влиять на решения или действия, на которых могут влиять или они полагают, что на них могут влиять решения или действия

Примечание 1 к определению: Наряду с термином «stakeholder» может использоваться термин «interested party»

[*] В тексте стандарта термины «управление риском» и «риск-менеджмент» используются как синонимы [прим. переводчика]

3.4

источник риска (risk source)

элемент, который сам по себе или в комбинации с другими может приводить к возникновению *риска* (3.1)

3.5

событие (event)

возникновение или изменение определенного набора обстоятельств

Примечание 1 к определению: Событие может происходить один или более раз, может иметь несколько причин и *последствий* (3.6).

Примечание 2 к определению: Событием также может быть то, что ожидалось, но не произошло, либо не ожидалось, но произошло.

Примечание 3 к определению: Событие может быть источником риска.

3.6

последствие (consequence)

результат *события* (3.5), влияющий на цели

Примечание 1 к определению: Последствие может быть определенным или неопределенным и иметь позитивное или негативное, прямое или косвенное влияние на цели.

Примечание 2 к определению: Последствия могут быть выражены качественно и количественно.

Примечание 3 к определению: Любые последствия могут нарастать вследствие эффекта «домино» и кумулятивного эффекта.

3.7

вероятность (likelihood)

возможность того, что что-то произойдет

Примечание 1 к определению: В терминологии *управления рисками* (3.2) слово «вероятность» используется для указания на возможность того, что что-то произойдет, независимо от того, устанавливается, измеряется или рассчитывается она объективно или субъективно, количественно или качественно, и описывается общими словами или математически (например, как вероятность или частота за определенный период времени).

Примечание 2 к определению: английский термин «likelihood» во многих языках не имеет прямого эквивалента; в то время как термин «probability» имеет такой эквивалент и часто используется. Однако в английском языке термин «probability» зачастую ограничен применением в качестве математического термина. Поэтому в терминологии управления рисками термин «likelihood» используется в предположении, что он будет иметь более широкий смысл, аналогичный смыслу термина «probability» во многих языках, за исключением английского.

3.8

средство управления (control)

мера, которая направлена на удержание на определенном уровне и/или изменение *риска* (3.1)

Примечание 1 к определению: Средства управления включают, но не ограничиваются этим, любой процесс, политику, устройство, процедуру или другие условия и/или действия, которые удерживают на определенном уровне и/или изменяют риск.

Примечание 2 к определению: Средства управления не всегда могут приводить к запланированным или предполагаемым изменениям.

4 Принципы

Целью управления рисками является создание и сохранение ценности. Оно повышает результативность работы, поощряет инновации и обеспечивает достижение целей.

Принципы, показанные на Рисунке 2, дают понимание характеристик результативного и эффективного управления рисками, поясняя его ценность, намерения и цели. Эти принципы являются основой для управления рисками и должны учитываться при разработке структуры и процессов управления рисками организации. Эти принципы должны позволять организации управлять влияниями неопределенности на ее цели.

Рисунок 2 — Принципы

Результативное управление рисками требует наличия элементов, показанных на Рисунке 2, и может быть дополнительно объяснено следующим образом.

a) Интегрированность

Управление рисками является неотъемлемой частью всей деятельности организации.

b) Структурированность и полнота

Структурированный и комплексный подход к управлению рисками способствует получению согласованных и сопоставимых результатов.

c) Настраиваемость

Структура системы и процесс управления рисками настраиваются и соответствуют внешнему и внутреннему контексту организации, связанному с ее целями.

d) Вовлеченность

Соответствующее и своевременное участие заинтересованных сторон позволяет учитывать их знания, мнения и представления. Это приводит к повышению осведомленности и обоснованности управления рисками.

e) Динамичность

Риски могут возникать, меняться или исчезать по мере изменения внешнего и внутреннего контекста организации. Управление рисками прогнозирует, выявляет, подтверждает и реагирует

на эти изменения и события своевременно и соответствующим образом.

f) Наилучшая доступная информация

Исходные данные для управления рисками основываются на информации о прошлом и текущей информации, а также на будущих ожиданиях. Управление рисками явным образом учитывает любые ограничения и неопределенности, связанные с такой информацией и ожиданиями. Информация должна быть своевременной, ясной и доступной для соответствующих заинтересованных сторон.

g) Факторы, связанные с людьми и культурой

Поведение людей и культура оказывают существенное влияние на все аспекты управления рисками на каждом уровне и этапе.

h) Постоянное улучшение

Управление рисками постоянно улучшается через обучение и изучение опыта.

5 Структура системы управления рисками

5.1 Общие положения

Цель структуры системы управления рисками заключается в оказании организации помощи в интеграции менеджмента риска в значимые виды деятельности и функции. Результативность управления рисками будет зависеть от его интеграции в процесс управления организацией, включая принятие решений. Это требует поддержки со стороны заинтересованных сторон, особенно высшего руководства.

Структура системы включает в себя такие элементы, как интеграция, проектирование, внедрение, оценка и совершенствование управления рисками в рамках всей организации. На рисунке 3 показаны элементы системы.

Рисунок 3 — Структура системы

Организация должна провести оценку своей существующей практики и процессов управления рисками с целью определения любых пробелов и устранения этих пробелов в рамках системы.

Элементы системы и методы их совместного функционирования должны быть адаптированы к потребностям организации.

5.2 Лидерство и обязательства

Высшее руководство и наблюдательные органы там, где они существуют, должны обеспечить интеграцию управления рисками во всю деятельность организации и должны демонстрировать лидерство и обязательства посредством:

— адаптации и внедрения всех элементов системы;

— формулирования положений или политики, определяющих подход к управлению рисками, план или направление действий;

— обеспечения необходимыми ресурсами для управления рисками;

— распределения полномочий, ответственности за выполнение и результат на соответствующих уровнях в рамках организации.

Это поможет организации:

— привести управление рисками в соответствие с ее целями, стратегией и культурой;

— признать обязательства и принять меры к их полному выполнению, включая добровольно принятые обязательства;

— установить степень и тип риска, которые могут или не могут быть признаны приемлемыми при формировании критериев риска, обеспечив доведение их до сведения организации и ее заинтересованных сторон;

— донести ценность управления рисками до всей организации и ее заинтересованных сторон;

— в продвижении систематического мониторинга рисков;

— обеспечить соответствие системы управления рисками контексту организации.

Высшее руководство отвечает за управление рисками, в то время как наблюдательные органы - за контроль в сфере управления рисками. От наблюдательных органов часто ожидается или требуется:

— обеспечить надлежащее рассмотрение рисков при постановке целей организации;

— понимать риски, с которыми сталкивается организация при достижении своих целей;

— обеспечить внедрение и результативное функционирование систем управления такими рисками;

— обеспечить, чтобы такие риски соответствовали целям организации;

— обеспечить надлежащий обмен информацией о таких рисках и управлении ими.

5.3 Интеграция

Интеграция управления рисками основывается на понимании организационной структуры и контекста. Структура может быть разной в зависимости от целей, задач и сложности организации. Управление рисками осуществляется во всех элементах организационной структуры. Каждый в организации несет ответственность за управление рисками.

Корпоративное руководство определяет курс организации, ее внешние и внутренние

взаимоотношения, а также правила, процессы и процедуры, необходимые для достижения ее цели. Менеджмент переводит указания корпоративного руководства в стратегию и связанные с ней цели, необходимые для достижения желаемых уровней устойчивого функционирования и выживания в долгосрочной перспективе. Определение ответственности и контрольных функций в сфере управления рисками в рамках организации является неотъемлемой частью управления организацией.

Интеграция управления рисками в деятельность организации представляет собой динамично протекающий и итеративный процесс, который должен быть адаптирован к потребностям и культуре организации. Управление рисками должно быть частью цели и руководства организацией, лидерства и обязательств, стратегии, задач и оперативной деятельности, а не существовать отдельно от них.

5.4 Разработка

5.4.1 Понимание организации и ее контекста

При разработке структуры системы управления рисками организация должна изучить и понять свой внешний и внутренний контекст.

Изучение внешнего контекста организации может включать, но не ограничиваться этим:

— факторы, относящиеся к социальной, культурной, политической, правовой, регулирующей, финансовой, технологической, экономической и экологической сфере, на международном, национальном, региональном или местном уровне;

— ключевые факторы и тенденции, влияющие на цели организации;

— отношения с внешними заинтересованными сторонами, их представления, ценности, потребности и ожидания;

— договорные отношения и обязательства;

— сложность сетевых структур и связей в них.

Изучение внутреннего контекста организации может включать, но не ограничиваться этим:

— видение, миссию и ценности;

— стиль управления, организационную структуру, роли и обязанности;

— стратегию, цели и политики;

— корпоративную культуру организации;

— стандарты, руководства и модели, принятые организацией;

— возможности в отношении ресурсов и знаний (например, финансов, времени, персонала, интеллектуальной собственности, процессов, систем и технологий);

— данные, информационные системы и информационные потоки;

— отношения с внутренними заинтересованными сторонами с учетом их представлений и ценностей;

— договорные отношения и обязательства;

— взаимозависимости и взаимосвязи.

5.4.2 Выражение приверженности управлению рисками

Высшее руководство и наблюдательные органы, где это применимо, должны демонстрировать и

выражать свою постоянную приверженность управлению рисками посредством политики, заявления или других форм, которые четко отражают цели организации и заинтересованность в управлении рисками. Эта приверженность должна находить свое выражение, но не ограничиваться этим, в:

— намерениях организации в части управления рисками и связях с целями организации и другими политиками;

— усилении необходимости интеграции управления рисками в общую культуру организации;

— движении в сторону интеграции управления рисками в основную деятельность и принятие решений;

— полномочиях, ответственности за выполнение и результаты;

— предоставлении необходимых ресурсов;

— способе разрешения конфликтов между целями;

— измерении показателей деятельности организации и отчетности по ним;

— анализе и улучшении.

О приверженности управлению рисками должна быть проинформирована организация и заинтересованные стороны в соответствующих случаях.

5.4.3 Назначение ролей, полномочий, ответственности за выполнение и результаты

Высшее руководство и наблюдательные органы, где это применимо, должно обеспечивать назначение полномочий, ответственности за выполнение и результаты для соответствующих ролей в сфере управления рисками и информирование о них на всех уровнях организации, и должны:

— подчеркивать, что управление рисками является основной обязанностью;

— определять лиц, имеющих ответственность и полномочия для управления рисками (владельцев рисков).

5.4.4 Распределение ресурсов

Высшее руководство и наблюдательные органы, где это применимо, должны обеспечить выделение соответствующих ресурсов для управления рисками, которые могут включать, но не ограничиваться этим:

— персонал, навыки, опыт и компетентность;

— процессы, методы и инструменты организации, используемые для управления рисками;

— документированные процессы и процедуры;

— системы управления информацией и знаниями;

— потребности в профессиональном развитии и обучении.

Организация должна учитывать возможности и ограничения имеющихся ресурсов.

5.4.5 Определение порядка коммуникаций и консультаций

Организация должна выработать утвержденный подход к коммуникациям и консультациям, с тем, чтобы поддерживать систему и содействовать результативному применению управления рисками. Коммуникации предполагают обмен информацией с целевой аудиторией. Консультации также предполагают наличие участников, обеспечивающих обратную связь, которая, как ожидается, будет вносить вклад и определять решения или иные действия. В соответствующих случаях методы и

содержание коммуникаций и консультаций должны отражать ожидания заинтересованных сторон.

Коммуникации и консультации должны быть своевременными и гарантировать, что соответствующей информацией собирается, сопоставляется, обобщается и сообщается, по мере необходимости, а также что обратная связь предоставляется и осуществляются улучшения.

5.5 Внедрение

Организация должна реализовывать элементы системы управления рисками путем:

— разработки соответствующего плана, включающего график и ресурсы;

— определения, где, когда и как принимаются различного рода решения в организации, и кем;

— изменения действующих процессов принятия решений, если это необходимо;;

— обеспечения четкого понимания и практической реализации организацией мер по управлению рисками.

Для успешного внедрения системы требуется участие и информированность заинтересованных сторон. Это позволяет организациям точно учитывать неопределенность в процессе принятия решений, обеспечивая при этом возможность учета любой новой или последующей неопределенности по мере ее возникновения.

Надлежащим образом разработанная и внедренная система управления рисками гарантирует, что процесс управления рисками будет частью всей деятельности организации, включая принятие решений, и что изменения во внешнем и внутреннем контекстах будут должным образом учтены.

5.6 Оценка

Для оценки результативности системы управления рисками организации необходимо:

— периодически измерять функционирование системы управления рисками в соответствии с ее назначением, планами внедрения, показателями и ожидаемыми характеристиками;

— определять, остается ли она пригодной для обеспечения достижения целей организации.

5.7 Улучшение

5.7.1 Адаптация

Организация должна вести постоянный мониторинг и изменять систему управления рисками с учетом внешних и внутренних изменений. Таким образом организация может повысить свою ценность.

5.7.2 Постоянное улучшение

Организация должна постоянно улучшать пригодность, адекватность и результативность системы управления рисками и методы интеграции процесса управления рисками.

По мере выявления соответствующих пробелов или возможностей для улучшения организация должна разрабатывать планы и задания и поручать их тем, кто отвечает за их осуществление. После внедрения эти улучшения должны способствовать совершенствованию управления рисками.

6 Процесс

6.1 Общие положения

Процесс управления рисками включает в себя систематическое применение политик, процедур и методов к деятельности, связанной с коммуникациями и консультированием, установлением контекста и оценкой, обработкой, мониторингом, анализом, документированием и формированием отчетности по рискам. Этот процесс показан на Рисунке 4.

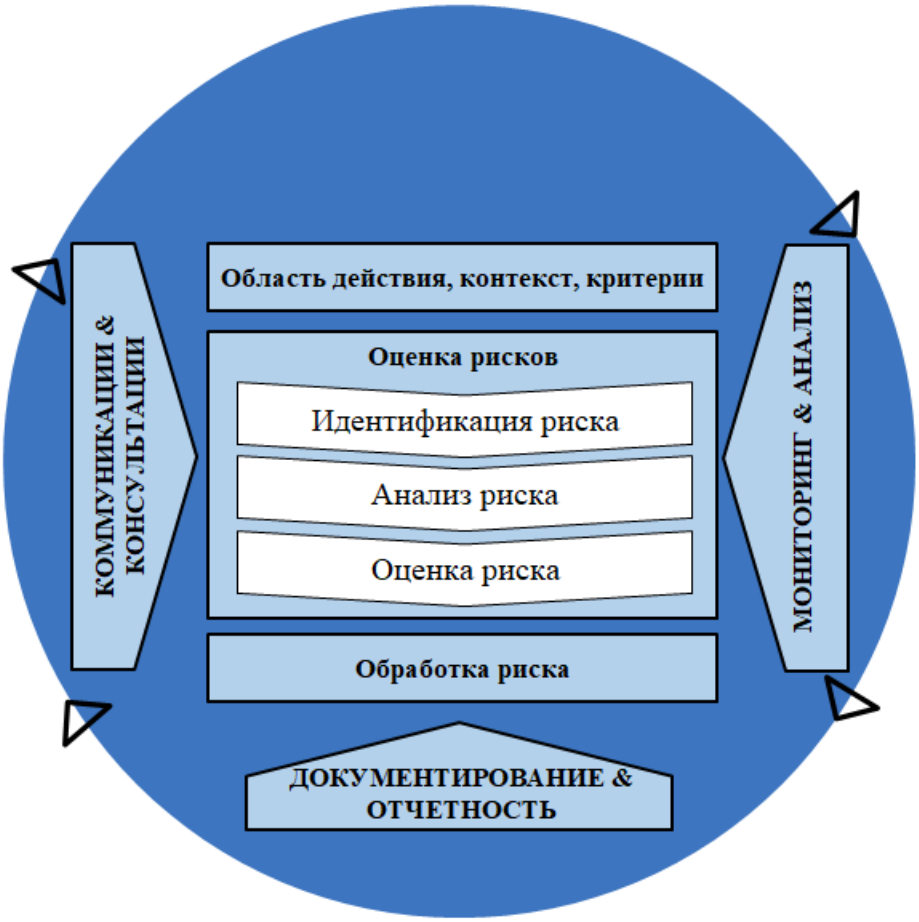


Рисунок 4 — Процесс

Процесс управления рисками должен быть неотъемлемой частью менеджмента и принятия решений и должен быть встроен в структуру, операции и процессы организации. Он может применяться на стратегическом, оперативном, программном или проектном уровнях.

Процесс управления рисками в организации может иметь различные способы реализации, адаптированные для достижения целей и соответствия внешним и внутренним факторам контекста, в рамках которого они применяются.

То, что поведение людей и культура имеют динамичный и изменчивый характер, должно учитываться на всех этапах процесса управления рисками.

Хотя процесс управления рисками часто представляется линейным, на практике он является итеративным (повторяющимся).

6.2 Коммуникации и консультации

Цель коммуникаций и консультаций заключается в оказании помощи соответствующим заинтересованным сторонам в понимании риска, оснований, на которых принимаются решения, и причин, по которым требуются конкретные действия. Коммуникации направлены на повышение осведомленности и понимания риска, в то время как консультации предполагают получение обратной связи и информации для обоснованного принятия решений. Тесная координация между ними должна способствовать фактическому, своевременному, актуальному, точному и понятному обмену информацией, с учетом вопросов конфиденциальности и целостности информации, а также права на неприкосновенность частной жизни.

Коммуникации и консультации с соответствующими внешними и внутренними заинтересованными сторонами должны осуществляться на всех этапах процесса управления рисками.

Коммуникация и консультации направлены на:

— объединение различных областей знаний на каждом этапе процесса управления рисками;

— обеспечение того, что при определении критериев риска и оценке рисков различные точки зрения учтены соответствующим образом;

— предоставление достаточной информации для обеспечения контроля рисков и принятия решений;

— формирование чувства вовлеченности и причастности у тех, кто подвержен риску.

6.3 Область действия, контекст и критерии

6.3.1 Общие положения

Цель установления области действия, контекста и критериев состоит в адаптации процесса управления рисками, обеспечивающей результативную оценку риска и принятие соответствующих мер. Установление области действия, контекста и критериев включает в себя определение границ процесса, а также понимание внешних и внутренних факторов контекста.

6.3.2 Определение области действия

Организация должна определить область, охватываемую деятельностью по управлению рисками.

Поскольку процесс управления рисками может применяться на различных уровнях (например, на стратегическом, оперативном, программном, проектном или других уровнях), важно иметь четкое представление о границах рассматриваемой области, соответствующих целях, которые должны быть приняты во внимание, и их согласованности с целями организации.

При планировании методики необходимо учитывать следующее:

— цели и решения, которые должны быть приняты;

— результаты, ожидаемые от действий, которые должны быть предприняты в процессе;

— время, место, что конкретно следует включить, что исключить;

— соответствующие инструменты и методы оценки рисков;

— необходимые ресурсы, ответственность за исполнение и сохраняемые записи;

— связи с другими проектами, процессами и видами деятельности.

6.3.3 Внешний и внутренний контекст

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

Контекст процесса управления рисками должен определяться на основе понимания факторов внешней и внутренней среды, в которых функционирует организация, и должен отражать конкретные условия деятельности, в которых должен применяться процесс управления рисками.

Понимание контекста важно, потому что:

— Управление рисками осуществляется в рамках целей и деятельности организации;

— источником риска могут быть организационные факторы;

— назначение и область применения процесса управления рисками могут быть взаимосвязаны с целями организации в целом.

Организация должна установить внешний и внутренний контекст процесса управления рисками, рассмотрев факторы, указанных в 5.4.1.

6.3.4 Определение критериев риска

Организация должна, принимая во внимание свои цели, установить степень и тип приемлемого или неприемлемого риска. Она также должна определить критерии для оценки значимости риска и обеспечения процессов принятия решений. Критерии риска должны соответствовать структуре системы управления рисками и учитывать конкретные цели и границы рассматриваемой деятельности. Критерии риска должны отражать ценности и цели организации, соответствовать ее ресурсам, политикам и положениям, связанным с риск-менеджментом. Критерии должны быть определены с учетом обязательств организации перед заинтересованными сторонами и их мнений.

Критерии риска должны устанавливаться в начале процесса оценки риска, но они могут динамично меняться и должны постоянно пересматриваться и, при необходимости, корректироваться.

Чтобы установить критерии риска, необходимо учитывать следующее:

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

— как будут определены и оценены последствия (как положительные, так и отрицательные) и вероятность;

— факторы, связанные со временем;

— единый подход в использовании измерений;

— как должен определяться уровень риска;

— как будут учитываться сочетания и последовательность множественных рисков;

— возможности организации.

6.4 Оценка риска

6.4.1 Общие положения

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

Оценка рисков должна проводиться систематически, итеративно и коллективно, опираясь на знания и мнения заинтересованных сторон. Она должна использовать наилучшую имеющуюся информацию,

дополняемую по запросу, если необходимо.

6.4.2 Идентификация риска

Цель идентификации рисков заключается в поиске, распознавании и описании рисков, которые могут способствовать или препятствовать достижению организацией своих целей. При идентификации рисков важное значение имеет значимость, пригодность и актуальность используемой информации.

Организация может использовать ряд методов для выявления неопределенностей, которые могут повлиять на одну или более целей. Следует учитывать следующие факторы и взаимосвязь между ними:

— материальные и нематериальные источники риска;

— причины и события;

— угрозы и возможности;

— уязвимости и потенциальные возможности;

— изменения во внешнем и внутреннем контексте;

— признаки возникающих рисков;

— характер и ценность активов и ресурсов;

— последствия и их влияние на цели;

— ограниченность знаний и достоверность информации;

— временны́е факторы;

— предубеждения, предположения и убеждения тех, кто участвует в оценке рисков.

Организация должна выявлять риски, независимо от того, находятся или нет их источники под ее контролем. Следует учитывать, что может быть два и более сценариев развития событий, которые могут привести к различным последствиям, имеющим материальный или нематериальный характер.

6.4.3 Анализ риска

Цель анализа риска заключается в понимании природы риска и его характеристик, включая, в соответствующих случаях, уровень риска. Анализ рисков включает детальное рассмотрение неопределенностей, источников риска, последствий, вероятности, событий, сценариев, средств управления и их результативности. Событие может иметь несколько причин и последствий и может влиять на несколько целей.

Анализ рисков может проводиться с различной степенью детализации и сложности в зависимости от цели анализа, наличия и надежности информации и имеющихся ресурсов. Методы анализа могут быть качественными, количественными или комбинированными в зависимости от обстоятельств и предполагаемого использования.

Анализ рисков должен учитывать такие факторы, как:

— вероятность событий и последствия;

— характер и масштабы последствий;

— сложность и взаимосвязи;

— временны́е факторы и изменчивость;

— результативность существующих средств управления;

— степень конфиденциальности и уровень доверия.

На анализ риска могут влиять любые расхождения во мнениях, предубеждения, представления о риске и оценки. Дополнительное влияние оказывает качество используемой информации, сделанные допущения и исключения, любые ограничения методов и способы их выполнения. Эти влияния должны быть рассмотрены, задокументированы и доведены до сведения лиц, принимающих решения.

События, имеющие высокую степень неопределенности, трудно поддаются количественной оценке. Это может быть проблемой при анализе событий с серьезными последствиями. В таких случаях использование комбинации методов, как правило, обеспечивает более глубокое понимание.

Анализ риска дает исходную информацию для оценки риска, принятия решений о том, следует ли обрабатывать риск и каким образом, а также о наиболее подходящей стратегии и методах обработки риска. Результаты дают информацию для решений, в которых делается выбор, и о вариантах, связанных с различными типами и уровнями риска.

6.4.4 Оценка риска

Целью оценки риска является обеспечение принятия решений. Оценка риска включает в себя сравнение результатов анализа риска с установленными критериями риска, чтобы определить, где требуются дополнительные действия.

Это может привести к решению:

— ничего более не предпринимать;

— рассмотреть варианты обработки рисков;

— провести дальнейший анализ для лучшего понимания риска;

— сохранить существующие средства управления;

— пересмотреть цели.

При принятии решений следует учитывать более широкий контекст, фактические и предполагаемые последствия для внешних и внутренних заинтересованных сторон.

Результаты оценки рисков должны документироваться, доводиться до сведения и затем подтверждаться на соответствующих уровнях организации.

6.5 Обработка риска

6.5.1 Общие положения

Цель обработки риска заключается в выборе и реализации вариантов мер по управлению риском.

Обработка риска представляет собой итеративный процесс, состоящий из:

— определения и выбора вариантов обработки риска;

— планирования и выполнения обработки рисков;

— оценки результативности такой обработки;

— принятия решения о приемлемости остаточного риска;

— осуществления дальнейших мер, если он не приемлем.

6.5.2 Выбор вариантов обработки риска

Выбор наиболее подходящего(ых) варианта(ов) обработки риска предполагает нахождение баланса между потенциальным выигрышем, получаемым в результате достижения целей, и затратами, усилиями или негативными последствиями осуществления выбранного варианта.

Варианты обработки рисков не обязательно являются взаимоисключающими или пригодными во всех обстоятельствах. Варианты обработки риска могут включать одно или несколько из следующих действий:

— избегание риска решением не начинать или не продолжать деятельность, которая ведет к риску;

— принятие или увеличение риска с целью реализации возможности;

— устранить источник риска;

— изменить вероятность;

— изменить последствия;

— разделить риск (например, посредством включения соответствующих положений в договоры, приобретения страховки);

— сохранение риска путем принятия обоснованного решения.

Обоснование мер по обработке рисков не ограничивается чисто экономическими соображениями и должно учитывать все установленные обязательства организации, добровольно принятые обязательства и мнения заинтересованных сторон. Выбор вариантов обработки рисков должен осуществляться в соответствии с целями организации, критериями риска и имеющимися ресурсами.

При выборе вариантов обработки рисков организация должна учитывать ценности, представления и потенциальное участие заинтересованных сторон, а также наиболее подходящие способы обмена информацией и консультаций с ними. Несмотря на равную результативность, одни методы обработки рисков могут быть более приемлемыми для некоторых заинтересованных сторон, чем другие.

Обработка рисков, даже если она тщательно проработана и внедрена, может не дать ожидаемых результатов и привести к непредвиденным последствиям. Мониторинг и анализ должны быть неотъемлемой частью реализации обработки риска, чтобы гарантировать, что различные формы обработки результативны и остаются таковыми.

Обработка рисков может также привести к возникновению новых рисков, которыми необходимо управлять.

Если нет доступных вариантов обработки или если имеющиеся варианты недостаточно воздействуют на риск, этот риск необходимо задокументировать и держать под постоянным контролем.

Лица, принимающие решения, и другие заинтересованные стороны должны быть осведомлены о характере и степени рисков, остающихся после обработки. Остаточный риск должен быть задокументирован и быть предметом мониторинга, анализа и, в соответствующих случаях, дальнейшей обработки.

6.5.3 Подготовка и выполнение планов обработки рисков

Цель планов обработки риска состоит в том, чтобы определить, как выбранные варианты обработки будут реализованы, чтобы мероприятия плана были понятны тем, кто участвует в их реализации, и можно было отслеживать степень выполнения плана. План обработки должен четко определять порядок, в котором должна осуществляться обработка риска.

Планы обработки должны быть частью планов менеджмента и процессов организации при консультациях с соответствующими заинтересованными сторонами.

Информация, представленная в плане обработки, должна включать в себя:

— обоснование выбора вариантов обработки, в том числе ожидаемые преимущества, которые будут получены;

— ответственных за утверждение и реализацию плана;

— предлагаемые меры;

— необходимые ресурсы, включая непредвиденные расходы;

— показатели результативности;

— ограничения;

— требуемые отчетность и мониторинг;

— когда меры должны быть осуществлены и завершены.

6.6 Мониторинг и анализ

Цель мониторинга и анализа состоит в обеспечении и повышении качества и результативности разработки и выполнения процесса, его результатов. Постоянный мониторинг и периодический анализ процесса управления рисками и его результатов должны быть запланированной частью процесса управления рисками с четко определенными обязанностями.

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

Результаты мониторинга и анализа должны учитываться в управлении деятельностью организации, при проведении измерений и формировании отчетности.

6.7 Регистрация результатов и отчетность

Процесс управления рисками и его результаты должны документироваться и распространяться соответствующими методами. Регистрация и отчетность нацелены на то, чтобы:

— распространять информацию о деятельности и результатах управления рисками во всей организации;

— предоставлять информацию для принятия решений;

— улучшать деятельность по управлению рисками;

— способствовать взаимодействию с заинтересованными сторонами, в том числе ответственными за результаты и осуществление действий по управлению рисками.

Решения, касающиеся создания, хранения и обработки документированной информации, должны принимать во внимание, но не ограничиваться этим: использование, конфиденциальность информации, а также факторы внешнего и внутреннего контекста.

Отчетность является неотъемлемой частью управления организацией и должна повышать качество диалога с заинтересованными сторонами и оказывать поддержку высшему руководству и надзорным органам в выполнении ими своих обязанностей.

Факторы, которые необходимо учитывать при составлении отчетности, включают, но не ограничиваются этим, следующее:

- различные заинтересованные стороны и их конкретные потребности и требования, связанные с информацией;

- затраты на представление отчетности, периодичность и своевременность;

- метод отчетности;

- значимость информации с точки зрения целей организации и принятия решений.

Библиография

[1] IEC 31010, *Risk management — Risk assessment techniques*