ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 31000— 2019

Менеджмент риска

ПРИНЦИПЫ И РУКОВОДСТВО

(ISO 31000:2018, Risk management — Guidelines, IDT)

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН некоммерческим партнерством «Русское Общество Управления Рисками» (НП «РусРиск») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 010 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 10 декабря 2019 г. № 1379-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 31000:2018 «Менеджмент риска. Принципы и руководство» (ISO 31000:2018 «Risk management — Guidelines», IDT).

Международный стандарт разработан Техническим комитетом ISO /ТС 262.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5)

5 ВЗАМЕН ГОСТ Р ИСО 31000—2010

6 Некоторые элементы настоящего стандарта могут являться объектами патентных прав.

Федеральный орган исполнительной власти в сфере стандартизации не несет ответственности за патентную чистоту содержания стандарта или за объективность указанной разработчиком информации о патентных правах патентообладателя (лицензиара), а также за условия лицензирования патентов, использованных в стандарте

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© ISO, 2018 — Все права сохраняются
© Стандартинформ, оформление, 2020

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

Введение IV
1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Принципы 3
5 Структура 4
5.1 Общие положения 4
5.2 Лидерство и приверженность 5
5.3 Адаптация 5
5.4 Проектирование и разработка 5
5.5 Внедрение 7
5.6 Оценка эффективности 7
5.7 Улучшение 7
6 Процесс 7
6.1 Общие положения 7
6.2 Обмен информацией и консультирование 8
6.3 Область применения, среда и критерии 8
6.4 Оценка риска 9
6.5 Обработка риска 11
6.6 Мониторинг и пересмотр 12
6.7 Документирование и отчетность 12
Библиография 13

Введение

Настоящий стандарт предназначен для лиц, чья деятельность направлена на создание и защиту ценностей организаций путем менеджмента риска, принятия решений, постановки и достижения целей, повышения эффективности деятельности.

Организации всех типов и размеров сталкиваются с внешними и внутренними факторами и влиянием, которое создает неопределенность в отношении достижения поставленных целей.

Менеджмент риска является итеративным процессом и помогает организациям в определении стратегии, достижении целей и принятии обоснованных решений.

Менеджмент риска является частью корпоративного управления организации и имеет фундаментальное значение для управления на всех уровнях. Он способствует совершенствованию системы управления организацией.

Менеджмент риска затрагивает любые виды деятельности, осуществляемые в рамках организации, и включает взаимодействие с причастными сторонами.

Менеджмент риска учитывает внешнюю и внутреннюю среду организации, включая поведение людей и культурные факторы.

Менеджмент риска основан на принципах, структуре и процессе, описанных в этом документе, как показано на рисунке 1. Вышеперечисленные компоненты могут быть частично или полностью внедрены в организации, однако они могут потребовать адаптации или улучшения для более эффективного, результативного и последовательного менеджмента риска.

Настоящий стандарт устанавливает ряд принципов, которые необходимо соблюдать, для того чтобы менеджмент риска был эффективным. Настоящий стандарт рекомендует, чтобы организации разрабатывали, внедряли и постоянно улучшали структуру и процесс менеджмента риска, что будет способствовать росту ценности организаций.

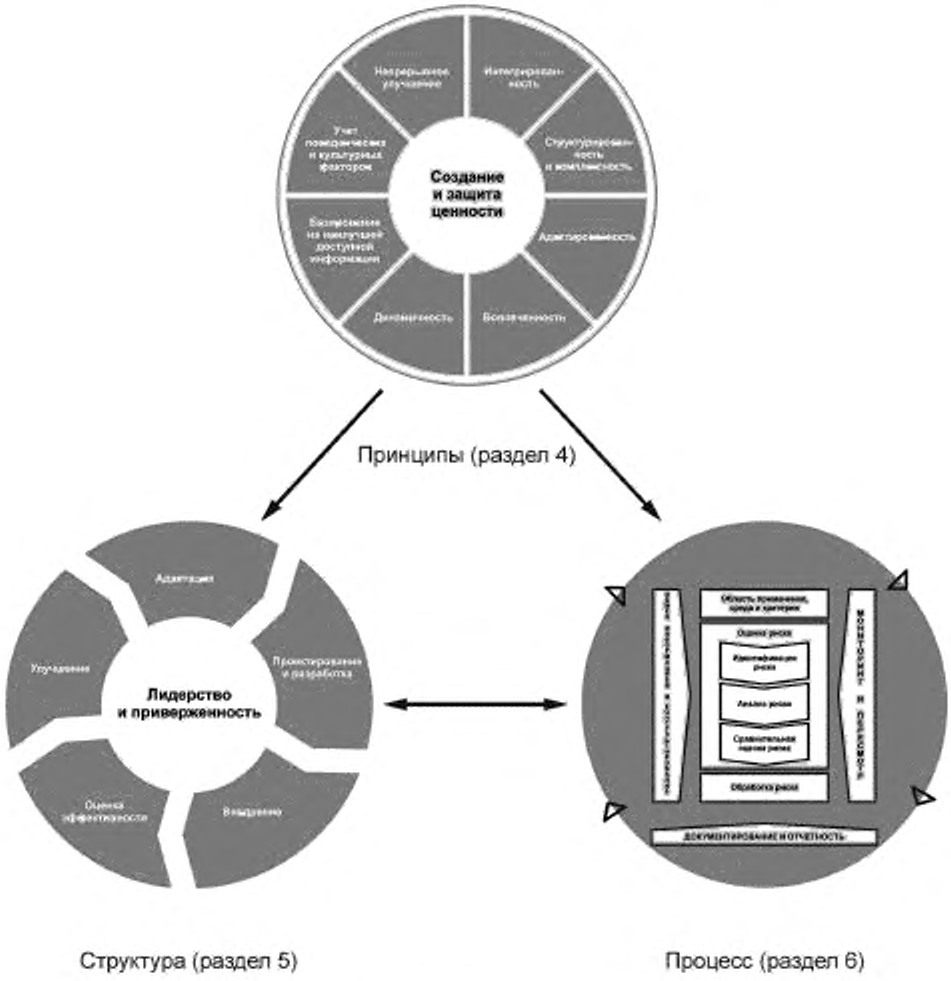

Рисунок 1 — Принципы, структура и процесс

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

ПРИНЦИПЫ И РУКОВОДСТВО

Risk management. Principles and guidelines

Дата введения — 2020—03—01

1 Область применения

В настоящем стандарте содержатся руководящие указания по менеджменту рисков, которым подвержены организации. Эти руководящие указания могут быть адаптированы для любой организации вне зависимости от рода ее деятельности.

Настоящий стандарт обеспечивает общий подход к менеджменту любых типов риска и не ограничивается конкретной отраслью или видом деятельности.

Настоящий стандарт может использоваться на протяжении всего периода существования организации и может применяться к любой деятельности, включая процесс принятия решений на всех уровнях управления.

2 Нормативные ссылки

Нормативные ссылки отсутствуют.

3 Термины и определения

В настоящем стандарте применены следующие термины и определения. ИСО и МЭК поддерживают стандартизованную базу терминов по следующим адресам.

- платформа Интернет-поиска ИСО доступна по адресу: gost.e-ecolog.ru
- IEC Electropedia (международный электротехнический словарь) доступен по адресу: *http://www.electropedia.org*

3.1 риск (risk): Следствие влияния неопределенности на достижение поставленных целей.

Примечание 1 — Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное).

Примечание 2 — Цели могут быть различными по содержанию (в области экономики, здоровья, экологии и т. п.) и назначению (стратегические, общеорганизационные, относящиеся к разработке проекта, конкретной продукции и процессу).

Примечание 3 — Риск часто характеризуют путем описания возможного события (3.5) и его последствий (3.6) или их сочетания.

Примечание 4 — Риск часто представляют в виде последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности.

Издание официальное

Примечание 5 — Неопределенность — это состояние полного или частичного отсутствия информации, необходимой для понимания события (3.5), его последствий (3.6) и их вероятностей.

3.2 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в области риска (3.1).

3.3 **причастная** (заинтересованная) **сторона** (stakeholder): Любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска.

Примечание — Лицо, принимающее решение, также является причастной стороной.

3.4 **источник риска** (risk source): Объект или деятельность, которые самостоятельно или в комбинации с другими обладают возможностью вызывать повышение риска (3.1).

Примечание — Источник риска может быть материальным или нематериальным.

3.5 **событие** (event): Возникновение или изменение специфического набора условий.

Примечание 1 — Событие может быть единичным или многократным и может иметь несколько причин.

Примечание 2 — Событие может быть определенным или неопределенным.

Примечание 3 — Событие может быть названо терминами «инцидент», «опасное событие» или «несчастный случай».

Примечание 4 — Событие без последствий (3.6) может также быть названо терминами «угроза возникновения опасного события», «угроза инцидента», «угроза поражения» или «угроза возникновения аварийной ситуации».

3.6 **последствие** (consequence): Результат воздействия события (3.5) на объект.

Примечание 1 — Результатом воздействия события может быть одно или несколько последствий.

Примечание 2 — Последствия могут быть определенными или неопределенными, могут быть ранжированы от позитивных до негативных.

Примечание 3 — Последствия могут быть выражены качественно или количественно.

Примечание 4 — Первоначальные последствия могут вызвать эскалацию дальнейших последствий по «принципу домино».

3.7 **правдоподобность (появления события)** (likelihood): Характеристика возможности и частоты появления события.

Примечание 1 — В менеджменте риска термин «правдоподобность» используют как характеристику возможности появления события, которая может быть определенной или неопределенной, измеримой или неизмеримой, объективной или субъективной, иметь качественную или количественную оценку и может быть выражена математически (как вероятность или частота за установленный период времени).

Примечание 2 — Английский термин «правдоподобность» не имеет прямого эквивалента в некоторых языках, вместо которого в этом случае применяют термин «вероятность». В английском языке термин «вероятность» часто применяют как чисто математический термин. Таким образом, в области управления риском в части терминологии термин «правдоподобность» использован в более широком смысле, чем в других языках, кроме английского.

3.8 **управление (риском)** (control): Меры, направленные на изменение риска (3.1).

Примечание 1 — Управление риском охватывает процессы, политику, устройства, методы и другие средства, используемые для модификации риска.

Примечание 2 — Управление не всегда может привести к ожидаемым результатам изменения риска.

3.8.1 **сравнительная оценка риска:** Процесс сравнения результатов анализа риска с критериями риска для определения приемлемости риска.

Примечание — Сравнительная оценка риска может быть использована при принятии решения об обработке риска.

4 Принципы

Целью менеджмента риска является создание и защита ценностей организации. Менеджмент риска повышает производительность, поощряет инновации и поддерживает достижение целей.

Принципы, представленные на рисунке 2, устанавливают характеристики эффективного и результативного менеджмента риска, отражают его ценности и объясняют его назначение и цель. Эти принципы являются основой менеджмента риска и должны учитываться при создании структуры и процесса менеджмента риска организации. Соблюдение принципов позволит организации управлять влиянием неопределенности в отношении достижения целей организации.



Рисунок 2 — Принципы

Эффективный менеджмент риска требует соблюдения принципов, представленных на рисунке 2, и может быть раскрыт следующим образом:

a) Интегрированность

Интегрированный менеджмент риска является неотъемлемой частью всей деятельности организации.

b) Структурированность и комплексность

Структурированный и комплексный подход к менеджменту риска способствует согласованным и сопоставимым результатам.

c) Адаптированность

Структура и процесс менеджмента риска настраиваются и соразмерны внешней и внутренней среде организации, ее целям.

d) Вовлеченность

Вовлеченность заключается в надлежащем и своевременном участии причастных сторон, что позволяет учитывать их знания, взгляды и мнения. Это приводит к повышению осведомленности и информативности в рамках менеджмента риска.

e) Динамичность

Риски могут возникать, меняться или исчезать по мере изменения внешней и внутренней среды организации. Менеджмент риска предвосхищает, обнаруживает, признает и реагирует на эти изменения и события соответствующим и своевременным образом.

f) Базирование на наилучшей доступной информации

В качестве исходных данных используются исторические и текущие данные, а также прогнозные ожидания. Менеджмент риска явно учитывает любые ограничения и неопределенности, связанные с исходными данными и ожиданиями. Информация должна быть актуальной, ясной и доступной для всех причастных сторон.

g) Учет поведенческих и культурных факторов

Поведение и культура человека существенно влияют на все аспекты менеджмента риска на каждом уровне и этапе.

h) Непрерывное улучшение

Менеджмент риска постоянно улучшается благодаря обучению и накоплению опыта.

5 Структура

5.1 Общие положения

Структура менеджмента риска предназначена для обеспечения возможности интеграции процесса менеджмента риска в основные направления деятельности и функции. Эффективность менеджмента риска будет зависеть от степени интеграции в управление организацией, включая процедуры принятия решений. Это требует поддержки со стороны причастных сторон, особенно высшего руководства организации.

Внедрение структуры менеджмента риска включает в себя интеграцию, проектирование и разработку, внедрение, оценку и улучшение менеджмента риска в организации. На рисунке 3 представлены компоненты структуры.



Рисунок 3 — Структура

Организация должна оценить существующую практику и процессы менеджмента риска, выявить существующие недостатки и устранить их в рамках структуры.

Компоненты структуры и их совместная работа должны быть адаптированы к потребностям организации.

5.2 Лидерство и приверженность

Руководители высшего звена и надзорные органы, если это применимо, должны обеспечить интеграцию менеджмента риска во все направления деятельности организации, при этом должны демонстрироваться лидерство и приверженность:

- адаптации и внедрению всех компонентов структуры;
- выпуску заявления или политики, которая устанавливает подход, план или порядок действий в отношении менеджмента риска;
- обеспечению выделения необходимых ресурсов для менеджмента риска;
- установлению полномочий, ответственности и подотчетности на соответствующих уровнях организации.

Это позволит организации:

- обеспечить соответствие менеджмента риска целям, стратегии и культуре организации;
- осознавать и придерживаться всех обязательств, включая добровольные обязательства организации;
- установить уровень и тип риска, который может или не может быть использован для разработки критериев риска, а также гарантий того, что данные критерии будут доведены до организации и ее причастных сторон;
- демонстрировать ценность менеджмента риска внутри организации и причастным сторонам;
- поддерживать систематический мониторинг рисков;
- обеспечить соответствие структуры менеджмента риска среде организации.

Руководители высшего звена отвечают за управление рисками, в то время как надзорные органы отвечают за осуществление надзора над данным процессом. Надзорные органы зачастую ожидают и требуют от организации:

- обеспечить адекватное рассмотрение рисков при определении целей организации;
- понимать риски, с которыми сталкивается организация при достижении своих целей;
- обеспечить эффективное внедрение и функционирование систем менеджмента риска;
- убедиться в соответствии такого рода рисков целям организации;
- обеспечить надлежащий обмен информацией о таких рисках и управлении ими.

5.3 Адаптация

Адаптация менеджмента риска основана на понимании организационной структуры и среды. Структуры различаются в зависимости от цели, задачи, сложности организации. Менеджмент риска осуществляется во всех элементах структуры организации. Каждый человек в организации несет ответственность за менеджмент риска.

Руководство управляет курсом организации, ее внешними и внутренними отношениями, а также правилами, процессами и практикой, необходимыми для достижения поставленной цели. Аппарат менеджмента преобразует курс руководства в стратегию и связанные с ней цели, необходимые для достижения желаемых уровней устойчивости и долгосрочной жизнеспособности. Распределение ответственности за менеджмент риска и надзорные функции внутри организации является неотъемлемой частью управления организацией.

Адаптация менеджмента риска в организации является динамичным и итеративным процессом, при адаптации нужно учитывать потребности и культуру организации. Менеджмент риска должен быть частью, а не отдельным элементом целей организации, ее системы управления, лидерства и приверженности, стратегии, задач и операций.

5.4 Проектирование и разработка

5.4.1 Понимание организации и ее среды

При проектировании и разработке структуры менеджмента риска организации следует изучить и понять ее внешнюю и внутреннюю среду. Изучение внешней среды организации может включать, но не ограничиваться:

- социальными, культурными, политическими, правовыми, нормативными, финансовыми, технологическими, экономическими и экологическими факторами на международном, национальном, региональном или местном уровнях;
- основными факторами и тенденциями, влияющими на цели организации;

- взаимоотношениями с внешними причастными сторонами, их восприятием, ценностями, потребностями и ожиданиями;
- договорными отношениями и обязательствами;
- сложностью существующих связей и зависимостей от внешних причастных сторон.

Изучение внутренней среды организации может включать, но не ограничиваться:

- видением, миссией и ценностями;
- управлением, организационной структурой, ролями и ответственностью;
- стратегией, целями и политикой;
- культурой организации;
- стандартами, директивами и моделями, принятыми организацией;
- возможностями, понимаемыми ресурсами и накопленными знаниями (например, капитал, время, люди, интеллектуальная собственность, процессы, системы и технологии);
- данными, информационными системами и информационными потоками;
- отношениями с внутренними причастными сторонами с учетом их мнения и ценностей;
- договорными отношениями и обязательствами;
- взаимозависимостями и взаимосвязями.

5.4.2 Демонстрация приверженности менеджменту риска

Руководители высшего звена и надзорные органы, где это применимо, должны демонстрировать и формулировать свою постоянную приверженность менеджменту риска посредством политики, деклараций или других форм, которые четко отражают цели организации и следование менеджменту риска. Обязательства должны включать, но не ограничиваться:

- целью организации в отношении менеджмента риска и связи с общими целями и другими политиками;
- закреплением необходимости интегрировать менеджмент риска в общую культуру организации;
- интеграцией менеджмента риска в основные виды деятельности и процесс принятия решений;
- определением полномочий, обязанностей и ответственности;
- обеспечением доступа к необходимым ресурсам;
- созданием механизмов решения конфликтных задач;
- измерением показателей эффективности организации и подготовки отчетности по ним;
- пересмотром и улучшением.

Об обязательствах в отношении менеджмента риска должны быть надлежащим образом проинформированы лица внутри организации и причастные стороны.

5.4.3 Определение организационных ролей, полномочий, обязанностей и ответственности

Руководители высшего звена и надзорные органы, где это применимо, должны обеспечивать, чтобы полномочия, обязанности и ответственность за соответствующие роли в отношении менеджмента риска были определены и доведены до сведения соответствующих лиц на всех уровнях организации, что должно:

- определять перечень лиц, у которых есть ответственность и полномочия для осуществления менеджмента риска (владельцев рисков);
- подчеркивать, что менеджмент риска является одной из основополагающих обязанностей.

5.4.4 Распределение ресурсов

Руководители высшего звена и надзорные органы должны быть уверены в наличии необходимых ресурсов для осуществления менеджмента риска, где это применимо, которые могут включать, но не ограничиваться:

- людьми, навыками, опытом и компетентностью;
- процессами, методами и инструментами организации, используемыми для менеджмента риска;
- документированными процессами и процедурами;
- системами управления информацией и знаниями;
- потребностями в профессиональном развитии и обучении.

Организация должна учитывать возможности и ограничения существующих ресурсов.

5.4.5 Установление механизмов обмена информацией и консультирования

Организация должна разработать и одобрить подход к обмену информацией и консультированию в целях поддержки структуры и содействия эффективному применению менеджмента риска.

Обмен информацией предполагает доведение необходимой информации до целевой аудитории. Консультирование также подразумевает получение обратной связи от участников процесса с целью ее учета при принятии решений и осуществлении других видов деятельности. Методы и сущность обмена информацией и консультирования должны отражать ожидания причастных сторон, где это уместно.

Обмен информацией и консультирование должны быть своевременными и обеспечивать сбор, сопоставление, обобщение и совместное использование соответствующей информации, а при необходимости — предоставление обратной связи и внедрение улучшений на ее основе.

5.5 Внедрение

Организация должна внедрять менеджмент риска путем:

- разработки соответствующего плана, определяющего необходимое время и ресурсы;
- определения того, где, когда, кем и как различные типы решений принимаются в рамках организации;
- изменения, при необходимости, процессов принятия решений;
- обеспечения четкого понимания и практической реализации механизмов управления рисками в рамках организации.

Успешное внедрение структуры менеджмента риска требует участия и осведомленности причастных сторон. Это позволяет организациям непосредственно учитывать неопределенность при принятии решений, а также обеспечивать принятие во внимание любой новой или последующей неопределенности по мере ее возникновения.

Надлежащим образом спроектированная и внедренная структура менеджмента риска гарантирует, что процесс менеджмента риска будет являться частью всей деятельности организации, включая процессы принятия решений, и что изменения во внешней и внутренней среде будут адекватно учтены.

5.6 Оценка эффективности

Для оценки эффективности структуры менеджмента риска организация должна:

- периодически оценивать эффективность работы структуры менеджмента риска по отношению к целям, планам реализации, показателям и ожидаемому поведению;
- определить, по-прежнему ли менеджмент риска содействует достижению целей организации.

5.7 Улучшение

5.7.1 Обновление

Организации следует осуществлять непрерывный мониторинг и обновление структуры управления рисками для реагирования на внешние и внутренние изменения. Осуществляя это, организация может повысить свою ценность.

5.7.2 Постоянное улучшение структуры

Организация должна постоянно улучшать применимость, адекватность и результативность работы структуры менеджмента риска, а также способы интеграции процесса менеджмента риска внутри организации.

По мере выявления соответствующих недостатков или возможностей для улучшения организации следует разрабатывать планы и задачи и поручать их ответственным за реализацию. После внедрения эти улучшения должны способствовать совершенствованию менеджмента риска.

6 Процесс

6.1 Общие положения

Процесс менеджмента риска предполагает систематическое применение политик, процедур и действий по обмену информацией и консультированию, определению среды, а также по оценке, обработке риска, мониторингу, пересмотру, документированию рисков и подготовки отчетности. Этот процесс показан на рисунке 4.

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

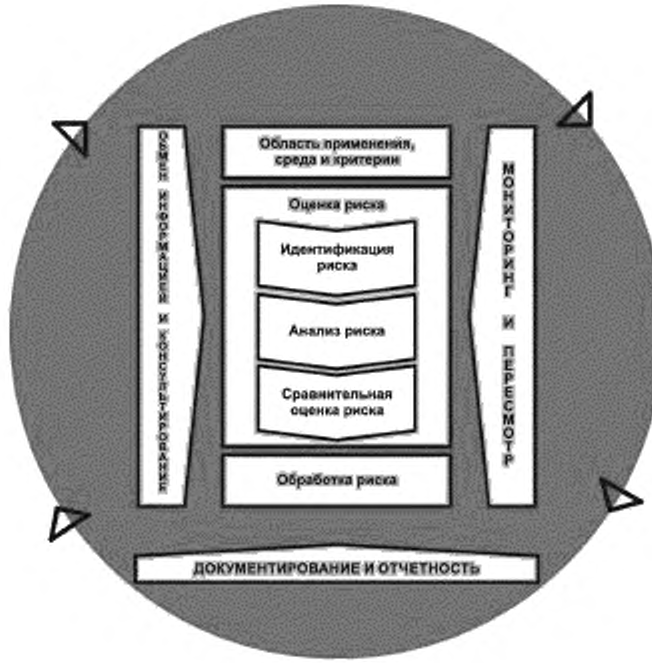

Рисунок 4 — Процесс

В организации может быть много применений процесса менеджмента риска, настроенных для достижения целей организации и соответствия внешней и внутренней среде, в которой они применяются.

Динамический и изменчивый характер поведения и культуры человека следует учитывать на протяжении всего процесса менеджмента риска. Хотя процесс менеджмента риска зачастую представляется как последовательный, на практике он является итеративным.

6.2 Обмен информацией и консультирование

Целью обмена информацией и консультирования является оказание помощи причастным сторонам в понимании риска, предпосылок, на основании которых принимаются решения, и причин, в отношении которых требуются конкретные действия. Обмен информацией направлен на повышение осведомленности и понимание риска, тогда как консультирование подразумевает получение обратной связи и информации для поддержки процесса принятия решений. Тесная взаимосвязь между данными процессами должна способствовать фактическому, своевременному, актуальному, точному и понятному движению информации в организации с учетом конфиденциальности и целостности информации, а также прав на частную жизнь отдельных лиц.

Обмен информацией и консультирование с соответствующими внешними и внутренними причастными сторонами должны проводиться на всех этапах процесса менеджмента риска.

Целями обмена информацией и консультирования являются:

- объединение различных областей знаний для каждого этапа процесса менеджмента риска;
- обеспечение учета различных взглядов при определении критериев риска и при оценке риска;
- предоставление достаточной информации для облегчения управления риском и принятия решений;
- создание чувства вовлеченности и причастности среди лиц, подверженных риску.

6.3 Область применения, среда и критерии

6.3.1 Общие положения

Цель определения области применения, среды и критериев заключается в адаптации процесса менеджмента риска, позволяющей эффективно оценивать риск и подбирать соответствующие методы обработки риска. Область применения, среда и критерии включают в себя определение

области применения процесса менеджмента риска с учетом понимания внешней и внутренней среды организации.

6.3.2 Определение области применения

Организация должна определить область применения в отношении действий, связанных с менеджментом риска.

Поскольку процесс менеджмента риска может применяться на разных уровнях (например, стратегическом, операционном, программном, проектном или др.), важно четко понимать рассматриваемую область применения, соответствующие цели, которые необходимо учитывать, а также их согласование с организационными целями.

При планировании подхода учитываются следующие факторы:

- 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, обязанности и документирование результатов;
- взаимосвязь с другими проектами, процессами и действиями.

6.3.3 Внешняя и внутренняя среда

Внешняя и внутренняя среда — это окружение, в котором организация стремится определить и достичь своих целей.

Понимание среды процесса менеджмента риска должно исходить из внешнего и внутреннего окружения, в котором работает организация, и отражать конкретные условия деятельности, к которым должен применяться процесс менеджмента риска.

Понимание среды важно, потому что:

- менеджмент риска происходит с учетом целей деятельности организации;
- организационные факторы могут быть источником риска;
- цель и область применения процесса менеджмента риска взаимосвязаны с общими целями организации.

Организация должна установить внешнюю и внутреннюю среду процесса менеджмента риска, рассмотрев факторы, упомянутые в 5.4.1.

6.3.4 Определение критериев риска

Организация должна указать размер и тип риска, который она может или не может принять по отношению к своим целям. Она также должна определять критерии для оценки значимости риска и поддержки процессов принятия решений. Критерии риска должны быть согласованы со структурой управления рисками и адаптированы к конкретным целям и объемам рассматриваемой деятельности. Критерии риска должны отражать ценности, цели и ресурсы организации и соответствовать политикам и заявлениям в отношении менеджмента риска. Критерии должны определяться с учетом обязательств организации и мнений причастных сторон.

Хотя критерии риска должны быть установлены в начале процесса оценки риска, они являются динамичными и в случае необходимости должны пересматриваться и корректироваться.

При определении критериев риска необходимо учитывать следующее:

- характер и тип неопределенностей, которые могут повлиять на результаты и достижение целей (как материальные, так и нематериальные);
- способ определения и оценки последствий (как положительных, так и отрицательных) и их вероятность;
- факторы, связанные со временем;
- корректность и согласованность применяемых методов измерений;
- порядок определения уровня риска;
- способ учета комбинации и последовательности множественных рисков;
- масштаб организации.

6.4 Оценка риска

6.4.1 Общие положения

Оценка риска — это процесс, охватывающий идентификацию риска, анализ риска и сравнительную оценку риска.

Оценка риска должна проводиться систематически, итеративно и совместно, опираясь на знания и мнения причастных сторон. Она должна базироваться на наилучшей имеющейся информации и дополняться по мере необходимости новыми данными.

6.4.2 Идентификация риска

Цель идентификации риска — найти, распознать и описать риски, которые могут помочь или помешать организации достичь своих целей. Для идентификации рисков важно использовать уместную, применимую и актуальную информацию.

Организация может использовать ряд методов для выявления неопределенностей, которые могут повлиять на достижение одной или нескольких целей. Следует учитывать следующие факторы и взаимосвязи между этими факторами:

- материальные и нематериальные источники риска;
- причины и события;
- угрозы и возможности;
- уязвимости и способности;
- изменения внешней и внутренней среды;
- 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.

Организация должна идентифицировать риски независимо от того, находятся ли источники данных рисков под контролем. Следует учитывать, что может быть более одного исхода в случае реализации риска, что может привести к различным материальным или нематериальным последствиям.

6.4.3 Анализ риска

Цель анализа риска заключается в том, чтобы понять природу риска и его характеристики, в том числе, когда это необходимо, уровень риска. Анализ риска включает подробное рассмотрение неопределенностей, источников риска, последствий, вероятности, событий, сценариев, методов управления риском и их эффективности. Событие может иметь несколько причин и последствий и может влиять на достижение нескольких целей.

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

Анализ риска должен учитывать такие факторы, как:

- вероятность событий и последствий;
- характер и масштабы последствий;
- сложность и взаимосвязь с другими рисками;
- факторы, связанные со временем, волатильность;
- эффективность существующих методов управления риском;
- уровень чувствительности и достоверности.

На анализ риска может влиять любое расхождение мнений, предвзятость, восприятие риска и суждения. Дополнительное влияние оказывает качество используемой информации, сделанные допущения и исключения, любые ограничения технологий и способов их применения. Эти факторы следует рассматривать, документировать и сообщать лицам, ответственным за принятие решений.

Крайне неопределенные события могут плохо поддаваться количественной оценке, что может являться проблемой при анализе событий с существенными последствиями. В таких случаях использование комбинации технологий обычно обеспечивает более глубокое понимание.

Анализ риска обеспечивает входные данные для оценки риска, принятия решения о том, следует ли обрабатывать риск и как, а также о наиболее подходящей стратегии и методах ее реализации. Результаты дают представление о сути принятого решения, которое является результатом выбора с учетом различных типов и уровней риска.

6.4.4 Сравнительная оценка риска

Цель сравнительной оценки риска заключается в поддержке принятия решений. Сравнительная оценка риска включает в себя сравнение результатов анализа риска с установленными критериями риска, чтобы определить, где требуются дополнительные действия. Это может привести к принятию следующих решений:

- не предпринимать никаких мер;
- рассмотреть варианты обработки риска;
- провести дальнейший анализ, чтобы лучше понять риск;
- поддерживать существующие методы управления риском;
- пересмотреть цели.

Решения должны учитывать широкое влияние среды, фактические и потенциальные последствия для внешних и внутренних причастных сторон.

Результаты сравнительной оценки риска должны быть задокументированы, доведены до сведения причастных сторон, а затем подтверждены на соответствующих уровнях организации.

6.5 Обработка риска

6.5.1 Общие положения

Целью обработки риска является выбор и реализация вариантов обработки риска.

Обработка риска представляет собой итеративный процесс, включающий:

- определение и выбор вариантов обработки риска;
- планирование и осуществление мероприятий по обработке риска;
- оценка эффективности такой обработки;
- принятие решений о приемлемости остаточного уровня риска;
- если риск неприемлем, осуществление дальнейшей обработки риска.

6.5.2 Выбор вариантов обработки риска

Выбор наиболее подходящего варианта (вариантов) обработки риска включает в себя принятие взвешенного решения с учетом потенциальных выгод от достижения целей с одной стороны и понесенных затрат, усилий или недостатков данного решения с другой.

Варианты обработки риска не обязательно являются взаимоисключающими или подходящими при любых обстоятельствах. Варианты обработки риска могут включать одно или несколько из следующих:

- избежание риска посредством решения не начинать или не продолжать деятельность, в результате которой возникает риск;
- принятие или увеличение риска для использования благоприятной возможности;
- устранение источника риска;
- изменение вероятности реализации риска;
- изменение последствий реализации риска;
- разделение риска с другой стороной или сторонами (например, договор аутсорсинга, страхование);
- осознанное удержание риска путем принятия обоснованного решения.

При выборе варианта обработки риска учитываются не только экономические соображения, но и все обязательства организации, включая добровольные обязательства и мнения причастных сторон. Выбор варианта обработки риска должен производиться в соответствии с целями организации, критериями риска и имеющимися ресурсами.

При выборе вариантов обработки риска организация должна учитывать ценности, восприятие и потенциальное вовлечение причастных сторон и наиболее подходящие способы обмена информации и консультирования с ними. Несмотря на эффективность, некоторые виды обработки риска могут быть более приемлемыми для некоторых причастных сторон, чем для других.

Методы обработки риска, даже если они тщательно разработаны и реализованы, могут не дать ожидаемых результатов и могут привести к непредвиденным последствиям. Мониторинг и пересмотр должны быть неотъемлемой частью реализации методов обработки риска, чтобы гарантировать, что различные формы обработки риска продолжат оставаться эффективными.

Обработка риска также может привести к новым рискам, которыми необходимо управлять.

Если отсутствуют доступные варианты обработки риска или если варианты недостаточно эффективны, риск следует задокументировать и держать под постоянным наблюдением.

Лица, принимающие решения, и другие причастные стороны должны быть осведомлены о характере и уровне остаточного риска после обработки риска. Остаточный риск должен быть задокументирован и подлежать регулярному мониторингу, пересмотру и, при необходимости, дальнейшей обработке.

6.5.3 Подготовка и реализация планов обработки риска

Целью реализации планов обработки риска является обеспечение того, чтобы выбранные варианты обработки риска были реализованы и поняты участвующими сторонами, а также, чтобы обсуществялся мониторинг их выполнения. План обработки риска должен четко определять порядок, в соответствии с которым следует осуществлять данную обработку.

Планы обработки риска должны быть интегрированы в планы управления и процессы организации по результатам консультирования с соответствующими причастными сторонами.

Информация, содержащаяся в плане обработки риска, должна включать:

- обоснование выбора вариантов обработки, включая ожидаемые выгоды;
- ответственных за утверждение и реализацию плана;
- предлагаемые действия;
- требуемые ресурсы, включая непредвиденные расходы;
- показатели эффективности;
- ограничения;
- требования к отчетности и мониторингу;
- сроки реализации и завершения мероприятий.

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 менеджмента риска и его результатов должны быть запланированной частью процесса менеджмента риска, ответственность за его выполнение должна быть четко определена.

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 пересмотра должны быть частью системы измерения эффективности деятельности, а также отчетности организации.

6.7 Документирование и отчетность

Процесс менеджмента риска и его результаты должны документироваться и отражаться в отчетности с помощью соответствующих механизмов. Регистрация и отчетность направлены на:

- информирование о деятельности по менеджменту риска и ее результатах по всей организации;
- предоставление информации для принятия решений;
- совершенствование деятельности по менеджменту риска;
- содействие в работе с причастными сторонами, включая лиц, ответственных за выполнение действий и подотчетность в процессе менеджмента риска.

Решения, касающиеся создания, хранения и обработки документированной информации, должны учитывать, но не ограничиваться возможностью ее использования, чувствительностью информации, внешней и внутренней средой.

Подготовка отчетности является неотъемлемой частью управления организацией, что должно повышать качество взаимодействия с причастными сторонами и поддерживать высшее руководство и надзорные органы в выполнении ими своих обязанностей. Факторы, которые следует учитывать при формировании отчетности, включают, но не ограничиваются:

- различиями причастных сторон и их специфическими потребностями и требованиями к информации;
- стоимостью, периодичностью и своевременностью отчетности;
- формой подготовки и способом предоставления отчетности;
- соответствием информации организационным целям и принимаемым решениям.

Библиография

[1] IEC 31010 Risk management — Risk assessment techniques (Менеджмент риска. Технологии оценки риска)

УДК 658.5.011:006.354 ОКС 03.100.01 IDT

Ключевые слова: риск, менеджмент риска, риск-менеджмент, оценка риска, анализ риска, обработка риска, руководство, принципы

БЗ 11—2019/29

Редактор *П.К. Одинцов*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 12.12.2019. Подписано в печать 17.01.2020. Формат 60 × 84 1/8. Гарнитура Ариал
Усл. печ. л. 2.32. Уч.-изд. л. 2,10.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru