

МЕНЕДЖМЕНТ РИСКОВ

Руководящие указания

МЕНЕДЖМЕНТ РЫЗЫКІ

Кіруючыя ўказанні

(ISO 31000:2018, IDT)

*Настоящий проект стандарта
не подлежит применению до его утверждения*



Ключевые слова: риск, менеджмент рисков, структура менеджмента риска, последствие, вероятность, источник риска, идентификация риска, оценка риска, анализ риска, уровень риска, обработка риска, критерии риска, остаточный риск

Предисловие

Цели, основные принципы, положения по государственному регулированию и управлению в области технического нормирования и стандартизации установлены Законом Республики Беларусь «О техническом нормировании и стандартизации».

1 ПОДГОТОВЛЕН научно-производственным республиканским унитарным предприятием «Белорусский государственный институт стандартизации и сертификации» (БелГИСС) ВНЕСЕН Госстандартом Республики Беларусь

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь от _____ 20____ № _____

3 Настоящий стандарт идентичен международному стандарту ISO 31000:2018 «Менеджмент риска. Руководящие указания» («Risk management – Guidelines», IDT).

Международный стандарт разработан техническим комитетом по стандартизации ISO/TC 262 «Менеджмент риска» Международной организации по стандартизации (ISO).

4 ВЗАМЕН СТБ ISO 31000-2015.

Настоящий стандарт не может быть воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Госстандарта Республики Беларусь

Издан на русском языке

Содержание

Введение	IV
1 Область применения	1
2 Нормативные ссылки.....	1
3 Термины и определения	1
4 Принципы.....	2
5 Структура.....	3
5.1 Общие положения.....	3
5.2 Лидерство и приверженность	4
5.3 Интеграция.....	5
5.4 Проектирование	5
5.5 Внедрение.....	6
5.6 Оценивание	6
5.7 Улучшение	7
6 Процесс	7
6.1 Общие положения.....	7
6.2 Коммуникации и консультирование.....	8
6.3 Область применения, контекст и критерии.....	8
6.4 Оценка рисков	9
6.5 Обработка рисков.....	10
6.6 Мониторинг, анализ и планирование действий.....	11
6.7 Ведение записей и отчетность	11
Библиография	13

Введение

Настоящий стандарт предназначен для использования персоналом, который создает и защищает ценности в организациях путем менеджмента рисков, принятия решений, установления и достижения целей и улучшения деятельности.

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

Менеджмент рисков является повторяющимся и способствует установлению стратегии организации, достижению целей и принятию обоснованных решений.

Менеджмент рисков является частью руководства и лидерства, и имеет фундаментальное значение для осуществления менеджмента организации на всех уровнях. Менеджмент рисков способствует улучшению систем менеджмента.

Менеджмент рисков является частью всех видов деятельности связанных с организацией и включает взаимодействие со стейкхолдерами.

Менеджмент рисков рассматривает внешний и внутренний контекст организации, включая поведение персонала и культурные факторы.

Менеджмент рисков основан на принципах, структуре и процессах, приведенных в настоящем стандарте, как показано на рисунке 1. Данные компоненты могут уже существовать в полной мере либо частично в рамках организации, однако они могут нуждаться в адаптации или улучшении чтобы менеджмент рисков был эффективным, результативным и согласованным.

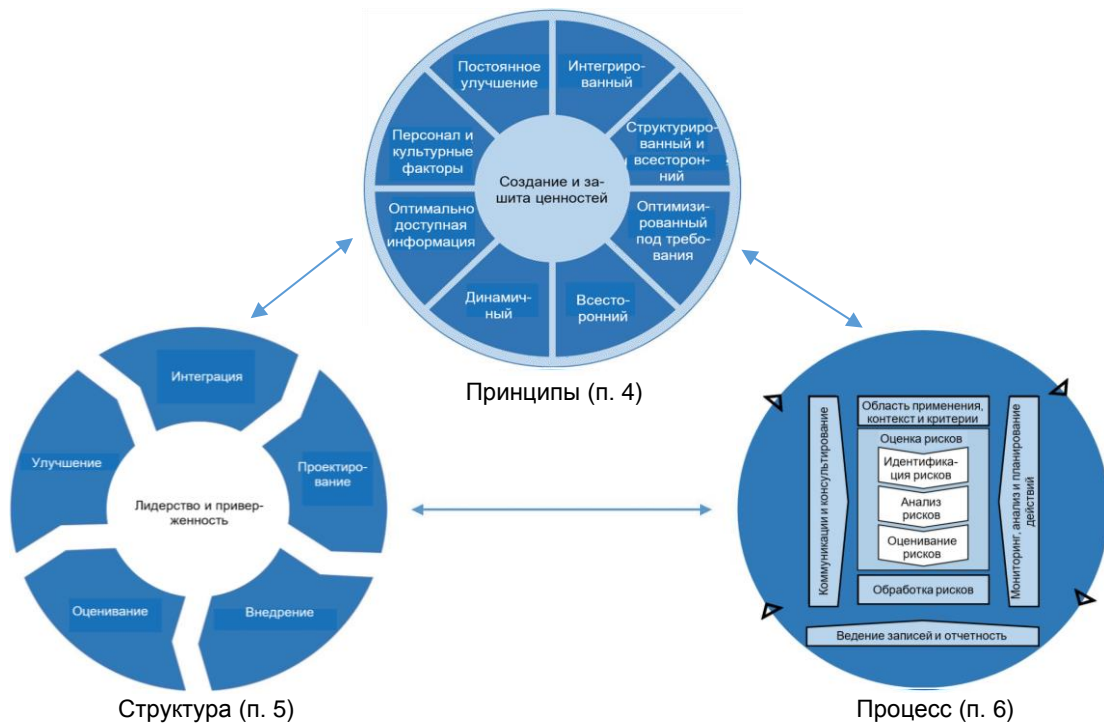


Рисунок 1 – Принципы, структура и процесс

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

МЕНЕДЖМЕНТ РИСКОВ
Руководящие указания**МЕНЕДЖМЕНТ РЫЗЫКІ**
Кіруючыя ўказанніRisk management
Guidelines

Дата введения _____

1 Область применения

Настоящий стандарт предоставляет руководящие указания по осуществлению менеджмента рисков с которыми сталкиваются организации. Применение настоящих руководящих указаний может быть подобрано под любую организацию и ее контекст.

Настоящий стандарт предоставляет общий подход к менеджменту любого типа риска и не является специфическим для отраслей промышленности или секторов.

Настоящий стандарт может использоваться на протяжении всего жизненного цикла организации и может применяться к любой деятельности, включая решения, принятые на всех уровнях.

2 Нормативные ссылки

В настоящем стандарте отсутствуют нормативные ссылки.

3 Термины и определения

Поддерживаемые ISO и IEC терминологические базы данных для использования в стандартизации находятся по следующим адресам:

– Платформа интернет-поиска ISO доступна по адресу: <http://www.iso.org/obp>

– IEC Electropedia: доступно на <http://www.electropedia.org>.

В настоящем стандарте применяют следующие термины с соответствующими определениями:

3.1 риск (risk): Воздействие неопределенности на цели.

Примечание 1 – Воздействие – отклонение от ожидания. Воздействие может быть положительным, отрицательным или и тем и другим и может обращаться, создавать или приводить к возможностям и угрозам.

Примечание 2 – Цели могут затрагивать различные аспекты и категории и могут быть применимы на различных уровнях.

Примечание 3 – Риск часто выражается в терминах: источники риска (3.4), потенциальные события (3.5), их последствия (3.6) и их вероятность (3.7).

3.2 менеджмент рисков (risk management): Скоординированная деятельность по руководству и управлению организацией в отношении риска (3.1)

3.3 стейкхолдер; заинтересованная сторона (stakeholder): Лицо или организация, которые могут воздействовать, подвергаться воздействию или воспринимать себя подверженными воздействию решения или деятельности.

Примечание 1 – Термин «заинтересованная сторона» (“interested party”) может использоваться как альтернатива термину «стейкхолдер» (“stakeholder”).

3.4 источник риска (risk source): Элемент, который отдельно или в комбинации потенциально может вызвать риск (3.1).

3.5 событие (event): Возникновение или изменение определенного набора обстоятельств.

Примечание 1 – Событие может возникнуть один или более раз и иметь разные причины и последствия (3.6).

Примечание 2 – Событие также может быть ожидаемым, которое не происходит, или неожиданным, которое происходит.

Примечание 3 – Событие может быть источником риска.

3.6 последствие (consequence): Выход события (3.5), влияющий на цели.

Примечание 1 – Последствие может быть определенным или неопределенным и может оказывать положительное и отрицательное, прямое или обратное воздействие на цели.

Примечание 2 – Последствия могут быть выражены качественно или количественно.

Примечание 3 – Любое последствие может спровоцировать каскадные и кумулятивные воздействия.

3.7 вероятность (likelihood): Случайность того, что что-либо произойдет.

Примечание 1 – В терминологии менеджмента риска (3.2) «вероятность (likelihood)» используется для обозначения случайности того, что что-либо произойдет, определенной, измеренной или установленной объективно или субъективно, выраженной качественно или количественно и описанной с использованием общих терминов или математически (таких, как вероятность или частота в заданный период времени).

Примечание 2 – Английский термин «likelihood» не имеет прямого эквивалента в некоторых языках, вместо него часто используют эквивалентный термин «probability». Однако в английском языке термин «probability» часто получает суженную интерпретацию как математический термин. Поэтому в терминологии менеджмента рисков термин «likelihood» имеет то же значение, что и термин «probability» во многих языках, кроме английского.

3.8 средство управления (control): мера, которая поддерживает и / или изменяет риск (3.1)

Примечание 1 – Средства управления включают, но не ограничиваются следующим: любой процесс, политика, устройство, практика или другие условия и/или действия, которые поддерживают и/или изменяют риск.

Примечание 2 – Средства управления не всегда позволяют достичь преднамеренного или предполагаемого изменения.

4 Принципы

Назначением менеджмента рисков является создание и защита ценностей. Менеджмент рисков улучшает пригодность, содействует инновациям и поддерживает достижение целей.

Принципы, приведенные на рисунке 2 предоставляют руководящие указания по назначению характеристик для результативного и эффективного менеджмента рисков, осуществляя обмен информацией о своей ценности и объясняя свои намерения и назначение. Принципы являются основой для осуществления менеджмента рисков, и их следует рассматривать, когда устанавливаются структуры и процессы менеджмента риска организации. Следует чтобы принципы позволяли организации осуществлять менеджмент последствий неопределенности оказывающий влияние ее цели.



Рисунок 2 – Принципы

Для результативного менеджмента риска требуются элементы, которые показаны на рисунке 2 и которые далее могут быть разъяснены следующим образом:

a) Интегрированный

Менеджмент рисков является неотъемлемой частью всей деятельности организации.

b) Структурированный и всеобщий

Структурированный и всеобщий подход к менеджменту риска способствует постоянным и сопоставимым результатам.

c) Оптимизированный под требования

Структура и процессы менеджмента риска оптимизированы и соразмерны с внешним и внутренним контекстом организации и относятся к ее целям.

d) Всесторонний

Соответствующее и своевременное вовлечение стейкхолдеров позволяет рассматривать их знания, взгляды и восприятия. Это приводит к повышению осведомленности и информированности о менеджменте рисков.

e) Динамичный

Риски могут возникать, изменяться или исчезать по мере изменения внешнего и внутреннего контекста организации. Менеджмент рисков предвидит, выявляет, подтверждает и откликается на изменения и события соответствующим и своевременным образом.

f) Основанный на лучшей из доступной информации

Входные данные для менеджмента рисков основываются на информации за прошлый и текущий периоды, а также основан на будущих ожиданиях. Менеджмент рисков точно учитывает любые ограничения и неопределенности, связанные с такой информацией и ожиданиями. Следует чтобы информация была своевременной, ясной и доступной для соответствующих стейкхолдеров.

g) Основанный на человеческих и культурных факторах

Поведение человека и культура значительно влияют на все аспекты менеджмента рисков на каждом уровне и стадии.

h) Постоянно улучшающийся

Менеджмент рисков постоянно улучшается через обучение и приобретение опыта.

5 Структура

5.1 Общие положения

Назначением структуры менеджмента риска является содействие организации в интеграции менеджмента рисков в значимые деятельность и функции. Результативность менеджмента рисков будет зависеть от его интеграции в руководство организацией, включая принятие решений. Для этого требуется поддержка от стейкхолдеров, в частности высшего руководства.

Разработка структуры охватывает интеграцию, проектирование, внедрение, оценивание, улучшение менеджмента риска по всей организации. На рисунке 3 показаны компоненты структуры.



Рисунок 3 – Структура

Организации следует оценить свои существующие практики менеджмента рисков и процессы, оценить любые пробелы и рассматривать эти пробелы в пределах структуры.

Компоненты структуры и способы их совместной работы следует подбирать под нужды организации.

5.2 Лидерство и приверженность

Высшему руководству и надзорным органам, где это применимо, следует обеспечить, чтобы менеджмент рисков был интегрирован во всю деятельность организации и демонстрировать лидерство и приверженность посредством:

- подбора и внедрением всех компонентов структуры;
- выпуска заявления или политики, которые устанавливают подход к менеджменту рисков, план или порядок действий;
- обеспечения выделения необходимых ресурсов для менеджмента рисков;
- установления полномочий, обязанностей и отчетности на соответствующих уровнях организации. Это поможет организации:
 - согласовывать менеджмент рисков с целями, стратегией и культурой;
 - признавать и рассматривать все обязанности, а также добровольные обязательства;
 - устанавливать величину и тип риска, которые могут или не могут быть использованы как руководящие указания для разработки критериев риска, гарантируя, что они будут сообщены организации и ее стейкхолдерам;
 - сообщать ценность менеджмента рисков организации и ее стейкхолдерам;
 - содействовать систематическому мониторингу рисков;
 - обеспечивать, чтобы структура менеджмента рисков продолжала оставаться соответствующей контексту организации.

Высшее руководство несет ответственность за осуществление менеджмента рисков, тогда как надзорные органы несут ответственность за осуществление надзора за менеджментом рисков. Часто от надзорных органов ожидается или требуется:

- обеспечивать, чтобы риски были соответствующим образом рассмотрены при установлении целей организации;
- понимать риски, с которыми сталкивается организация при достижении своих целей;

- обеспечивать, чтобы системы, осуществляющие менеджмент таких рисков, внедрялись и функционировали результативно;
- обеспечивать, чтобы такие риски были соответствующими контексту целей организации;
- обеспечивать, чтобы информация о таких рисках и их менеджменте сообщалась должным образом.

5.3 Интеграция

Интеграция менеджмента рисков основана на понимании структур и контекста организации. Структуры различаются в зависимости от назначения, целей и сложности организации. Менеджмент рисков осуществляется в каждой части структуры организации. Все в организации имеют обязанности в области менеджмента рисков.

Руководство организации определяет направления ее развития, ее внешние и внутренние взаимоотношения, правила, процессы и практики, необходимые для достижения намерений организации. Структуры менеджмента переводят направления развития в стратегию и связанные цели, требуемые для достижения желаемых уровней устойчивой пригодности и долгосрочной жизнеспособности. Определение отчетности в области менеджмента риска и надзорных функций внутри организации являются неотъемлемой частью руководства организацией.

Интеграция менеджмента рисков в организацию является динамичным и повторяющимся процессом, и ее следует подстраивать под нужды и культуру организации. Следует, чтобы менеджмент рисков был частью и не был отделен от назначения, руководства, лидерства и приверженности, стратегии, целей и операционной деятельности организации.

5.4 Проектирование

5.4.1 Понимание организации и ее контекста

При проектировании структуры менеджмента риска организации следует изучить и понять ее внешний и внутренний контекст.

Изучение внешнего контекста организации может включать, но не ограничивается:

- социальными, культурными, политическими, юридическими, законодательными, финансовыми, технологическими, экономическими, природными факторами на международном, национальном, региональном или локальном уровне;
- ключевыми движущими факторами и трендами, влияющими на цели организации;
- отношением, восприятием, ценностями, потребностями и ожиданиями внешних стейкхолдеров;
- договорными отношениями и обязательствами;
- сложность сетей и зависимостей.
- сложностями сетевой работы и зависимостями.

Изучение внутреннего контекста организации может включать (но не ограничивается этим):

- видение, миссия и ценности;
- руководство, организационную структуру, роли и ответственность за результат;
- стратегия, цели и политики;
- культуру организации;
- стандарты, руководящие указания и модели, принятые в организации;
- возможности, воспринимаемые в виде ресурсов и знаний (например, капитал, время, персонал, интеллектуальная собственность, процессы, системы и технологии);
- данные, информационные системы и информационные потоки;
- отношения с внутренними стейкхолдерами с учетом их восприятия и ценностей;
- договорные отношения и обязательства;
- взаимозависимости и взаимосвязи.

5.4.2 Формулирование обязательств по менеджменту рисков

Высшее руководство и надзорные органы, где это применимо, должны демонстрировать и формулировать свою постоянную приверженность менеджменту рисков посредством политики, заявлений или других форм, которые ясно отражают цели организации и приверженность к менеджменту рисков. Обязательства могут включать (но не ограничивается этим):

- намерения организации по менеджменту рисков и связь с ее целями и другими политиками;
- усиление необходимости интегрировать менеджмент рисков в общую культуру организации;
- введение интеграции менеджмента рисков в основные виды бизнес деятельности и в принятие решений;
- полномочия, обязанности и отчетность;

- предоставление необходимых ресурсов;
- каким образом разрешается конфликт целей;
- измерение и отчетность в рамках показателей пригодности организации;
- анализ и планирование действий, и улучшение.

О приверженности менеджменту рисков следует сообщить в организации и стейкхолдерам, в зависимости от обстоятельств.

5.4.3 Назначение организационных ролей, полномочий, обязанностей и отчетности

Высшему руководству и надзорным органам, где это применимо, следует обеспечить, чтобы полномочия, обязанности и отчетность по соответствующим ролям в отношении менеджмента рисков были назначены и сообщены на всех уровнях организации, и следует:

- подчеркнуть, что менеджмент рисков является основной обязанностью;
- идентифицировать отдельных лиц, ответственных за результат и обладающих полномочиями по менеджменту рисков (владельцы риска).

5.4.4 Распределение ресурсов

Высшему руководству и надзорным органам, где это применимо, следует обеспечивать выделение соответствующих ресурсов для менеджмента рисков, которые могут включать (но не ограничиваются):

- персонал, навыки, опыт и компетенцию;
- процессы, методы и инструменты организации, которые будут использоваться для осуществления менеджмента рисков;
- документированные процессы и процедуры;
- системы менеджмента информации и знаний;
- профессиональное развитие и потребности в подготовке.

Организации следует учитывать возможности и ограничения существующих ресурсов.

5.4.5 Установление коммуникаций и консультирование

Организации следует установить одобренный подход к коммуникациям и консультациям, чтобы поддержать структуру и способствовать результативному применению менеджмента рисков. Коммуникация предполагает обмен информацией с целевой аудиторией. Консультация также охватывает участников, предоставляющих обратную связь с ожиданиями, что это будет способствовать и вносить вклад в общие решения или другие действия. Следует, чтобы методы и содержание коммуникаций и консультаций отражали ожидания стейкхолдеров, где это уместно.

Следует чтобы коммуникации и консультации были своевременными и обеспечивали, чтобы соответствующая информация собиралась, сопоставлялась, обобщалась и распространялась, в зависимости от обстоятельств, а также обеспечивалась обратная связь и проводились улучшения.

5.5 Внедрение

Организации следует внедрить структуру менеджмента риска путем:

- разработки соответствующего плана, включая распределение времени и ресурсов;
- идентификации того, где, когда и как различные типы решений принимаются в рамках организации и кем;
- изменения применимых процессов принятия решений, где это необходимо;
- обеспечения того, чтобы организационные мероприятия по менеджменту рисков были четко поняты и применены на практике.

Успешное внедрение структуры требует участия и осведомленности стейкхолдеров. Это позволяет организациям явно учитывать неопределенность при принятии решений, а также обеспечивает возможность учета любой новой или последующей неопределенности по мере ее возникновения.

Правильно спроектированная и внедренная структура менеджмента риска обеспечит, чтобы процесс менеджмента риска являлся частью всей деятельности организации, включая принятие решений, и что изменения во внешнем и внутреннем контекстах будут адекватно учтены.

5.6 Оценивание

Чтобы обеспечить оценивание результативности системы менеджмента рисков, организации следует:

- периодически измерять пригодность структуры менеджмента рисков относительно намерений, планов внедрения, показателей и ожидаемого поведения;
- определить, остается ли он приемлемым для поддержки достижения целей организации.

5.7 Улучшение

5.7.1 Адаптация

Организации следует постоянно осуществлять мониторинг и адаптировать структуру менеджмента рисков для учета внешних и внутренних изменений. При этом организация может увеличить свою ценность.

5.7.2 Постоянное улучшение

Организации следует постоянно улучшать приемлемость, адекватность и результативность структуры менеджмента рисков и пути интеграции процессов менеджмента рисков.

По мере идентификации соответствующих пробелов в или возможностей для улучшения организации следует разработать планы и задачи и назначить ответственных за их выполнение. Следует чтобы после внедрения эти улучшения способствовали усилению менеджмента рисков.

6 Процесс

6.1 Общие положения

Процесс менеджмента риска включает в себя систематическое применение политик, процедур и практик к деятельности по информированию и консультированию, установлению контекста и оценке, обработке, мониторингу, анализу и планированию действий, ведению записей и отчетности о рисках. Этот процесс показан на рисунке 4.

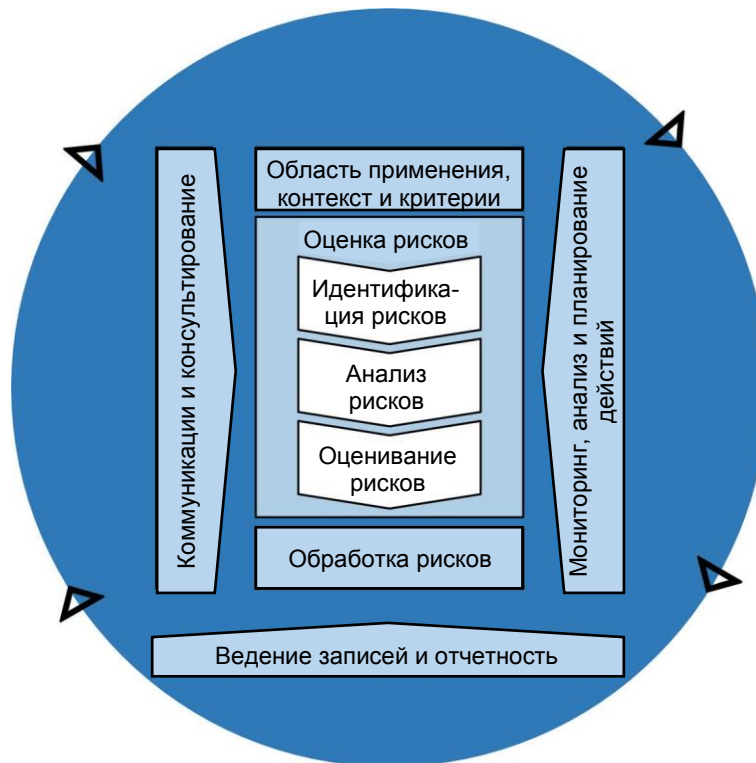


Рисунок 4 – Процесс

Следует чтобы процесс менеджмента рисков стал неотъемлемой частью менеджмента и принятия решений и был интегрирован в структуру, операционную деятельность и процессы организации. Он может применяться на стратегическом, операционном, программном или проектном уровнях.

Может быть много применений процесса менеджмента рисков в организации, приспособленных для достижения целей и для соответствия внешнему и внутреннему контексту, в котором он применяется.

Динамический и вариационный характер человеческого поведения и культуры следует учитывать на протяжении всего процесса менеджмента рисков.

Хотя процесс менеджмента рисков часто представляется последовательным, на практике он повторяющийся.

6.2 Коммуникации и консультирование

Назначение коммуникаций и консультаций - помочь соответствующим стейкхолдерам понять риск, основу, на которой принимаются решения, и причины, которые требуют конкретных действий. Коммуникация направлена на содействие осознанию и пониманию риска, тогда как консультации подразумевают получение обратной связи и информации для поддержки принятия решений. Следует чтобы тесная координация между ними способствовала фактическому, своевременному, актуальному, точному и понятному обмену информацией с учетом конфиденциальности и целостности информации, а также прав на неприкосновенность частной жизни отдельных лиц.

Следует чтобы коммуникация и консультирование с соответствующими внешними и внутренними стейкхолдерами осуществлялась в пределах каждого и в рамках всех шагов процесса менеджмента рисков.

Коммуникация и консультации направлены на то, чтобы:

- объединить различные области знаний для каждого шага процесса менеджмента рисков;
- обеспечивать рассмотрение соответствующим образом различных точек зрения при определении критериев риска и при оценивании рисков;
- предоставлять достаточную информацию для облегчения наблюдения за рисками и принятия решений;
- создать чувство вовлеченности и причастности среди тех, кто подвержен риску.

6.3 Область применения, контекст и критерии

6.3.1 Общие положения

Назначением определения области применения, контекста и критериев является настройка процесса менеджмента рисков, позволяющая проводить результативную оценку рисков и соответствующую обработку рисков. Область применения, контекст и критерии включают определение области применения процесса и понимание внешнего и внутреннего контекста.

6.3.2 Определение области применения

Организации следует определить область применения своей деятельности по менеджменту рисков.

Поскольку процесс менеджмента рисков может быть применен на разных уровнях (например, на стратегическом, операционном, программном, проектном или для других видов деятельности), важно четко понимать рассматриваемую область применения, связанные цели, которые следует учитывать, и соответствие его целям организации.

При планировании подхода рассматриваются следующие факторы:

- цели и решения, которые необходимо принять;
- ожидаемые выходы шагов, которые будут предприняты в процессе;
- время, место, что конкретно включено и исключено;
- соответствующие инструменты и техники оценки риска;
- требуемые ресурсы, обязанности и записи, которые должны вестись;
- взаимоотношения с другими проектами, процессами и действиями.

6.3.3 Внешний и внутренний контекст

Внутренний и внешний контекст – это среда, в которой организация стремится определять и достигать своих целей.

Контекст процесса менеджмента рисков следует установить на основе понимания внешней и внутренней среды, в которой организация выполняет операционную деятельность и следует чтобы он отражал специфику среды для деятельности, к которой должен применяться процесс менеджмента рисков.

Понимание контекста важно, потому что:

- менеджмент рисков осуществляется в контексте целей и деятельности организации;
- организационные факторы могут быть источником риска;
- назначение и область применения процесса менеджмента рисков могут быть взаимосвязаны с целями организации в целом.

Организации следует установить внешний и внутренний контекст процесса менеджмента рисков с учетом факторов, упомянутых в 5.4.1.

6.3.4 Определение критериев риска

Организации следует указать величину и тип риска, который она может или не может принять, относительно целей. Следует также определить критерии для оценивания значимости риска и для поддержки процессов принятия решений. Критерии риска должны быть согласованы со структурой менеджмента риска и оптимизированы к конкретным намерениям и области применения деятельности, которая рассматривается. Следует чтобы критерии риска отражали ценности, цели и ресурсы организации и согласовывались с политиками и заявлениями об осуществлении менеджмента рисков.

Критерии следует определять с учетом рассмотрения обязательств организации и мнений стейкхолдеров.

Хотя критерии риска должны быть установлены в начале процесса оценки риска, они являются динамичными и их следует постоянно пересматривать, а также исправлять при необходимости.

Чтобы установить критерии риска, следует рассмотреть следующее:

- характер и тип неопределенностей, которые могут повлиять на выходы и цели (как материальные, так и нематериальные);
- как будут определены и измерены последствия (как положительные, так и отрицательные) и их вероятность;
- факторы, связанные со временем;
- согласованность в использовании измерений;
- как должен быть определен уровень риска;
- как будут учитываться комбинации и последовательности множественных рисков;
- потенциал организации.

6.4 Оценка рисков

6.4.1 Общие положения

Оценка рисков – это общий процесс идентификации рисков, анализа рисков и оценивания рисков.

Оценку риска следует проводить систематически, итерационно и в сотрудничестве со стейкхолдерами, опираясь на их знания и мнения. Для этого следует использовать лучшую доступную информацию, дополненную дальнейшими запросами по мере необходимости.

6.4.2 Идентификация рисков

Назначением идентификации риска является поиск, признание и описание рисков, которые могут помочь или помешать организации достичь своих целей. При идентификации рисков важна соответствующая, подходящая и актуальная информация.

Организация может использовать ряд техник для идентификации неопределенностей, которые могут воздействовать на одну или несколько целей. Следует рассматривать следующие факторы и взаимосвязь между этими факторами:

- материальные и нематериальные источники риска;
- причины и события;
- угрозы и возможности;
- уязвимости и возможности;
- изменения во внешнем и внутреннем контексте;
- показатели появления рисков;
- характер и ценность активов и ресурсов;
- последствия и их воздействие на цели;
- ограниченность знаний и надежность информации;
- факторы, связанные со временем;
- предвзятость, предположения и убеждения тех, кто вовлечен.

Организации следует идентифицировать риски независимо от того, находятся ли их источники под ее управлением или нет. Следует учитывать, что может быть более одного типа выходов, которые могут привести к множеству последствий материального или нематериального характера.

6.4.3 Анализ рисков

Назначение анализа рисков состоит в том, чтобы понять природу риска и его характеристики, включая, если применимо, уровень риска. Анализ рисков включает подробное рассмотрение неопределенностей, источников риска, последствий, вероятности, событий, сценариев, средств управления и их результативности. Событие может иметь множественные причины и последствия и может воздействовать на множество целей.

Анализ рисков может осуществляться с различной степенью детальности и сложности в зависимости от цели анализа, доступности информации и доступных ресурсов. Анализ может быть качественным, количественным либо их комбинацией в зависимости от обстоятельств и предназначения для использования.

Следует чтобы анализ рисков учитывал такие факторы, как:

- вероятность событий и последствий;
- характер и масштабы последствий;
- сложность и связность;
- связанные со временем факторы и волатильность;
- результативность существующих средств управления;
- уровни чувствительности и достоверности.

На анализ риска могут влиять любые расхождения мнений, предвзятость, восприятие риска и суждения. Дополнительно на качество используемой информации влияют сделанные предположения и исключения, любые ограничения для техник и способы их выполнения. Следует чтобы это влияние было рассмотрено, задокументировано и доведено до сведения лиц, принимающих решения.

Высоко неопределенные события могут быть трудно определить количественно. Это может быть проблемой при анализе событий со значимыми последствиями. В таких случаях использование комбинации техник обычно дает лучшее понимание.

Анализ рисков предоставляет входные данные для оценивания рисков, принятия решений относительно необходимости дальнейшей обработки рисков и как ее провести, а также для выбора наиболее подходящей стратегии и методов обработки рисков. Результаты дают понимание для принятия решений, когда делается выбор, а варианты предусматривают различные типы и уровни риска.

6.4.4 Оценивание рисков

Назначением оценивания риска является поддержка решений. Оценивание риска включает сравнение результатов анализа риска с установленными критериями риска, чтобы определить, где требуются дополнительные действия. Это может привести к решению:

- ничего не делать дальше;
- рассмотреть варианты обработки риска;
- провести дальнейший анализ, чтобы лучше понять риск;
- поддерживать существующие средства управления;
- пересмотреть цели.

Следует чтобы решения учитывали более широкий контекст, а также фактические и предполагаемые последствия для внешних и внутренних стейкхолдеров.

Следует чтобы выходы оценивания риска были записаны, доведены до сведения и затем валидированы на соответствующих уровнях организации.

6.5 Обработка рисков

6.5.1 Общие положения

Назначением обработки риска является выбор и внедрение вариантов для рассмотрения риска. Обработка рисков предусматривает повторяющийся процесс, состоящий из:

- формулирования и выбора вариантов обработки риска;
- планирования и внедрения обработки риска;
- проведения оценки результативности этой обработки;
- решения, является ли остаточный риск приемлемым;
- если он не приемлем, проведения дальнейшей обработки.

6.5.2 Выбор вариантов обработки рисков

Выбор наиболее подходящего варианта (ов) обработки риска включает в себя баланс потенциальных выгод, полученных в связи с достижением целей и затрат, усилий или вреда от внедрения.

Варианты обработки рисков не обязательно являются взаимоисключающими или подходящими для всех обстоятельств. Варианты обработки риска могут включать одно или несколько из следующего:

- избегание риска посредством принятия решения не начинать или не продолжать деятельность, которая обуславливает возникновение риска;
- принятие или повышение риска для использования возможностей;
- устранение источника риска;
- изменение вероятности;
- изменение последствий;

- разделение риска (например, по контракту, путем покупки страховки);
- сохранение риска на основании обоснованного решения.

Обоснование обработки риска является более широким, чем чисто экономические соображения, и должно учитывать все обязательства организации, добровольно принятые обязанности и мнения стейкхолдеров. Следует чтобы выбор вариантов обработки риска осуществлялся в соответствии с целями организации, критериями риска и доступными ресурсами.

При выборе вариантов обработки рисков организации следует рассматривать ценности, восприятие и потенциальное вовлечение стейкхолдеров, а также наиболее подходящие способы коммуникации и консультирования с ними. Несмотря на одинаковую результативность, некоторые варианты обработки рисков могут быть более приемлемыми для одних стейкхолдеров, чем для других.

Обработка риска, даже если она тщательно спроектирована и внедрена, может не дать ожидаемых выходов и может привести к непреднамеренным последствиям. Мониторинг и пересмотр должны быть неотъемлемой частью внедрения обработки рисков, чтобы обеспечивать гарантию того, что различные формы обработки рисков становятся и остаются результативными.

Обработка риска также может вводить новые риски, менеджмент которых необходимо осуществлять.

Если нет доступных вариантов обработки или если варианты обработки недостаточно модифицируют риск, следует чтобы риск был зарегистрирован и постоянно пересматривался.

Следует, чтобы лица, принимающие решения, и другие стейкхолдеры были осведомлены о характере и величине оставшегося риска после обработки риска. Следует, чтобы оставшийся риск был задокументирован и подвергался мониторингу, пересмотру и, при необходимости, дальнейшей обработке.

6.5.3 Подготовка и внедрение планов обработки рисков

Назначением планов обработки риска является установление того, как будут реализованы выбранные варианты обработки, чтобы участники могли понять договоренности и осуществляли мониторинг хода выполнения плана. Следует, чтобы план обработки рисков четко идентифицировал порядок, в соответствии с которыми следует применять обработку рисков.

Планы обработки следует интегрировать в планы и процессы менеджмента организации и консультироваться с соответствующими стейкхолдерами.

Следует, чтобы информация, представленная в планах обработки рисков, включала:

- обоснование для выбора вариантов обработки, включая ожидаемые выгоды, которые должны быть получены;
- тех, кому назначены отчетность и обязанности по одобрению и внедрению плана;
- предлагаемые действия;
- необходимые ресурсы, включая чрезвычайные ситуации;
- измерения пригодности;
- ограничения;
- требуемая отчетность и мониторинг;
- указание о том, когда действия должны быть предприняты и завершены.

6.6 Мониторинг, анализ и планирование действий

Назначением мониторинга, анализа и планирования действий является обеспечение и улучшение качества и результативности процессов проектирования, внедрения и их выходов. Следует чтобы постоянный мониторинг, периодический анализ и планирование действий процесса менеджмента риска и его выходов были запланированными частями процесса менеджмента риска с четко определенными обязанностями.

Мониторинг, анализ и планирование действий следует осуществлять на всех стадиях процесса. Мониторинг, анализ и планирование действий включают планирование, сбор и анализ информации, запись результатов и предоставление обратной связи.

Следует чтобы результаты мониторинга, анализа и планирования действий были включены в менеджмент пригодности организации, ее деятельность по измерениям и отчетность.

6.7 Ведение записей и отчетность

Процесс менеджмента рисков и его выходы следует документировать и представлять с помощью соответствующих механизмов. Запись и отчетность направлены на:

- обмен информацией о деятельности и выходах менеджмента риска во всей организации;
- предоставление информации для принятия решений;

СТБ ISO 31000/ПР_1

- улучшение деятельности по менеджменту риска;
- содействие взаимодействию с стейкхолдерами, в том числе по обязанностям и отчетности в области деятельности по менеджменту риска.

Следует чтобы решения, касающиеся создания, хранения и обработки документированной информации принимали во внимание, но не ограничивались: использованием информации, чувствительностью информации, а также внешним и внутренним контекстом.

Отчетность является неотъемлемой частью руководства организацией и следует чтобы повышалось качество диалога со стейкхолдерами и оказывалась поддержка высшему руководству и надзорным органам в выполнении их обязанностей. Факторы, которые следует учитывать при составлении отчетности, включают, но не ограничиваются:

- различные стейкхолдеры и их конкретные информационные потребности и требования;
- стоимость, частота и своевременность отчетности;
- метод отчетности;
- актуальность информации для целей организации и принятия решений.

Библиография

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