

МЕНЕДЖМЕНТ РИСКА

Принципы и руководящие указания

МЕНЕДЖМЕНТ РЫЗЫКІ

Прынцыпы і кіруючыя ўказанні

(ISO 31000:2009, IDT)

Настоящий проект стандарта не подлежит применению до его утверждения



УДК

МКС 03.100.01.

КП 02

IDT

Ключевые слова: риск, менеджмент риска, 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 _____ № _____.

3 Настоящий стандарт идентичен международному стандарту ISO 31000:2009 Risk management – Principles and guidelines (Менеджмент риска. Принципы и руководство).

Международный стандарт разработан рабочей группой по менеджменту риска Технического руководящего бюро (ТМБ) Международной организации по стандартизации (ISO).

Перевод с английского языка (en).

Официальные экземпляры международного стандарта, на основе которого подготовлен настоящий государственный стандарт, и международных стандартов, на которые даны ссылки, имеются в Национальном фонде ТНПА.

В тексте стандарта ссылки на международные стандарты актуализированы.

Сведения о соответствии государственных стандартов ссылочным международным стандартам приведены в дополнительном приложении Д.А.

Степень соответствия – идентичная (IDT)

4 ВВЕДЕН ВПЕРВЫЕ

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

Издан на русском языке

Содержание

Введение	
1 Область применения	
2 Термины и определения	
3 Принципы.....	
4 Структура.....	
4.1 Общие положения	
4.2 Полномочия и обязательства	
4.3 Проектирование структуры менеджмента риска	
4.4 Применение менеджмента риска	
4.5 Мониторинг и анализ структуры	
4.6 Постоянное улучшение структуры	
5 Процесс	
5.1 Общие положения	
5.2 Обмен информацией и консультирование	
5.3 Определение контекста	
5.4 Оценка риска	
5.5 Обработка риска	
5.6 Мониторинг и анализ	
5.7 Документирование процесса менеджмента риска	
Приложение А (справочное) Признаки усовершенствованного менеджмента	
Библиография	
Приложение Д.А (справочное) Сведения о соответствии государственных стандартов ссылочным международным стандартам	

Введение

Организации всех типов и размеров сталкиваются с внутренними и внешними факторами, а также воздействиями, которые порождают неопределенность в отношении того, достигнут ли они своих целей, и сроков достижения целей. Влияние такой неопределенности на цели организации и есть «риск».

Вся деятельность организации включает в себя риск. Организации осуществляют управление риском посредством идентификации риска, анализа риска и последующего оценивания, будет ли риск изменен посредством обработки, чтобы соответствовать критериям риска. На протяжении всего этого процесса они обмениваются информацией и консультируются с заинтересованными сторонами, осуществляют контроль и анализ риска, а также действия по управлению, которые изменяют риск для обеспечения того, что обработки риска в дальнейшем больше не потребуется. Настоящий стандарт подробно описывает этот систематический и логический процесс.

Поскольку все организации в определенной степени управляют риском, настоящий стандарт устанавливает ряд принципов, которые необходимо соблюдать для того, чтобы менеджмент риска был результативным. Настоящий стандарт рекомендует, чтобы организации разрабатывали, внедряли и постоянно улучшали структуру, цель которой заключается в интегрировании процесса менеджмента риска в общее управление организацией, стратегию и планирование, менеджмент, процессы отчетности, политику, ценности и культуру.

Менеджмент риска может применяться ко всей организации в любое время, во многих областях и на многих уровнях, а также к особым функциям, проектам и видам деятельности.

Несмотря на непрерывное развитие практики менеджмента во многих отраслях с целью соответствия различным потребностям, принятие постоянных процессов в рамках общей структуры может способствовать эффективному и результативному менеджменту риска во всей организации. Обобщенный подход, приведенный в настоящем стандарте, устанавливает принципы и руководство по менеджменту любого вида риска систематическим, прозрачным и надежным образом, и в рамках любой области и содержания.

Каждая конкретная область или сфера применения менеджмента риска имеет свои отдельные потребности, потребителей, представления и критерии. Поэтому, основной особенностью настоящего стандарта является включение «определения контекста» как вида деятельности в начало этого обобщенного процесса менеджмента риска. При определении контекста необходимо рассматривать цели организации, окружающую среду, в которой эти цели осуществляются, заинтересованные стороны и разнообразие критериев риска, все то, что помогает выявлять и оценивать характер и сложность этих рисков.

На рисунке 1 показана взаимосвязь принципов менеджмента риска, структура, в которой он возникает, и процесс менеджмента риска, приведенный в настоящем стандарте.

Применение менеджмента риска в соответствии с настоящим стандартом дает возможность организации:

- повышать вероятность достижения целей;
- поддерживать проактивный менеджмент;
- осознавать необходимость идентифицировать и обрабатывать риск во всей организации;
- улучшать идентификацию возможностей и опасных событий;
- соответствовать законодательным и другим обязательным требованиям, а также международным нормам;
- улучшать обязательное и добровольное представление информации;
- улучшать управление;
- повышать уверенность и доверие заинтересованных сторон;
- устанавливать надежную базу для принятия решений и планирования;
- совершенствовать контроль;
- эффективно распределять и использовать ресурсы для обработки риска;
- повышать эффективность и результативность;
- совершенствовать обеспечение безопасности и здоровья, а также защиты окружающей среды;
- совершенствовать меры по предотвращению потерь и действия по контролю происшествий;
- сводить к минимуму потери;
- улучшать обучение на рабочем месте; и
- повышать устойчивость организации.

Настоящий стандарт предназначен для удовлетворения потребностей широкого круга заинтересованных сторон, включая:

- а) лиц, ответственных за разработку политики менеджмента риска, в рамках их организаций;
- б) лиц, ответственных за обеспечение результативного менеджмента риска в рамках организации в целом, или в рамках конкретной области, проекта или деятельности;
- с) лиц, которым необходимо оценивать результативность организации в управлении риском; и
- д) разработчиков стандартов, руководств, процедур и кодексов установившейся практики, которые в целом или частично, устанавливают, как осуществлять управление риском в рамках определенного содержания этих документов.

Современные практики менеджмента и процессы многих организаций включают компоненты менеджмента риска, а многие организации уже используют соответствующий процесс менеджмента риска для конкретных типов риска или обстоятельств. В этих случаях организация может принять решение о проведении критического анализа используемых ею практик и процессов с учетом настоящего стандарта.

В настоящем стандарте используются оба выражения: «управление риском» и «менеджмент риска». В общих чертах выражение «менеджмент риска» касается архитектуры (принципов, структуры и процесса) для результативного управления риском, тогда как выражение «управление риском» касается применения этой архитектуры к конкретным рискам.

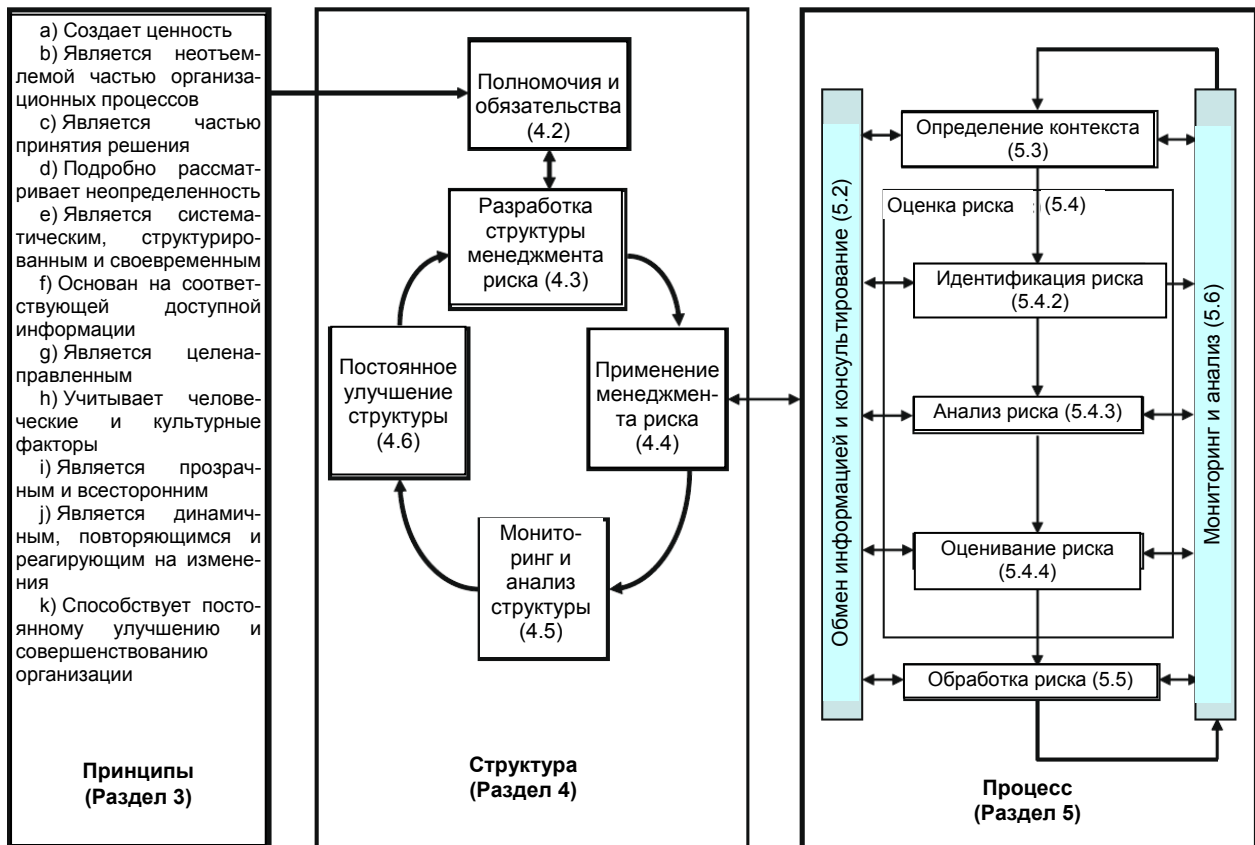


Рисунок 1 – Взаимосвязь между принципами, структурой и процессом менеджмента риска

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

МЕНЕДЖМЕНТ РИСКА
Принципы и руководящие указанияМЕНЕДЖМЕНТ РЫЗЫКІ
Прынцыпы і кіруючыя ўказанніRisk management
Principles and guidelines

Дата введения xxxx-xx-xx

1 Область применения

Настоящий стандарт устанавливает принципы и содержит общие руководящие указания по менеджменту риска.

Настоящий стандарт может использоваться любыми государственными, частными или общественными организациями, ассоциациями, группами лиц или отдельными лицами. Следовательно, настоящий стандарт не является специфическим для какой-либо промышленности или отрасли.

Примечание – Для всех пользователей настоящего стандарта применяется общий термин «организация».

Настоящий стандарт может применяться в течение всего жизненного цикла организации и для широкого спектра видов деятельности, включая стратегии и решения, операции, процессы, функции, проекты, продукцию, услуги и активы.

Настоящий стандарт можно применять к любому типу риска, независимо от его характера, а также отрицательных или положительных последствий.

Несмотря на то, что стандарт предоставляет общие руководящие указания, он не предназначен для обеспечения одинакового менеджмента риска во всех организациях. При создании и применении планов и структуры менеджмента риска необходимо учитывать различные потребности конкретной организации, ее определенные цели, контекст, структуру, деятельность, процессы, функции, проекты, продукцию, услуги или активы и конкретные используемые практические методы.

Настоящий стандарт применяется для гармонизации процессов менеджмента риска, описанных в существующих и будущих стандартах. Он устанавливает общий подход, поддерживающий стандарты, распространяющиеся на конкретные риски и/или отрасли, и не заменяет эти стандарты.

Данный стандарт не предназначен для целей сертификации.

2 Термины и определения

В настоящем стандарте применяют следующие термины с соответствующими определениями.

2.1 риск (risk): Результат неопределенности в отношении целей

Примечание 1 – Результат – это отклонение от предполагаемого (положительного и/или отрицательного).

Примечание 2 – Цели могут иметь различные аспекты (например, финансовые цели, цели охраны здоровья и безопасности, экологические цели) и могут применяться на различных уровнях (стратегических, в масштабах организации, проекта, продукции или процесса).

Примечание 3 – Риск часто характеризуется возможными **событиями** (2.17) и **последствиями** (2.18) или их сочетанием.

Примечание 4 – Риск часто выражают в виде комбинации последствий события (включая изменения в обстоятельствах) и связанной с ним **вероятностью** (2.19) возникновения.

Примечание 5 – Неопределенность – это состояние, недостаточность (даже частичная) информации, связанной с пониманием события или знаниями о нем, его последствиями или вероятностью.

[ISO Guide 73:2009, определение 1.1]

2.2 менеджмент риска (risk management): Скоординированные действия по руководству и управлению организацией в отношении **риска** (2.1)

[ISO Guide 73:2009, определение 2.1]

Проект, первая редакция

2.3 структура менеджмента риска (risk management framework): Ряд компонентов, обеспечивающих принципы и организационные мероприятия по разработке, применению, **мониторингу** (2.28), анализу и постоянному улучшению **менеджмента риска** (2.2) в масштабе всей организации

Примечание 1 – Принципы включают политику, цели, полномочия и обязательства по менеджменту **риска** (2.1).

Примечание 2 – Организационные мероприятия включают планы, взаимосвязи, ответственность, ресурсы, процессы и деятельность.

Примечание 3 – Структура менеджмента риска входит в общую стратегическую политику и принципы деятельности.

[ISO Guide 73:2009, определение 2.1.1]

2.4 политика менеджмента риска (risk management policy): Утверждение общих намерений и направлений деятельности организации в отношении **менеджмента риска** (2.2)

[ISO Guide 73:2009, определение 2.1.2]

2.5 отношение к риску (risk attitude): Подход организации к оценке и, в результате, к сохранению, принятию или исключению **риска** (2.1)

[ISO Guide 73:2009, определение 3.7.1.1]

2.6 план менеджмента риска (risk management plan): Схема **структуры менеджмента риска** (2.3), определяющая подход, элементы менеджмента и ресурсы, применяемые для управления **риском** (2.1)

Примечание 1 – Элементы менеджмента обычно включают процедуры, методы, распределение обязанностей, последовательность действий и время.

Примечание 2 – План менеджмента риска может применяться для конкретной продукции, процесса и проекта, а также к части или ко всей организации.

[ISO Guide 73:2009, определение 2.1.3]

2.7 владелец риска (risk owner): Лицо или объект, которое имеет соответствующие полномочия и несет ответственность за управление **риском** (2.1)

[ISO Guide 73:2009, определение 3.5.1.5]

2.8 процесс менеджмента риска (risk management process): Систематическое применение политики, процедур и методов управления к деятельности по обмену информацией, консультированию, установлению контекста, а также идентификации, анализу, оценке, обработке, **мониторингу** (2.28) и анализу **риска** (2.1)

[ISO Guide 73:2009, определение 3.1]

2.9 установление контекста (establishing the context): Определение внешних и внутренних параметров, принимаемых во внимание при осуществлении менеджмента риска, и установление области применения и **критериев риска** (2.22) для **политики менеджмента риска** (2.4)

[ISO Guide 73:2009, определение 3.3.1]

2.10 внешний контекст (external context): Внешняя среда, в которой организация стремится к достижению своих целей

Примечание – Внешний контекст может включать:

- культурную, социальную, политическую, правовую, законодательную, финансовую, технологическую, экономическую, естественную и рыночную среду на международном, региональном, национальном или локальном уровне;

- основные факторы и тенденции, влияющие на цели организации; и

- взаимосвязи с **заинтересованными сторонами** (2.13), их ожидания и ценности.

[ISO Guide 73:2009, определение 3.3.1.1]

2.11 внутренний контекст (internal context): Внутренняя среда, в которой организация стремится к достижению своих целей

Примечание – Внутренний контекст может включать:

- управление, организационную структуру, функции и ответственность;

- политику, цели и стратегии для их достижения;

- возможности, рассматриваемые в отношении ресурсов и знаний (например, капитал, время, люди, процессы, системы и технологии);

- информационные системы, информационные потоки и процессы принятия решений (как официальные, так и неофициальные);

- взаимосвязи с внутренними заинтересованными сторонами, их ожидания и ценности;

- деятельность организации;

- стандарты, руководства и модели, принятые организацией; и

- форма и объем контрактных взаимоотношений.

[ISO Guide 73:2009, определение 3.3.1.2]

2.12 обмен информацией и консультирование (communication and consultation): Непрерывные и повторяющиеся процессы, которые организация осуществляет для обеспечения, совместного использования или получения информации, а также ведения диалога с **заинтересованными сторонами** (2.13) в отношении менеджмента **риска** (2.1)

Примечание 1 – Информация может касаться наличия, характера, формы, **вероятности** (2.19), важности, оценки, приемлемости и применения менеджмента риска.

Примечание 2 – Консультирование – это двусторонний процесс квалифицированного обмена информацией между организацией и заинтересованными сторонами до принятия решения по вопросу или перед определением направления деятельности по этому вопросу. Консультирование является:

- процессом, который влияет на принятие решения посредством скорее воздействия, чем полномочий; и
- входными данными для процесса принятия решения, а не совместным принятием решения.

[ISO Guide 73:2009, определение 3.2.1]

2.13 заинтересованная сторона (stakeholder): Лицо или организация, которые могут воздействовать, или могут быть подвергнуты воздействию, а также которые осознают, что на них влияет какое-либо решение или деятельность

Примечание – Лицо, принимающее решение, может быть заинтересованной стороной.

[ISO Guide 73:2009, определение 3.2.1.1]

2.14 оценка риска (risk assessment): Общий процесс **идентификации риска** (2.15), **анализа риска** (2.21) и **оценивания риска** (2.24)

[ISO Guide 73:2009, определение 3.4.1]

2.15 идентификация риска (risk identification): Процесс выявления, исследования и описания **рисков** (2.1)

Примечание 1 – Идентификация включает идентификацию **источников риска** (2.16), **событий** (2.17), их причин и возможных **последствий** (2.18).

Примечание 2 – Идентификация риска может включать статистические данные, теоретический анализ, обоснованную точку зрения и заключение специалиста, а также потребности **заинтересованной стороны** (2.13).

[ISO Guide 73:2009, определение 3.5.1]

2.16 источник риска (risk source): Элемент, который отдельно или в комбинации, может вызывать **риск** (2.1)

Примечание – Источник риска может быть материальным и нематериальным.

[Руководство ISO Guide 73:2009, определение 3.5.1.2]

2.17 событие (event): Возникновение или изменение определенного ряда обстоятельств

Примечание 1 – Событие может возникать один раз или несколько раз и может иметь несколько причин.

Примечание 2 – Событие может включать то, что может и не произойти.

Примечание 3 – Иногда событие можно рассматривать как «инцидент» или «происшествие».

Примечание 4 – Событие без **последствий** (2.18) можно также рассматривать как «происшествие без последствий», «инцидент», «угрозу серьезного инцидента» или «опасное событие».

[ISO Guide 73:2009, определение 3.5.1.3]

2.18 последствие (consequence): Результат **события** (2.17), влияющий на цели

Примечание 1 – Событие может привести к ряду последствий.

Примечание 2 – Последствие может быть определенным или неопределенным, и может иметь положительное и отрицательное влияние на цели.

Примечание 3 – Последствия могут выражаться качественно или количественно.

Примечание 4 – Первоначальные последствия могут возрасти в результате цепной реакции.

[ISO Guide 73:2009, определение 3.6.1.3]

2.19 вероятность (likelihood): Вероятность того, что что-то может произойти

Примечание 1 – В терминологии менеджмента риска термин «вероятность» используется в отношении возможности того, что может произойти, либо определенное, измеренное или установленное объективно или субъективно, качественно или количественно, либо описанное с использованием общих условий или математически (например, вероятность или периодичность в заданный период времени).

Примечание 2 – Английский термин «likelihood» не имеет прямого эквивалента в некоторых языках, вместо него часто используют термин «probability». Однако, в английском языке термин «probability» часто интерпретируют в узком смысле, как математический термин. Следовательно, в терминологии менеджмента риска термин «likelihood» используют с тем намерением, что он должен иметь ту же самую широкую интерпретацию, которую термин «probability» имеет во многих языках, кроме английского языка.

[ISO Guide 73:2009, определение 3.6.1.1]

2.20 профиль риска (risk profile): Описание любого ряда **рисков** (2.1)

Примечание – Ряд рисков может включать риски, которые относятся ко всей организации, ее части, или риски, определенные иным образом.

[ISO Guide 73:2009, определение 3.8.2.5]

2.21 анализ риска (risk analysis): Процесс понимания характера **риска** (2.1) и определения **уровня риска** (2.23)

Примечание 1 – Анализ риска обеспечивает основу для **оценивания риска** (2.24) и принятия решений, касающихся **обработки риска** (2.25).

Примечание 2 – Анализ риска включает оценку риска.

[ISO Guide 73:2009, определение 3.6.1]

2.22 критерии риска (risk criteria): Задачи, в соответствии с которыми оценивают значимость **риска** (2.1)

Примечание 1 – Критерии риска основываются на целях организации и **внешнем** (2.10) и **внутреннем контексте** (2.11).

Примечание 2 – Критерии риска могут быть установлены на основании стандартов, законов, стратегий и других требований.

[ISO Guide 73:2009, определение 3.3.1.3]

2.23 уровень риска (level of risk): Величина **риска** (2.1) или комбинации рисков, выраженная как сочетание **последствий** (2.18) и их **вероятности** (2.19)

[ISO Guide 73:2009, определение 3.6.1.8]

2.24 оценивание риска (risk evaluation): Процесс сравнения результатов **анализа риска** (2.21) с установленными **критериями риска** (2.22) для определения, является ли **риск** (2.1) и/или его величина приемлемыми или допустимыми

Примечание – Оценивание риска способствует принятию решения в отношении **обработки риска** (2.25).

[ISO Guide 73:2009, определение 3.7.1]

2.25 обработка риска (risk treatment): Процесс изменения **риска** (2.1)

Примечание 1 – Обработка риска может включать:

- предотвращение риска посредством принятия решения не начинать или не продолжать деятельность, в результате которой возникает риск;
- принятие риска или увеличение риска для достижения цели;
- устранение **источника риска** (2.16);
- изменение **вероятности** (2.19);
- изменение **последствий** (2.18);
- разделение риска с другой стороной или сторонами (включая контракты и финансирование риска); и
- принятие риска на основании обоснованного решения.

Примечание 2 – Обработка риска, имеющего отрицательные последствия, иногда упоминается как «снижение риска», «устранение риска», «предотвращение риска» и «уменьшение риска».

Примечание 3 – Обработка риска может создавать новые риски или изменять существующие риски.

[ISO Guide 73:2009, определение 3.8.1]

2.26 управление (control): Мера, которая меняет **риск** (2.1)

Примечание 1 – Управление включает любой процесс, политику, совет, практику или другие действия, которые изменяют риск.

Примечание 2 – Управление не всегда может вызывать установленный или предполагаемый результат изменения.

[Руководство ISO 73:2009, определение 3.8.1.1]

2.27 остаточный риск (residual risk): **Риск** (2.1), сохраняющийся после **обработки риска** (2.25)

Примечание 1 – Остаточный риск может содержать в себе неидентифицированный риск.

Примечание 2 – Остаточный риск может также называться как «принимаемый риск».

[ISO Guide 73:2009, определение 3.8.1.6]

2.28 мониторинг (monitoring): Постоянная проверка, контроль, наблюдение или определение состояния с целью идентификации изменения относительно требуемого или ожидаемого уровня

Примечание – Мониторинг можно применять к **структуре менеджмента риска** (2.3), **процессу менеджмента риска** (2.8), **рисуку** (2.1) или **управлению** (2.26).

[ISO Guide 73:2009, определение 3.8.2.1]

2.29 анализ (review): Деятельность, предпринимаемая для определения пригодности, адекватности и результативности предмета рассмотрения для достижения установленных целей

Примечание – Анализ можно применять к **структуре менеджмента риска** (2.3), **процессу менеджмента риска** (2.8), **рисуку** (2.1) или **управлению** (2.26).

[ISO Guide 73:2009, определение 3.8.2.2]

3 Принципы

Для эффективного менеджмента риска организация должна на всех уровнях соответствовать следующим принципам:

а) Менеджмент риска создает и обеспечивает ценность

Менеджмент риска обеспечивает достижение целей и улучшение деятельности, например, в целях обеспечения здоровья и безопасности людей, безопасности, соответствия законодательным требованиям, признания общественностью, охраны окружающей среды, качества продукции, управления проектом, результативности деятельности, управления и создания репутации.

b) Менеджмент риска является неотъемлемой частью всех организационных процессов

Менеджмент риска не является отдельным видом деятельности, отделенным от основной деятельности и процессов организации. Менеджмент риска – это часть обязательств руководства и неотъемлемая часть всех организационных процессов, включая стратегическое планирование, а также все процессы управления проектом и изменения.

c) Менеджмент риска является частью принятия решения

Менеджмент риска помогает лицам, принимающим решения, делать обоснованный выбор, определять приоритетность действий и определять различия между альтернативными планами действий.

d) Менеджмент риска подробно рассматривает неопределенность

Менеджмент риска детально рассматривает неопределенность, характер этой неопределенности и принимаемые меры.

e) Менеджмент риска является систематическим, структурированным и своевременным

Систематический, своевременный и структурированный подход к менеджменту риска способствует эффективности, а также получению непротиворечивых, сопоставимых и достоверных результатов.

f) Менеджмент риска основывается на соответствующей доступной информации

Входные данные для процесса менеджмента риска основываются на таких источниках информации, как статистические данные, опытные данные, обратная связь с заинтересованными сторонами, наблюдения, прогнозы и оценки экспертов. Однако, лица, принимающие решения, должны быть информированы и принимать во внимание любые ограничения данных или используемого моделирования, а также возможности расхождений среди экспертов.

g) Менеджмент риска является целенаправленным

Менеджмент риска должен соответствовать внешнему и внутреннему контексту и профилю риска.

h) Менеджмент риска учитывает человеческие и культурные факторы

Менеджмент риска учитывает возможности, восприятия и намерения людей за пределами и внутри организации, которые могут способствовать или затруднять достижение целей организации.

i) Менеджмент риска является прозрачным и всесторонним

Соответствующее и своевременное вовлечение заинтересованных сторон и, в частности, лиц, принимающих решение на всех уровнях организации, обеспечивает то, что менеджмент риска является обоснованным и своевременным. Участие этих сторон также позволяет учитывать их точки зрения при определении критериев риска.

j) Менеджмент риска является динамичным, повторяющимся и реагирующим на изменение

Менеджмент риска постоянно определяет и реагирует на изменение. Так как возникают внешние и внутренние события, изменяется контекст и знания, проводится мониторинг и анализ рисков, возникают новые риски, некоторые из них изменяются, а другие риски исчезают.

к) Менеджмент риска способствует постоянному улучшению организации

Организации должны разрабатывать и применять стратегии по улучшению менеджмента риска в дополнение ко всем другим аспектам организации.

Приложение А содержит рекомендации для организаций, стремящихся управлять риском эффективно.

4 Структура

4.1 Общие положения

Применение менеджмента риска будет зависеть от эффективности структуры менеджмента, обеспечивающей основу и меры, которые должны применяться в организации на всех уровнях. Структура способствует эффективному менеджменту риска посредством применения процесса менеджмента риском (см. раздел 5) на разных уровнях и в рамках конкретных контекстов организации. Структура гарантирует, что информация о риске, полученная в процессе менеджмента риска, соответствующим образом документируется и используется в качестве основы для принятия решений и отчетности на всех соответствующих уровнях организации.

В настоящем разделе представлены необходимые элементы структуры менеджмента риска, а также способ, обеспечивающий их взаимосвязь и повторение, как показано на рисунке 2.

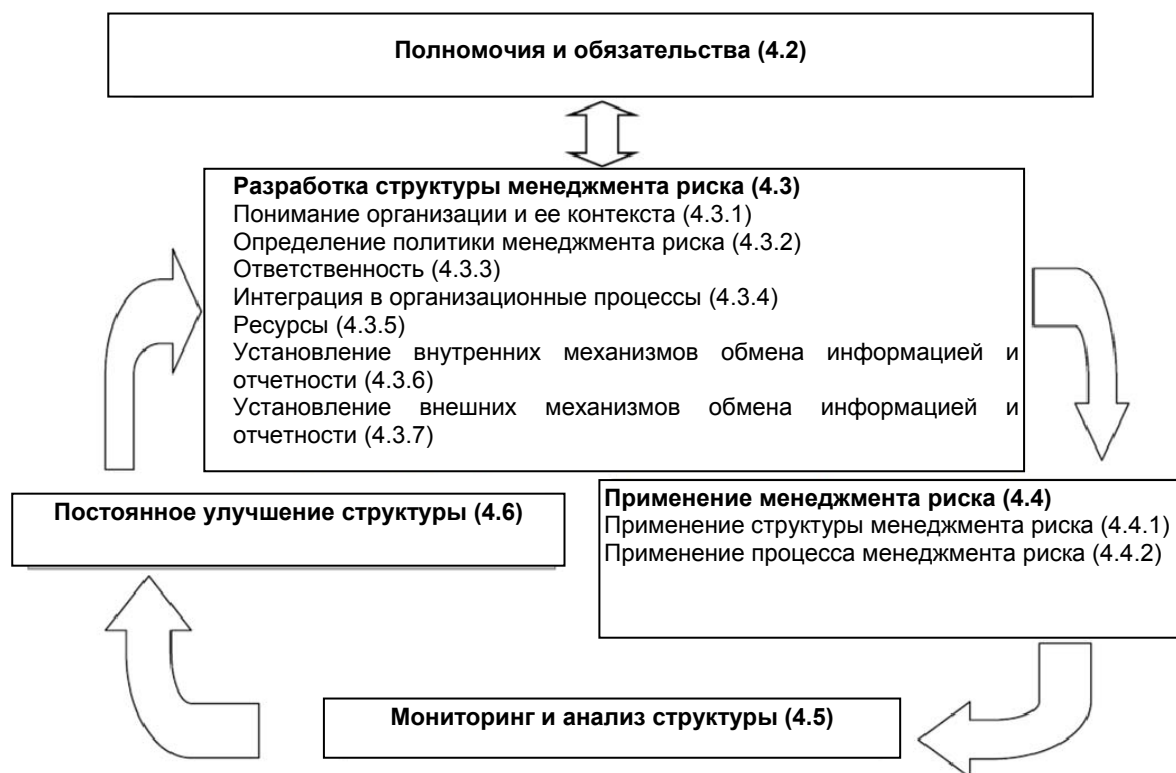


Рисунок 2 – Взаимосвязь между элементами структуры менеджмента риска

Данная структура предназначена не для создания системы менеджмента, а для помощи организации во внедрении менеджмента риска в общую систему менеджмента. Следовательно, организации должны адаптировать элементы структуры для своих конкретных потребностей.

Если процедуры и процессы менеджмента, существующие в организации, включают элементы менеджмента риска, или если организация уже внедрила процесс менеджмента риска для конкретных типов риска или ситуаций, то тогда их необходимо анализировать и оценивать в соответствии с настоящим стандартом, включая признаки, приведенные в приложении А, чтобы определить их адекватность и эффективность.

4.2 Полномочия и обязательства

Внедрение менеджмента риска и обеспечение его постоянной эффективности требует принятия строгого и постоянного обязательства со стороны руководства организации, а также стратегического и детального планирования для выполнения обязательств на всех уровнях. Руководство должно:

- определять и поддерживать политику менеджмента риска;
- обеспечивать согласованность деятельности организации и политики менеджмента риска;
- определять показатели эффективности менеджмента риска, которые согласуются с показателями эффективности организации;
- определять и согласовывать цели менеджмента риска с целями и стратегиями организации;
- обеспечивать соответствие обязательным требованиям;
- устанавливать ответственность и обязательства на соответствующих уровнях организации;
- обеспечивать распределение необходимых ресурсов для менеджмента риска;
- предоставлять информацию заинтересованным сторонам о преимуществах менеджмента риска; и
- обеспечивать постоянное соответствие структуры менеджмента риска.

4.3 Разработка структуры менеджмента риска

4.3.1 Понимание организации и ее контекста

Прежде чем приступить к проектированию и внедрению структуры менеджмента риска, важно оценить и определить как внешний, так и внутренний контекст организации, т.к. они могут значительным образом влиять на разработку структуры.

Оценивание внешнего контекста организации может включать:

- а) социальную, культурную, политическую, правовую, законодательную, финансовую, техноло-

гическую, экономическую, естественную и рыночную среду на международном, региональном, национальном или локальном уровнях;

б) основные движущие силы и направления, воздействующие на цели организации; и

с) взаимосвязи с внешними заинтересованными сторонами, восприятия и ценности.

Оценивание внутреннего контекста организации может включать:

- руководство, организационную структуру, роли и обязанности;
- политику, цели и стратегии, необходимые для достижения этих целей;
- потенциальные возможности, исходя из наличия ресурсов и знаний (например, капитала, времени, людей, процессов, систем и технологий);
- информационные системы, информационные потоки и процессы принятия решений (как официальные, так и неофициальные);
- взаимосвязи с внутренними заинтересованными сторонами, восприятия и ценности;
- деятельность организации;
- стандарты, руководства и модели, применяемые организацией; и
- форму и объем контрактных взаимоотношений.

4.3.2 Определение политики менеджмента риска

Политика менеджмента риска должна четко устанавливать цели организации и обязательства в отношении менеджмента риска и, как правило, рассматривать следующее:

- логическое обоснование организации менеджмента риска;
- связи между целями, политикой организации и политикой менеджмента риска;
- обязанности и обязательства в отношении менеджмента риска;
- области, имеющие противоречащие интересы;
- обязательство обеспечения необходимыми ресурсами;
- подходы для оценивания и документирования менеджмента риска; и
- обязательство анализировать и улучшать политику и структуру менеджмента риска периодически, а также в зависимости от событий или изменения обстоятельств.

Информация о политике менеджмента риска должна предоставляться соответствующим образом.

4.3.3 Ответственность

Организация должна обеспечивать наличие обязательств, полномочий и соответствующей компетентности для менеджмента риска, включая применение и поддержание процесса менеджмента риска и обеспечение адекватности, результативности и эффективности менеджмента. Этому может содействовать:

- установление владельцев риска, которые имеют обязательства и полномочия по управлению рисками;
- установление лица, ответственного за разработку, внедрение и поддержание структуры менеджмента риска;
- установление ответственности работников на всех уровнях организации за процесс менеджмента риска;
- установление показателей результативности, а также внешних и/или внутренних процессов отчетности и распространения; и
- обеспечение соответствующих уровней отчетности.

4.3.4 Интеграция в организационные процессы

Менеджмент риска необходимо включать во все процедуры и процессы организации таким образом, чтобы он осуществлялся соответствующим образом, эффективно и результативно. Процесс менеджмента риска должен стать частью организационных процессов и не должен отделяться от них. В частности, менеджмент риска следует включать в разработку политики, стратегическое планирование, планирование деятельности и анализ, а также в процессы изменения управления.

Должен быть разработан план менеджмента риска в масштабах организации, обеспечивающий применение политики менеджмента риска и включение менеджмента риска во все процедуры и процессы организации. План менеджмента риска может быть интегрирован в другие планы организации, например, в стратегический план.

4.3.5 Ресурсы

Организация должна распределять соответствующие ресурсы для менеджмента риска.

Необходимо рассматривать:

- людей, знания, опыт и компетентность;

- ресурсы, необходимые для каждого этапа процесса менеджмента риска;
- процессы, методы и инструменты организации, которые необходимо использовать для менеджмента риска;
- документированные процессы и процедуры;
- информацию и знания систем менеджмента; и
- программы обучения.

4.3.6 Установление внутренних механизмов обмена информацией и отчетности

Организация должна установить механизмы внутреннего обмена информацией и предоставления отчетов для обеспечения ответственности, а также обязательств по предоставлению отчетов о риске. Эти механизмы должны гарантировать, что:

- информация об основных элементах структуры менеджмента риска и любых последующих изменениях предоставляется соответствующим образом;
- осуществляется соответствующее внутренне доведение информации о структуре, ее эффективности и результатах;
- на соответствующих уровнях и своевременно предоставляется соответствующая информация, полученная при осуществлении менеджмента риска;
- существуют процессы консультирования с внутренними заинтересованными сторонами.

Эти механизмы должны, при необходимости, включать процессы сбора информации о риске из различных источников, а также необходимо рассмотреть степень конфиденциальности такой информации.

4.3.7 Установление внешних механизмов обмена информацией и отчетности

Организация должна разрабатывать и использовать план обмена информацией с внешними заинтересованными сторонами. Он должен включать:

- вовлечение соответствующих заинтересованных сторон и обеспечение эффективного обмена информацией;
- внешнюю отчетность, соответствующую законодательным, обязательным и руководящим требованиям;
- обеспечение обратной связи и отчетности об обмене информацией и консультациях;
- использование обмена информацией для обеспечения конфиденциальности в организации; и
- обмен информацией с заинтересованными сторонами в случае кризисной ситуации или непредвиденных обстоятельств.

Эти механизмы должны при необходимости включать процессы сбора информации о риске из разных источников, а также необходимо рассмотреть степень конфиденциальности такой информации.

4 Применение менеджмента риска

4.4.1 Применение структуры менеджмента риска

При применении организационной структуры менеджмента риска организация должна:

- определить соответствующие сроки и стратегию по применению структуры;
- применять политику и процесс менеджмента риска к организационным процессам;
- соответствовать законодательным и другим обязательным требованиям;
- гарантировать, что принятие решений, включая разработку и установление целей, согласовано с результатами процессов менеджмента риска;
- проводить информационные и обучающие собрания; и
- обмениваться информацией и консультироваться с заинтересованными сторонами для обеспечения того, что структура менеджмента риска остается соответствующей.

4.4.2 Применение процесса менеджмента риска

Процесс менеджмента риска, приведенный в разделе 5, обеспечивает менеджмент риска и применяется на основании плана менеджмента риска на всех соответствующих уровнях и для всех функций организации как часть ее процедур и процессов.

4.5 Мониторинг и анализ структуры

Чтобы гарантировать, что менеджмента риска является эффективным и продолжает соответствовать деятельности организации, организация должна осуществлять следующее:

- оценивать менеджмент риска на основании показателей, соответствие которых периодически

пересматривают;

- периодически оценивать выполнение плана менеджмента риска и отклонение от него;
- периодически анализировать структуру менеджмента риска, политику и план с учетом внутреннего и внешнего контекста организации;
- предоставлять информацию о риске, описывать выполнение плана менеджмента риска и политики менеджмента риска; и
- анализировать эффективность структуры менеджмента риска.

4.6 Постоянное улучшение структуры

Основываясь на результатах мониторинга и анализа, следует принимать решения в отношении того, как можно улучшить структуру менеджмента риска, политику и план. Эти решения должны приводить к улучшениям менеджмента риска и деятельности управлению риском.

5 Процесс

5.1 Общие положения

Процесс менеджмента риска должен быть:

- неотъемлемой частью менеджмента;
- встраиваться в деятельность и процедуры; и
- соответствовать бизнес-процессам организации.

Процесс включает деятельность, приведенную в 5.2 – 5.6. Процесс менеджмента риска показан на рисунке 3.

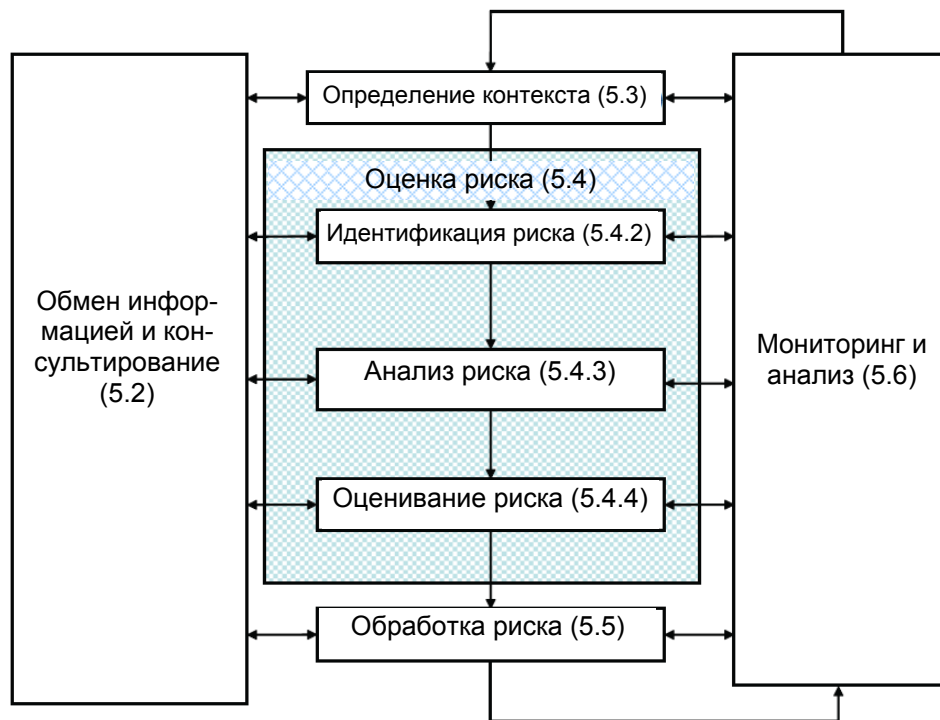


Рисунок 3 – Процесс менеджмента риска

5.2 Обмен информацией и консультирование

Обмен информацией и консультирование с внешними и внутренними заинтересованными сторонами осуществляются на всех этапах процесса менеджмента риска.

Поэтому планы по обмену информацией и консультированию должны разрабатываться на раннем этапе. Они должны рассматривать вопросы, касающиеся самого риска, его причин, его последствий (если известны) и мер, предпринимаемых для его обработки. Должен осуществляться эффективный внешний и внутренний обмен информацией и консультирование с тем, чтобы гарантировать, что лица, ответственные за реализацию процесса менеджмента риска и заинтересованные лица представляют, на каком основании принимаются решения, и осознают причины того, почему требуются конкретные действия.

Подход, касающийся консультативной группы, может:

- помочь соответствующим образом установить контекст;

- гарантировать, что интересы заинтересованных сторон осознаются и рассматриваются;
- обеспечивать идентификацию рисков соответствующим образом;
- соединять вместе различные области оценки для анализа рисков;
- обеспечивать рассмотрение должным образом различных точек зрения при определении критериев риска и при оценивании рисков;
- обеспечивать утверждение и обоснование плана обработки риска;
- усовершенствовать соответствующее управление изменениями во время процесса менеджмента риска; и
- разрабатывать соответствующий внешний и внутренний обмен информацией и план консультирования.

Обмен информацией и консультирование с заинтересованными сторонами является важным аспектом, так как выводы о риске основываются на восприятии риска заинтересованными сторонами. Эти восприятия могут различаться вследствие различий в ценностях, потребностях, предположениях, концепциях и интересах заинтересованных сторон. Так как точки зрения могут иметь существенное влияние на принимаемые решения, то восприятия заинтересованных сторон необходимо идентифицировать, документировать и учитывать в процессе принятия решений.

Обмен информацией и консультирование должны обеспечивать соответствующий, точно определенный и доступный обмен информацией с учетом аспектов конфиденциальности и сохранности.

5.3 Определение контекста

5.3.1 Общие положения

Посредством установления контекста организация формулирует свои цели, определяет внешние и внутренние параметры, которые следует принимать во внимание при осуществлении менеджмента риска, а также определяет область применения и критерии риска для процесса. Поскольку многие эти параметры аналогичны тем, которые рассматриваются при разработке структуры менеджмента риска (см. 4.3.1), при определении контекста процесса менеджмента риска, их следует рассматривать более подробно и, в частности, то, как они связаны с областью применения конкретного процесса менеджмента риска.

5.3.2 Установление внешнего контекста

Внешний контекст – это внешняя среда, в которой организация стремится достигать свои цели.

Понимание внешнего контекста является важным, чтобы гарантировать, что цели и интересы внешних заинтересованных сторон рассматриваются при разработке критериев риска. Он основывается на контексте всей организации, но с конкретными подробностями законодательных и обязательных требований, восприятиями заинтересованных сторон и другими аспектами рисков, характерными для области применения процесса менеджмента риска.

Внешний контекст может включать:

- социальную, культурную, политическую, правовую, законодательную, финансовую, технологическую, экономическую, естественную и рыночную среду на международном, региональном, национальном или локальном уровне;
- основные факторы и тенденции, влияющие на цели организации; и
- взаимосвязи с внешними заинтересованными сторонами, их восприятия и ценности.

5.3.3 Установление внутреннего контекста

Внутренний контекст – это внутренняя среда, в которой организация стремится достигать свои цели.

Процесс менеджмента риска должен соответствовать деятельности, процессам, структуре и стратегии организации. Внутренний контекст – это что-либо в масштабе организации, что может влиять на способ, которым организация будет осуществлять менеджмента риска. Его необходимо определить, потому что:

- а) менеджмент риска имеет место в контексте целей организации;
- б) цели и критерии конкретного проекта, процесса или деятельности следует рассматривать, принимая во внимание цели организации в целом; и
- в) некоторые организации не устанавливают возможности достижения своих стратегических, проектных или экономических целей, и это влияет на обязательства организации, надежность, доверие и ценность.

Необходимо понимать внутренний контекст. Он может включать:

- руководство, организационную структуру, функции и обязательства;
- политику, цели и стратегии, имеющиеся для достижения этих целей;
- возможности, исходя из ресурсов и знаний (например, капитал, время, люди, процессы, сис-

темы и технологии);

- взаимосвязи с внутренними заинтересованными сторонами, их восприятия и ценности;
- деятельность организации;
- информационные системы, информационные потоки и процессы принятия решений (как официальные, так и неофициальные);
- стандарты, руководства и модели, принятые организацией; и
- форму и объем контрактных взаимоотношений.

5.3.4 Установление контекста процесса менеджмента риска

Необходимо устанавливать цели, стратегии, область применения и параметры деятельности организации или тех ее частей, где применяется процесс менеджмента риска. Менеджмент риска следует предпринимать с полным рассмотрением необходимости обоснования ресурсов, используемых при осуществлении менеджмента риска. Следует также определять требуемые ресурсы, ответственность и полномочия, а также сохраняемые записи.

Контекст процесса менеджмента риска изменяется в зависимости от потребностей организации. Он может включать:

- определение задач и целей менеджмента риска;
- определение ответственности за процесс менеджмента риска и в рамках этого процесса;
- определение области применения, а также границ менеджмента риска, включая отдельные дополнения и ограничения;
- определение деятельности, процесса, функции, проекта, продукции, услуги или актива, исходя из времени и расположения;
- определение взаимосвязей между конкретным проектом, процессом или деятельностью и другими проектами, процессами или видами деятельности организации;
- определение методологии оценки риска;
- определение способа оценки показателей и эффективности менеджмента риска;
- установление и определение решений, которые необходимо принять; и
- определение, анализ и обозначение границ необходимых исследований, их объемов и целей, а также ресурсов, требуемых для таких исследований.

Рассмотрение данных и других значимых факторов, должно способствовать обеспечению того, что принятый подход менеджмента риска соответствует обстоятельствам, организации и рискам, влияющим на достижение ее целей.

5.3.5 Определение критериев риска

Организация должна определять критерии, которые необходимо использовать для оценки значимости риска. Критерии должны отражать ценности, цели и ресурсы организации. Некоторые критерии могут устанавливаться на основе законодательных и обязательных требований, а также других требований, которые взяла на себя организация. Критерии риска должны быть согласованы с политикой менеджмента риска организации (см. 4.3.2), определены в начале любого процесса менеджмента риска и должны подвергаться постоянному анализу.

При определении критериев риска необходимо рассматривать следующие факторы:

- характер и типы причин и последствий, которые могут возникать, и то, как их следует измерять;
- как следует определять вероятность;
- временные рамки вероятности и/или последствия(ий);
- как должен быть определен уровень риска;
- мнения заинтересованных сторон;
- уровень, на котором риск становится приемлемым или допустимым; и
- принимать ли во внимание комбинации нескольких рисков и, если да, то, каким образом и какие комбинации следует рассматривать.

5.4 Оценка риска

5.4.1 Общие положения

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

Примечание – ISO/IEC 31010 содержит руководство по методам оценки.

5.4.2 Идентификация риска

Организация должна идентифицировать источники риска, области воздействия, события (включая изменения в обстоятельствах) и их причины, а также их потенциальные последствия. Цель данного этапа заключается в составлении подробного перечня рисков, основанного на тех событиях, которые могут создавать, повышать, предотвращать, снижать, ускорять или замедлять достижение целей. Важно идентифицировать риски, связанные с отклонением от благоприятного события. Полная идентификация является важной, так как риск, который не был идентифицирован на данном этапе, не будет включен в дальнейший анализ.

Идентификация должна включать риски независимо от того, контролирует ли организация его источник или нет, даже если источник риска или его причина могут быть не очевидны. Идентификация риска должна включать исследование воздействий конкретных последствий, включая каскадные и кумулятивные эффекты. Также необходимо рассматривать широкий спектр последствий, даже если источник риска или его причина могут быть не очевидны. Наряду с идентификацией событий, которые могут произойти, необходимо рассматривать возможные причины и сценарии, которые показывают, какие последствия могут происходить. Следует рассматривать все значимые причины и последствия.

Организация должна применять инструменты и методики идентификации риска, которые подходят для ее целей и возможностей, а также соответствуют рискам, с которыми она сталкивается. При идентификации рисков большое значение имеет соответствующая и актуализированная информация. При необходимости она должна включать соответствующую дополнительную информацию. Для идентификации рисков должны привлекаться люди с соответствующими знаниями.

5.4.3 Анализ риска

Анализ риска обеспечивает понимание риска. Анализ риска предоставляет входные данные для оценивания риска и принятия решений, относительно обработки рисков, а также для выбора стратегий и методов наиболее подходящей обработки рисков. Анализ риска может также предоставлять входные данные для принятия решений, когда требуется сделать выбор, а варианты включают различные типы и уровни риска.

Анализ риска включает рассмотрение причин и источников риска, их положительных и отрицательных последствий и вероятности того, что эти последствия могут произойти. Следует идентифицировать факторы, влияющие на последствия и вероятность их возникновения. Риск анализируют посредством определения последствий и вероятности их возникновения, а также других признаков риска. Событие может иметь различные последствия и может воздействовать на различные цели. Во внимание также следует принимать существующие средства управления, их результативность и эффективность.

Способ, которым выражают последствия и вероятность их возникновения, и способ их объединения с целью определения уровня риска, должны отражать тип риска, имеющуюся информацию и цель, для которой результат оценки риска должен использоваться. Все это должно соответствовать критериями риска. Важно также рассматривать взаимозависимость различных рисков и их источников.

При анализе рассматривают достоверность определения уровня риска и его чувствительность к предположениям и допущениям, а также доводят информацию до лиц, принимающих решения, и при необходимости других заинтересованных сторон. Необходимо установить и выделить такие факторы, как наличие разных точек зрения среди экспертов, неопределенность, доступность, качество, количество и актуальность информации, а также ограничения моделирования.

Анализ риска может осуществляться с различной степенью детальности анализа, в зависимости от риска, цели анализа и информации, данных и имеющихся ресурсов. Анализ может быть качественным, полуколичественным или количественным, либо их комбинацией в зависимости от обстоятельств.

Последствия и вероятность их возникновения можно определять посредством моделирования результатов события или ряда событий, или на основе экстраполяции экспериментальных исследований или имеющихся данных. Последствия могут быть выражены в виде материальных или нематериальных воздействий. В некоторых случаях требуется несколько численных значений или признаков для определения последствий и вероятности их возникновения для различных сроков, мест, групп или ситуаций.

5.4.4 Оценивание риска

Целью оценивания риска является содействие принятию решений, основанных на результатах анализа риска, относительно необходимости обработки рисков и установления приоритета осуществления обработки риска.

Оценивание риска включает сравнение уровня риска, выявленного в процессе анализа, с кри-

териями риска, установленными при рассмотрении контекста. На основании этого сравнения определяется необходимость обработки риска.

При принятии решений следует учитывать более широкий контекст риска и включать рассмотрение допустимых рисков, принимаемых сторонами, за исключением организации, которая извлекает выгоду из риска. Решения должны быть приняты в соответствии с законодательными, обязательными и другими требованиями.

При некоторых обстоятельствах оценивание риска приводит к решению о проведении дополнительного анализа. Оценивание риска также может привести к решению не обрабатывать риск каким-либо образом, за исключением применения средств управления. На это решение влияет отношение организации к риску и установленные критерии риска.

5.5 Обработка риска

5.5.1 Общие положения

Обработка риска включает выбор одного или нескольких вариантов изменения рисков и применение этих вариантов. Меры обработки обеспечивают применение средств управления или меняют средства управления.

Обработка риска включает циклический процесс:

- оценивания обработки риска;
- принятия решения, являются ли уровни остаточного риска допустимыми;
- проведение новой обработки риска, если уровни остаточного риска не допустимы; и
- оценивание результативности этой обработки.

Варианты обработки риска не обязательно могут быть взаимоисключающими или быть подходящими для всех обстоятельств. Варианты могут включать:

- a) предотвращение риска посредством принятия решения не начинать или не продолжать деятельность, в результате которой возникает риск;
- b) принятие или увеличение риска для достижения цели;
- c) устранение источника риска;
- d) изменение вероятности;
- e) изменение последствий;
- f) разделение риска с другой стороной или сторонами (включая контракты и финансирование риска); и
- g) принятие риска на основании обоснованного решения.

5.5.2 Выбор вариантов обработки риска

Выбор наиболее подходящего варианта обработки риска включает сопоставление затрат и усилий по реализации с извлекаемыми преимуществами с учетом законодательных, обязательных и других требований, таких как социальная ответственность и защита окружающей среды. При принятии решения следует принимать во внимание риски, которые требуют обработки риска, не обоснованной с экономической точки зрения, например, риски серьезные (значительные отрицательные последствия), но редкие (с низкой вероятностью возникновения).

Варианты обработки можно рассматривать и применять либо по отдельности, либо в комбинации. Организация обычно может извлекать преимущества от принятия комбинации вариантов обработки.

При выборе вариантов обработки риска организация должна рассматривать интересы и восприятия заинтересованных сторон и наиболее подходящие способы обмена информацией с ними. Если варианты обработки риска могут воздействовать на риск где-либо еще в организации, или в отношении заинтересованных сторон, то при принятии решения это следует учитывать. Несмотря на одинаковую эффективность, некоторые варианты обработки риска для одних заинтересованных сторон могут быть более приемлемыми, чем для других.

План обработки риска должен четко определять порядок, в соответствии с которым должны применяться отдельные варианты обработки риска.

Сама по себе обработка риска может вызывать риски. Существенным риском может быть отсутствие или неэффективность мер обработки риска. Мониторинг должен быть неотъемлемой частью плана обработки риска, чтобы гарантировать, что меры остаются эффективными.

Обработка риска может также вызывать вторичные риски, которые необходимо оценивать, обрабатывать, контролировать и анализировать. Эти вторичные риски должны включаться в тот же план обработки, что и первоначальный риск, и не рассматриваться как новый риск. Необходимо идентифицировать и поддерживать связь между двумя рисками.

5.5.3 Подготовка и реализация планов обработки риска

Целью планов обработки риска является документирование того, как должны реализовываться выбранные варианты обработки. Информация, представленная в планах обработки рисков, должна включать:

- основания для выбора вариантов обработки риска, включая ожидаемые преимущества, которые будут получены;
- лиц, отвечающих за утверждение плана, а также лиц, ответственных за реализацию плана;
- предлагаемые действия;
- требования к ресурсам, включая возможные непредвиденные обстоятельства;
- показатели выполнения и ограничения;
- требования к отчетности и мониторингу; и
- сроки и график выполнения.

Планы обработки рисков должны быть объединены с процессами менеджмента организации и должны обсуждаться с соответствующими заинтересованными сторонами.

Лица, принимающие решения, и другие заинтересованные стороны должны быть осведомлены о характере и степени остаточного риска после обработки риска. Остаточный риск должен быть документально оформлен и должен подвергаться мониторингу, анализу и, при необходимости, дополнительной обработке.

5.6 Мониторинг и анализ

Мониторинг и анализ должны быть планируемой частью процесса менеджмента риска и включать регулярную проверку или контроль. Они могут быть периодическими или специальными.

Должна быть четко определена ответственность за мониторинг и анализ.

Процессы мониторинга и анализа, осуществляемые организацией, должны включать все аспекты процесса менеджмента риска в целях:

- обеспечения того, что средства контроля являются эффективными и результативными как для проектирования, так и для функционирования;
- получения дополнительной информации для улучшения оценки риска;
- анализа и изучения событий (включая инциденты без последствий), изменений, основных направлений развития, успехов и неудач;
- выявления изменений во внешнем и внутреннем контексте, включая изменения критериев риска, а также риска, который может потребовать пересмотра обработок риска и приоритетов; и
- идентификации возникающих рисков.

Выполнение планов обработки рисков определяет оценку деятельности. Результаты могут быть включены в общий менеджмент организации, оценку, а также деятельность по предоставлению внешней и внутренней информации.

Результаты мониторинга и анализа должны быть документально оформлены и, при необходимости, доведены до сведения на внешнем и внутреннем уровнях, а также должны использоваться в качестве входных данных для пересмотра структуры менеджмента риска (см. 4.5).

5.7 Документирование процесса менеджмента риска

Деятельность по менеджменту риска должна быть прослеживаемой. В процессе менеджмента риска записи обеспечивают основу для улучшения методов и инструментов, а также всего процесса.

При принятии решений о ведении записей необходимо принимать во внимание следующее:

- потребности организации в постоянном накоплении знаний;
- преимущества повторного использования информации в целях управления;
- затраты и усилия, включенные в создание и поддержание записей;
- законодательные, обязательные требования, а также потребности, связанные с особенностями деятельности, относящиеся к записям;
- метод доступа, простота восстановления и носители информации;
- срок хранения; и
- конфиденциальность информации.

Приложение А (справочное)

Признаки усовершенствованного менеджмента риска

А.1 Общие положения

Все организации должны стремиться достичь соответствующего уровня функционирования их структуры менеджмента риска в соответствии с важностью решений, которые должны быть приняты. Перечень признаков, приведенный ниже, представляет обобщенный уровень менеджмента риска. Чтобы помочь организациям в оценке их деятельности в соответствии с критериями для каждого признака, предоставляется несколько показателей.

А.2 Основные результаты

А.2.1 Организация имеет современное, правильное и всестороннее понимание своих рисков.

А.2.2 Риски организации находятся в пределах критериев риска.

А.3 Признаки

А.3.1 Постоянное улучшение

Акцент делают на постоянное улучшение менеджмента риска через установление целей деятельности организации, измерение, анализ и последующее изменение процессов, систем, ресурсов, возможностей и навыков.

Это может подтверждаться наличием определенных целей деятельности, согласно которым оценивают деятельность организации и каждого отдельного менеджера. Результаты деятельности могут быть опубликованы и доведены до сведения. Обычно проводят, как минимум, годовой анализ деятельности, а затем анализ процессов, а также установление пересмотренных целей деятельности на следующий период.

Такая оценка менеджмента риска является неотъемлемой частью оценки всей деятельности организации и системы оценки работы отделов и отдельных работников.

А.3.2 Полная ответственность за осуществление менеджмента риска

Усовершенствованный менеджмент риска включает всестороннюю, полностью определенную и принятую ответственность за риски, управление и задачи обработки риска. Назначенные отдельные работники, обладающие соответствующими навыками и имеющие надлежащие ресурсы, берут на себя полную ответственность перед внешними и внутренними заинтересованными сторонами за проверку средств управления, контроль за рисками, усовершенствование средств управления и эффективный обмен информацией о рисках, а также менеджмент риска.

Это могут подтвердить все члены организации, которые должны быть осведомлены в полном объеме о рисках, средствах управления и задачах, за которые они несут ответственность. Обычно, это должно быть записано в должностных инструкциях, содержаться в базах данных или информационных системах. Распределение функций при осуществлении менеджмента риска, ответственности и обязательств должно быть частью всех применяемых программ организации.

Организация должна обеспечивать ответственных лиц всем необходимым для выполнения своей функции, а также предоставлять им полномочия, время, обучение, ресурсы и навыки, достаточные для выполнения своих обязательств.

А.3.3 Применение менеджмента риска при принятии всех решений

Все принимаемые в организации решения, независимо от уровня важности и значимости, включают в себя рассмотрение рисков и применение менеджмента риска в определенной степени.

Это может быть указано в документах заседаний и решениях, подтверждающих, что подробные обсуждения рисков имели место. Кроме того, должна обеспечиваться возможность видеть, что все элементы менеджмента риска представлены в основных процессах принятия решений, осуществляемых в организации, например, решения по распределению капитала, основным проектам, а также реструктуризации и организационных изменениях. По этим причинам всесторонне обоснованный менеджмент риска должен прослеживаться в масштабах организации и обеспечивать основу для эффективного управления.

А.3.4 Постоянный обмен информацией

Усовершенствованный менеджмент риска включает постоянный обмен информацией с внешними и внутренними заинтересованными сторонами, включая всестороннее и периодическое представление информации о применении менеджмента риска, как части надлежащего управления.

Это может подтверждаться обменом информацией с заинтересованными сторонами как неотъемлемым и важным элементом менеджмента риска. Обмен информацией правильно рассматривать как двусторонний процесс, обеспечивающий, чтобы обоснованные решения принимались в отношении уровня рисков и необходимости обработки рисков в соответствии с установленными всесторонними критериями риска.

Всестороннее и периодическое внешнее и внутреннее представление информации о существенных рисках и о применении менеджмента риска способствует в значительной степени эффективному управлению в масштабах организации.

А.3.5 Полная интеграция в структуру управления организации

Менеджмент риска рассматривается как центральный процесс управления, в котором риски рассматриваются с точки зрения влияния на неопределенность в отношении целей. Структура и процесс управления основываются на менеджменте риска. Руководители рассматривают эффективный менеджмент риска как важный аспект для достижения целей организации.

Это может подтверждаться применением руководителями термина «неопределенность» в отношении рисков, а также использованием термина в важных письменных материалах организации. Этот признак также обычно отражается в заявлениях организации, касающихся политики, в частности, той, которая относится к менеджменту риска. Как правило, этот признак должен подтверждаться посредством проведения интервью с руководителями, а также через подтверждение их действий и заявлений.

Библиография

ISO Guide 73:2009

Risk management – Vocabulary
(Менеджмент риска. Словарь)

ISO/IEC 31010:2009

Risk management – Risk assessment techniques
(Менеджмент рисков. Методики оценки риска)

Приложение Д.А
(справочное)**Сведения о соответствии государственных стандартов ссылочным международным стандартам****Таблица Д.А.1 – Сведения о соответствии государственных стандартов ссылочным международным стандартам другого года издания**

Обозначение и наименование ссылочного международного стандарта	Обозначение и наименование международного стандарта другого года издания	Степень соответствия	Обозначение и наименование государственного стандарта
ISO Guide 73:2009 Менеджмент риска. Словарь	ISO/IEC Guide 73:2002 Менеджмент рисков. Словарь. Руководящие указания по применению в стандартах	IDT	СТБ ИСО/МЭК Руководство 73-2005 Менеджмент риска. Термины и определения (ISO/IEC Guide 73:2002, IDT)

Заместитель директора БелГИСС
по подтверждению соответствия

И. И. Осмола

Начальник ТО-10

А. А. Поживилко

Инженер 1-й категории ТО-10

Ю. Г. Боровец