Утвержден и введен в действие
Приказом Федерального
агентства по техническому
регулированию и метрологии
от 21 декабря 2010 г. N 883-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ РИСКА

ПРИНЦИПЫ И РУКОВОДСТВО

Risk management. Principles and guidelines

ISO 31000:2009
Risk management - Principles and guidelines
(IDT)

ГОСТ Р ИСО 31000-2010

Группа Т58

ОКС 03.100.01

Дата введения
1 сентября 2011 года

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения".

Сведения о стандарте

1 ПОДГОТОВЛЕН Научно-техническим центром "ИНТЕК" на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 100 "Стратегический и инновационный менеджмент"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 21 декабря 2010 г. N 883-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 31000:2009 "Менеджмент риска. Принципы и руководство" (ISO 31000:2009 "Risk management - Principles and guidelines")

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и

поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "Национальные стандарты". Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Введение

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

Вся деятельность организации включает в себя риск. Организации осуществляют риск-менеджмент посредством его идентификации, его анализа и последующего оценивания, будет ли риск изменен воздействием, чтобы соответствовать установленным критериям риска. На протяжении всего этого процесса они обмениваются информацией и консультируются с заинтересованными сторонами, а также наблюдают и анализируют риск и действия по управлению, которые изменяют риск для гарантии того, что какого-либо воздействия на риск 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 эффективным. Настоящий стандарт рекомендует, чтобы организации разрабатывали, внедряли и постоянно улучшали инфраструктуру, цель которой заключается в интегрировании процесса менеджмента риска в общее управление, стратегию и планирование, менеджмент, процессы отчетности, политику, ценности и культуру.

Менеджмент риска <1> может применяться ко всей организации в любое время в ее многих областях и на многих уровнях, а также к особым функциям, проектам и видам деятельности.

<1> В силу этого во многих областях установилась различная словоупотребительная практика в отношении понятия "менеджмент риска". Поэтому очень часто в научно-технической литературе встречается словосочетание "риск-менеджмент". Далее по тексту стандарта, где это уместно, а также для простоты данное словосочетание используется наряду с общепринятым.

Несмотря на непрерывное развитие практики менеджмента во многих отраслях с целью соответствия различным потребностям, внедрение постоянных процессов в рамках общей инфраструктуры может способствовать эффективному и результативному управлению рисками во всей организации. Обобщенный подход, описанный в настоящем стандарте, устанавливает принципы и руководства управления рисками любой формы системным, прозрачным и надежным образом и в рамках любой области и содержания.

Каждая конкретная отрасль или сфера применения риск-менеджмента имеет свои отдельные потребности, потребителей, восприятия и критерии. Поэтому основной особенностью настоящего стандарта является включение "определения ситуации (контекста)" как деятельности, проводимой в начале общего процесса риск-менеджмента. При определении ситуации (контекста) необходимо рассматривать цели организации, окружающую среду, в которой эти цели достигаются, заинтересованные стороны и разнообразие критериев риска, все то, что помогает выявлять и оценивать характер и сложность этих рисков.

На рисунке 1 показаны взаимосвязи принципов менеджмента риска, инфраструктуры и процессов менеджмента риска, описанных в настоящем стандарте.

При применении и поддержании в соответствии с настоящим стандартом риск-менеджмент дает возможность организации:

- повышать возможность достижения целей;

- поддерживать активный менеджмент;

- осознавать необходимость идентификации и воздействия на риски по всей организации;

- улучшать идентификацию возможностей и угроз;

- отвечать соответствующим законодательным и другим обязательным требованиям и международным нормам;

- улучшать обязательную и управленческую отчетность;

- улучшать управление;

- укреплять доверие заинтересованных сторон;

- создавать надежный базис для принятия решений и планирования;

- совершенствовать управление;

- эффективно распределять и использовать ресурсы для воздействия на риск;

- повышать функциональную эффективность и результативность;

- повышать уровень обеспечения безопасности, здоровья, а также защиты окружающей среды;

- совершенствовать предотвращение потерь и менеджмент инцидентов;

- сводить к минимуму потери;

- улучшать обучение в организации;

- повышать устойчивость организации.

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

a) лиц, ответственных за разработку политики управления рисками внутри организации;

b) лиц, ответственных за обеспечение эффективности управления рисками в рамках организации в целом или в рамках конкретной области, проекта или деятельности;

c) лиц, которым необходимо оценивать эффективность организации по управлению рисками;

d) разработчиков стандартов, руководств, процедур и добросовестных практик, которые в целом или частично устанавливают, как осуществлять риск-менеджмент в рамках конкретных

ситуаций в этих документах.

Современные практики и процессы управления многих организаций включают компоненты риск-менеджмента, а многие организации уже используют формальный процесс риск-менеджмента для конкретных типов риска или обстоятельств. В этих случаях организация может принять решение о проведении критического обзора используемых ею практик и процессов в свете настоящего стандарта.

В настоящем стандарте используются оба выражения: как термин "менеджмент риска ("risk management")", так и термин "управление риском" ("managing risk"). В общих чертах "менеджмент риска" относится к архитектуре (принципам, инфраструктуре и процессу) эффективного управления рисками, в то время как "управление рисками" относится к применению этой архитектуры к конкретным рискам.

Международный стандарт был подготовлен рабочей группой по риск-менеджменту Технического управляющего бюро ИСО (ТМВ).

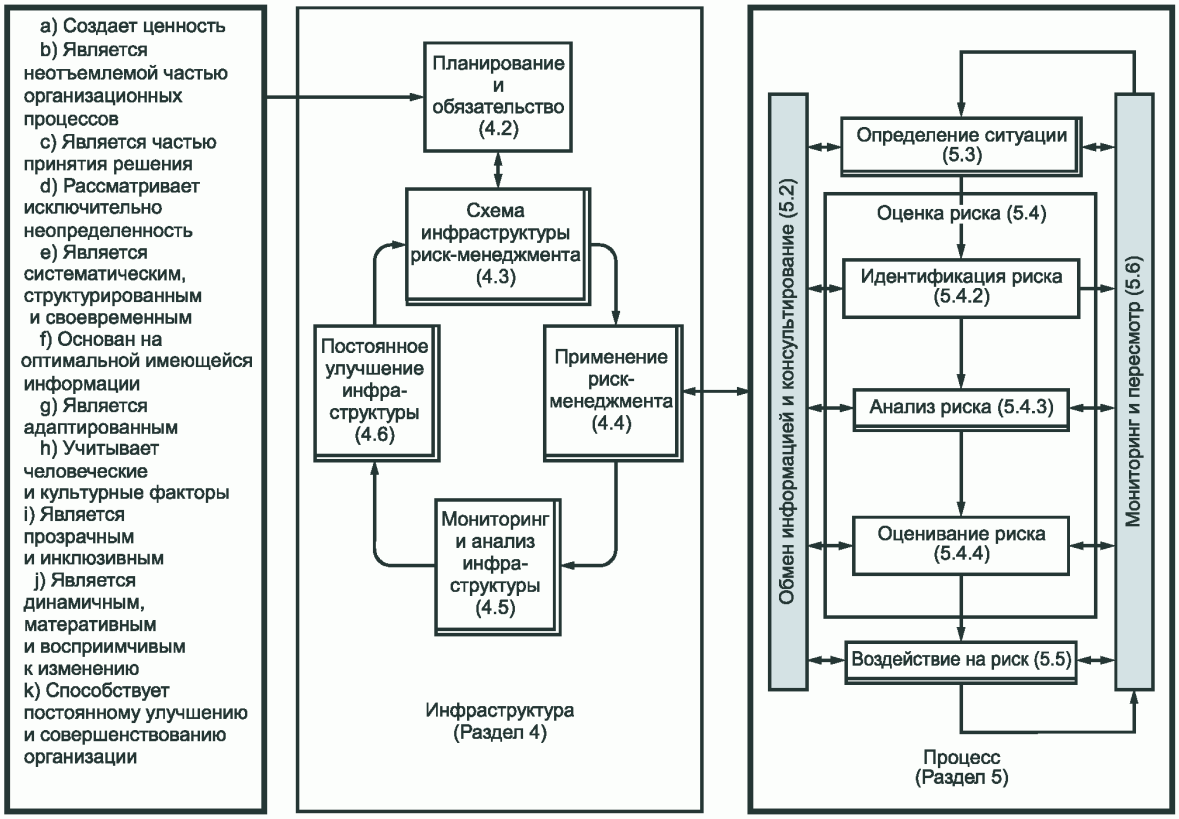

Рисунок 1 - Взаимосвязи между принципами, инфраструктурой и процессом менеджмента риска

1 Область применения

Настоящий стандарт устанавливает принципы и общее руководство по риск-менеджменту.

Настоящий стандарт может использовать любое государственное, частное или общественное предприятие, ассоциация, группа лиц или отдельное лицо. Этот стандарт не

является специфическим для какой-либо промышленности или отрасли.

Примечание - Всех различных пользователей настоящего стандарта называют для удобства общим термином "организация".

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

Настоящий стандарт может применяться к любому типу риска, независимо от его характера, а также того, имеет ли он отрицательные или положительные последствия.

Несмотря на то что настоящий стандарт предоставляет обобщенное руководство, он не предназначен для обеспечения единообразия риск-менеджмента во всех организациях. При создании и применении планов, касающихся инфраструктуры риск-менеджмента, необходимо учитывать различные потребности конкретной организации, ее частные цели, ситуацию (контекст), структуру, операции, процессы, функции, проекты, продукты, услуги или активы, а также конкретную практику, принятую в организации.

Это следует понимать в том смысле, что настоящий стандарт необходимо использовать для гармонизации процессов управления риском, описанных в существующих действующих и будущих стандартах. Он устанавливает общий подход для поддержки стандартов, распространяющихся на конкретные риски и/или отрасли, и не заменяет эти стандарты.

Настоящий стандарт не предназначен для целей сертификации.

2 Термины и определения

В настоящем стандарте применяют следующие термины с соответствующими определениями:

2.1 **риск** (risk): Влияние неопределенности на цели.

Примечание 1 - Влияние - это отклонение от того, что ожидается (положительное и/или отрицательное).

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

Примечание 3 - Риск часто характеризуется ссылкой на потенциально возможные **события** (2.17) и **последствия** (2.18) или их комбинации.

Примечание 4 - Риск часто выражают в виде комбинации последствий событий (включая изменения в обстоятельствах) и связанной с этим вероятности или возможности наступления (2.19).

Примечание 5 - Неопределенность - это состояние, заключающееся в недостаточности, даже частичной, информации, понимания или знания относительно события, его последствий или его возможности.

[Руководство ИСО 73:2009, определение 1.1]

2.2 **менеджмент риска, риск-менеджмент** (risk management): Скоординированные действия по управлению организацией с учетом **риска** (2.1).

[Руководство ИСО 73:2009, определение 2.1]

2.3 **инфраструктура менеджмента риска** (risk management framework): Набор компонентов, обеспечивающих основы и организационные меры и структуру для разработки, внедрения, **мониторинга** (2.28), пересмотра и постоянного улучшения **менеджмента риска** (2.2) в масштабе всей организации.

Примечание 1 - Основы включают политику, цели, полномочия и обязательства по управлению риском (2.1).

Примечание 2 - Организационные меры и структура включают планы, взаимосвязи, ответственность, ресурсы, процессы и деятельность.

Примечание 3 - Инфраструктура менеджмента риска встроена во все стратегические и операционные политики и практики организации.

[Руководство ИСО 73:2009, определение 2.1.1]

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

[Руководство ИСО 73:2009, определение 2.1.2]

2.5 **отношение к риску** (risk attitude): Подход организации к оценке и в конечном счете к использованию благоприятных возможностей, удержанию, принятию или недопущению **риска** (2.1).

[Руководство ИСО 73:2009, определение 3.7.1.1]

2.6 **план менеджмента риска** (risk management plan): Документ **в инфраструктуре менеджмента риска** (2.3), определяющий подход, элементы управления и ресурсы, используемые при менеджменте риска (2.1).

Примечание 1 - Элементы менеджмента риска обычно включают процедуры, практики, распределение обязанностей и ответственности, последовательность и время деятельности.

Примечание 2 - План менеджмента риска может применяться для конкретного продукта, процесса и проекта, а также к части или ко всей организации.

[Руководство ИСО 73:2009, определение 2.1.3]

2.7 **владелец риска** (risk owner): Лицо или организационная единица, которые имеют полномочия и несут ответственность за управление **рисками** (2.1).

[Руководство ИСО 73:2009, определение 3.5.1.5]

2.8 **процесс менеджмента риска** (risk management process): Систематическое применение политик, процедур и практик менеджмента к деятельности по обмену информацией, консультированию, установлению ситуации (контекста) и идентификации, анализу, оцениванию, воздействию на риск, мониторингу (2.28) и пересмотру **риска** (2.1).

[Руководство ИСО 73:2009, определение 3.1]

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

менеджмента рисков (2.4).

[Руководство ИСО 73:2009, определение 3.3.1]

2.10 **внешняя ситуация (контекст)** (external context): Внешняя среда, в которой организации стремятся к достижению своих целей.

Примечание - Внешняя ситуация **(контекст)** может включать:

- культурную, социальную, правовую, регулирующую, финансовую, технологическую, экономическую, естественную и рыночную среду на международном, национальном, региональном или на местном уровне;
- основные движущие силы и тенденции, влияющие на цели организации;
- взаимосвязи с **заинтересованными сторонами** (2.13), их ожидания и ценности.

[Руководство ИСО 73:2009, определение 3.3.1.1]

2.11 **внутренняя ситуация (контекст)** (internal context): Внутренняя среда, в которой организация стремится к достижению своих целей.

Примечание - Внутренняя ситуация **(контекст)** может включать:

- руководство, организационную структуру, роли и ответственности;
- политики, цели и стратегии, доступные с точки зрения их достижения;
- возможности, понимаемые в отношении ресурсов и знания (например, капитал, время, люди, процессы, системы и технологии);
- информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);
- взаимосвязи с внутренними заинтересованными сторонами, их ожиданиями и ценностями;
- организационную культуру;
- стандарты, руководства и модели, принятые организацией;
- форму и содержание контрактных отношений.

[Руководство ИСО 73:2009, определение 3.3.1.2]

2.12 **обмен информацией и консультирование** (communication and consultation): Непрерывные и итерационные процессы, которые организация осуществляет для обеспечения, совместного использования или получения информации и ведения диалога с **заинтересованными сторонами** (2.13), касающегося управления **рисками** (2.1).

Примечание 1 - Информация может касаться наличия, характера, формы, вероятности или **возможности** (2.19), важности, приемлемости, **оценивания** (2.24) и **воздействия на риск** (2.25).

Примечание 2 - Консультирование - это двусторонний процесс квалифицированного обмена информацией между организацией и ее заинтересованными сторонами по любому вопросу, перед тем как вынести решение или перед определением направления решения этого вопроса.

Консультирование - это:

- процесс, который воздействует на принимаемое решение посредством влияния, а не властных полномочий;
- отправная точка принятия решений, а не совместное принятие решений.

[Руководство ИСО 73:2009, определение 3.2.1]

2.13 **заинтересованная сторона** (stakeholder): Лицо или организация, которые могут воздействовать, или на которые могут воздействовать, или которые считают, что на них влияет какое-либо решение или деятельность.

Примечание - Лицо, принимающее решения, может быть заинтересованной стороной.

[Руководство ИСО 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).

[Руководство ИСО 73:2009, определение 3.4.1]

2.15 **идентификация риска** (risk identification): Процесс обнаружения, распознавания и описания **рисков** (2.1).

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

Примечание 2 - Идентификация риска может использовать исторические данные, теоретический анализ, обоснованную точку зрения и экспертные мнения и потребности **заинтересованных** сторон (2.13).

[Руководство ИСО 73:2009, определение 3.5.1]

2.16 **источник риска** (risk source): Элемент, который отдельно или в комбинации имеет собственный потенциал, чтобы вызвать риск (2.1).

Примечание - Источник риска может быть материальным и нематериальным.

[Руководство ИСО 73:2009, определение 3.5.1.2]

2.17 **событие** (event): Возникновение или изменение ряда конкретных обстоятельств.

Примечание 1 - Событие может иметь одно или несколько происхождений и может иметь несколько причин.

Примечание 2 - Событие может заключаться в том, что какое-то явление не имело места.

Примечание 3 - Иногда событие может рассматриваться как "инцидент" или "несчастный случай".

Примечание 4 - Событие без **последствий** (2.18) можно также рассматривать как "случайное избежание", "инцидент", "почти опасное или опасное", "почти произошедшее".

[Руководство ИСО 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, может иметь положительные и отрицательные влияния на цели.

Примечание 3 - Последствия могут выражаться качественно или количественно.

Примечание 4 - Первоначальные последствия могут усиливаться за счет эффекта домино.

[Руководство ИСО 73:2009, определение 3.6.1.3]

2.19 **вероятность, возможность** (likelihood): Шанс того, что что-то может произойти.

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

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

[Руководство ИСО 73:2009, определение 3.6.1.1]

2.20 **профиль риска** (risk profile): Описание какого-либо набора рисков (2.1).

Примечание - Такой набор может включать риски, которые относятся ко всей организации, ее части или определенные иным образом.

[Руководство ИСО 73:2009, определение 3.8.2.5]

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

Примечание 1 - Анализ риска обеспечивает основу для **оценивания риска** (2.24) и решений, касающихся **воздействия на риск** (2.25).

Примечание 2 - Анализ риска включает определение степени риска.

[Руководство ИСО 73:2009, определение 3.6.1]

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

Примечание 1 - Критерии риска основываются на целях организации и **внешней** (2.10) и **внутренней ситуации (контекста)** (2.11).

Примечание 2 - Критерии риска могут быть взяты из стандартов, законов, политик и других требований.

[Руководство ИСО 73:2009, определение 3.3.1.3]

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

[Руководство ИСО 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 относительно **воздействия на риск** (2.25).

[Руководство ИСО 73:2009, определение 3.7.1]

2.25 **воздействие на риск** (risk treatment): Процесс модификации (изменения) **риска** (2.1).

Примечание 1 - Воздействие на риск может включать:

- избежание риска посредством решения не начинать или не продолжать деятельность, в результате которой возникает риск;
- принятие или увеличение риска для использования благоприятной возможности;
- устранение **источника риска** (2.16);
- изменение вероятности или **возможности** (2.19);
- изменение **последствий** (2.18);
- разделение риска с другой стороной или сторонами (включая контракты и финансирование риска);
- осознанное удержание риска.

Примечание 2 - Воздействие на риск, имеющий отрицательные последствия, иногда называют "смягчением риска", "устранением риска", "предупреждением риска" и "снижением риска".

Примечание 3 - Воздействие на риск может создавать новые риски или изменять существующие риски.

[Руководство ИСО 73:2009, определение 3.8.1]

2.26 **контроль риска** (control): Мера, которая модифицирует (изменяет) **риск** (2.1).

Примечание 1 - Контроль риска может включать любой процесс, политику, методику, практику или другие действия, модифицирующие риск.

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

[Руководство ИСО 73:2009, определение 3.8.1.1]

2.27 **остаточный риск** (residual risk): **Риск** (2.1), сохраняющийся после **воздействия на риск** (2.25).

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

Примечание 2 - Остаточный риск может быть также известен как "удержанный риск".

[Руководство ИСО 73:2009, определение 3.8.1.6]

2.28 **мониторинг** (monitoring): Постоянная проверка, надзор, критическое наблюдение или определение состояния с целью идентифицировать изменения относительно требуемого или ожидаемого уровня.

Примечание - Мониторинг можно применять к **инфраструктуре менеджмента риска** (2.3), **процессу менеджмента риска** (2.8), **риску** (2.1) или контролю **риска** (2.26).

[Руководство ИСО 73:2009, определение 3.8.2.1]

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

Примечание - Процедуры пересмотра можно применять к **структуре менеджмента риска** (2.3), **процессу менеджмента риска** (2.8), **риску** (2.1) или **контролю риска** (2.26).

[Руководство ИСО 73:2009, определение 3.8.2.2]

3 Принципы

В целях эффективного управления риском организация должна на всех уровнях соответствовать нижеуказанным принципам:

a) **риск-менеджмент создает и защищает ценность** <1>.

<1> В контексте корпоративного и финансового риск-менеджмента - общепринятый перевод термина "стоимость".

Риск-менеджмент наглядно способствует достижению целей и улучшению деятельности, например, обеспечения здоровья и безопасности людей, защиты, соответствия законодательным и другим обязательным требованиям, общественного признания, защиты окружающей среды, качества продукции, менеджмента проектов, результативности функций, руководства и репутации;

b) **риск-менеджмент является неотъемлемой частью всех организационных процессов**.

Риск-менеджмент не является обособленной деятельностью, которая отделена от основной деятельности и процессов в организации. Риск-менеджмент - это часть обязательств руководства и неотъемлемая часть всех организационных процессов, включая стратегическое планирование и все процессы управления проектами и изменениями;

c) **риск-менеджмент является частью процесса принятия решений**.

Риск-менеджмент помогает лицам, принимающим решения, делать обоснованный выбор, определять приоритетность действий и проводить различия между альтернативными направлениями действий;

d) **риск-менеджмент явным образом связан с неопределенностью**.

Риск-менеджмент четко учитывает неопределенность, характер этой неопределенности и как с ней обращаться;

e) **риск-менеджмент является систематическим, структурированным и своевременным**.

Систематический, регулярный и структурированный подход к риск-менеджменту способствует эффективности и устойчивым, сравнимым и надежным результатам;

f) **риск-менеджмент основывается на наилучшей доступной информации**.

Входные данные для процесса риск-менеджмента основываются на таких источниках информации, как исторические данные, опыт, обратная связь от заинтересованных сторон, наблюдения, прогнозы и экспертные оценки. Однако лица, принимающие решения, должны отдавать себе отчет и принимать во внимание любые ограничения данных или используемого моделирования или возможности расхождений мнений среди экспертов.

g) **риск-менеджмент является адаптируемым**.

Риск-менеджмент должен соответствовать внешней и внутренней ситуации (контексту) и

профилю риска;

h) **риск-менеджмент учитывает человеческие и культурные факторы**.

Риск-менеджмент признает возможности, восприятия и намерения людей за пределами и внутри организации, которые могут способствовать или затруднять достижение целей организации;

i) **риск-менеджмент является прозрачным и учитывает интересы заинтересованных сторон**.

Соответствующее и своевременное вовлечение заинтересованных сторон и, в частности, лиц, принимающих решения, на всех уровнях организации гарантирует, что риск-менеджмент остается на надлежащем уровне и отвечает современным требованиям. Это позволяет заинтересованным сторонам быть должным образом представленными и быть уверенными в том, что их мнение принимается во внимание в процессе установления критериев риска;

j) **риск-менеджмент является динамичным, итеративным и реагирующим на изменения**.

Риск-менеджмент непрерывно распознает изменения и реагирует на них. Как только происходит внешнее или внутреннее событие, контекст или знания изменяются, осуществляются мониторинг и пересмотр рисков, новые риски появляются, некоторые изменяются, другие исчезают;

k) **риск-менеджмент способствует постоянному улучшению организации**.

Организации должны разрабатывать и применять стратегии повышения совершенства риск-менеджмента одновременно с другими своими аспектами.

В Приложении А приведены дальнейшие рекомендации организациям, желающим управлять рисками более эффективно.

4 Инфраструктура

4.1 Общие положения

Успех риск-менеджмента зависит от эффективности инфраструктуры менеджмента, предоставляющей базовые основы и мероприятия, которые должны использоваться во всей организации на всех уровнях. Инфраструктура способствует эффективному управлению рисками посредством применения процесса риск-менеджмента (см. раздел 5) на различных уровнях и в рамках конкретной ситуации **(контекста)** в организации. Инфраструктура гарантирует, что информация о риске, полученная из процесса риск-менеджмента, должным образом регистрируется и используется в качестве основы для принятия решения и отчетности на всех соответствующих уровнях организации.

В настоящем разделе представлены необходимые элементы инфраструктуры риск-менеджмента и способ, обеспечивающий их взаимосвязь итеративным образом, как показано на рисунке 2.

Рисунок 2 - Взаимосвязь между элементами инфраструктуры риск-менеджмента

Настоящая инфраструктура предназначена не для того, чтобы предписать систему управления, а для того, чтобы оказать содействие организации во внедрении риск-менеджмента в свою общую систему менеджмента. Таким образом, организации должны адаптировать элементы инфраструктуры для своих конкретных потребностей.

Если практики и процессы менеджмента, существующие в организации, включают элементы риск-менеджмента или если организация уже приняла формально процесс риск-менеджмента для отдельных рисков или ситуаций, то их необходимо критически анализировать и оценивать на соответствие настоящему стандарту, включая признаки, содержащиеся в Приложении А, чтобы определить их адекватность и эффективность.

4.2 Полномочия и обязательства

Внедрение риск-менеджмента и обеспечение его постоянной эффективности требует принятия со стороны руководства организации четко сформулированных и последовательно выполняемых обязательств по реализации плана управления на всех уровнях, а также подробного стратегического планирования для выполнения этих обязательств. Руководство должно:

- определять и поддерживать политику менеджмента риска;

- гарантировать согласованность культуры организации и ее политики менеджмента риска;

- определять критерии эффективности риск-менеджмента, которые должны соотноситься с критериями эффективности организации в целом;

- согласовывать цели риск-менеджмента с целями и стратегиями организации;

- обеспечивать правовое и регулятивное соответствие;

- устанавливать ответственность и обязательства на соответствующих уровнях в масштабах организации;

- обеспечивать распределение необходимых ресурсов для риск-менеджмента;

- предоставлять информацию своим заинтересованным сторонам о выгодах риск-менеджмента и

- обеспечивать, чтобы инфраструктура риск-менеджмента продолжала оставаться соответствующей.

4.3 Разработка инфраструктуры менеджмента риска

4.3.1 Понимание организации и ее ситуации (контекста)

Прежде чем приступить к разработке и внедрению инфраструктуры риск-менеджмента, важно оценить и понять как внешнюю, так и внутреннюю ситуацию (контекст) в организации, т.к. она может значительным образом влиять на разработку инфраструктуры.

Оценивание внешней ситуации (контекста) организации может включать, но не ограничиваться этим:

a) социальную и культурную, политическую, правовую, регулирующую, финансовую, технологическую, экономическую, природную и рыночную среду на международном, национальном, региональном или местном уровнях;

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

c) взаимосвязи с внешними заинтересованными сторонами, их ценностями и восприятием.

Оценивание внутренней ситуации (контекста) организации может включать, но не ограничиваться этим:

- управление, организационную структуру, роли и обязанности;

- политики, цели и стратегии, необходимые для достижения этих целей;

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

- информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);

- взаимосвязи с внутренними заинтересованными сторонами, их ценностями и восприятием;

- культуру организации;

- стандарты, руководства и модели, принятые организацией, и

- форму и содержание контрактных отношений.

4.3.2 Установление политики менеджмента риска

Политика менеджмента рисков должна четко устанавливать цели организации и обязательства в отношении риск-менеджмента и, как правило, закреплять:

- обоснование потребности организации в менеджменте риска;

- связи между целями и политиками организации и политикой менеджмента риска;

- подотчетность и ответственность в отношении риск-менеджмента;

- способы разрешения конфликтов интересов;

- обязательство по обеспечению доступа к необходимым ресурсам для содействия лицам, подотчетным и ответственным за риск-менеджмент;

- способ, которым будут измерять и отчитываться об эффективности деятельности по риск-менеджменту;

- обязательство пересматривать и улучшать политику и инфраструктуру риск-менеджмента периодически, а также в случае наступления событий или изменения обстоятельств.

Политика риск-менеджмента должна быть правильно донесена до заинтересованных сторон.

4.3.3 Ответственность

Организация должна обеспечивать наличие ответственности, полномочий и соответствующей компетенции для риск-менеджмента, включая внедрение и поддержку процесса риск-менеджмента и обеспечение адекватности, результативности и эффективности любого контроля. Этому должно способствовать:

- установление владельцев рисков, ответственных и уполномоченных управлять рисками;

- определение лиц, ответственных за разработку, внедрение и поддержание инфраструктуры риск-менеджмента;

- установление других видов ответственности работников на всех уровнях в организации за процесс риск-менеджмента;

- установление процессов измерения результативности и внешних и/или внутренних процессов отчетности и ее доведения до сведения руководства;

- обеспечение соответствующих уровней признания.

4.3.4 Интеграция в организационные процессы

Риск-менеджмент необходимо включать во все практики и процессы организации таким образом, чтобы он осуществлялся адекватно, эффективно и результативно. Процесс риск-менеджмента должен стать частью этих организационных процессов и не должен отделяться от них. В частности, риск-менеджмент должен быть встроен в разработку политики, в процессы стратегического и бизнес-планирования, включая корректировку планов, а также в процесс управления изменениями.

План менеджмента риска должен быть разработан в масштабах организации для того, чтобы гарантировать применение политики риск-менеджмента и включение риск-менеджмента во все практики и процессы организации. План менеджмента риска может быть интегрирован в другие планы организации, например в стратегический план.

4.3.5 Ресурсы

Организация должна предоставить ресурсы, достаточные для целей риск-менеджмента.

Необходимо учитывать:

- людей, навыки, опыт и компетентность;

- ресурсы, необходимые для каждого этапа процесса риск-менеджмента;

- процессы, методы и инструменты организации, которые необходимо использовать для риск-менеджмента;

- документированные процессы и процедуры;

- системы управления информацией и знаниями;

- программы обучения.

4.3.6 Установление внутренних механизмов обмена информацией и отчетности

Организация должна установить механизмы внутреннего обмена информацией с тем, чтобы поддерживать и способствовать обеспечению распределения ответственности и полномочий по риск-менеджменту. Эти механизмы должны гарантировать, что:

- информация о ключевых элементах инфраструктуры риск-менеджмента и о любых последующих модификациях предоставляется надлежащим образом;

- имеется в наличии соответствующая внутренняя отчетность об инфраструктуре, ее эффективности и результатах;

- на соответствующих уровнях и своевременно предоставляется соответствующая информация, полученная на основе применения риск-менеджмента;

- используются процессы консультирования с внутренними заинтересованными сторонами.

Эти механизмы должны, где это целесообразно, включать процессы по сбору информации о риске из различных источников и могут потребовать проверки источников информации.

4.3.7 Установление внешних механизмов обмена информацией и отчетности

Организация должна разработать и применить план обмена информацией с внешними заинтересованными сторонами. Он должен включать:

- вовлечение соответствующих заинтересованных сторон и обеспечение эффективного обмена информацией;

- внешнюю отчетность для соответствия правовым, регулятивным и руководящим требованиям;

- обеспечение обратной связи и отчетности об обмене информацией и консультациях;

- использование обмена информацией для достижения доверия к организации;

- обмен информацией с заинтересованными сторонами в случае кризиса или непредвиденных обстоятельств.

Эти механизмы должны, где это целесообразно, включать процессы сбора информации о риске из различных источников и могут потребовать проверки источников такой информации.

4.4 Внедрение менеджмента риска

4.4.1 Внедрение инфраструктуры менеджмента риска

При внедрении организационной инфраструктуры менеджмента риска организация должна:

- определить соответствующие сроки и стратегию по применению инфраструктуры;

- применять политику и процесс риск-менеджмента к организационным процессам;

- соответствовать законодательным и другим регулятивным требованиям;

- гарантировать, что принятие решения, включая разработку и установление целей, согласовано с результатами процессов риск-менеджмента;

- проводить информационные и обучающие сессии;

- обмениваться информацией и консультироваться с заинтересованными сторонами с целью обеспечения того, что инфраструктура риск-менеджмента остается на должном уровне.

4.4.2 Внедрение процесса менеджмента риска

Внедряя риск-менеджмент, необходимо обеспечить выполнение процесса риск-менеджмента, приведенного в разделе 5, в соответствии с планом менеджмента риска на всех должных функциональных уровнях организации как часть ее деятельности и процессов.

4.5 Мониторинг и пересмотр инфраструктуры менеджмента риска

Чтобы гарантировать, что риск-менеджмент является эффективным и продолжает поддерживать деятельность организации, организация должна:

- оценивать качество риск-менеджмента с помощью индикаторов, которые периодически пересматриваются для сохранения актуальности;

- периодически сравнивать продвижение с планом по менеджменту риска и определять отклонения от него;

- периодически пересматривать инфраструктуру, политику и план менеджмента риска для обеспечения их адекватности в рамках внутреннего и внешнего контекста организации;

- предоставлять информацию о рисках, об исполнении плана по менеджменту риска и о том, насколько хорошо организация следует политике управления рисками;

- оценивать эффективность инфраструктуры риск-менеджмента.

4.6 Постоянное улучшение инфраструктуры

Основываясь на результатах мониторинга и пересмотра, следует принимать решения в отношении улучшения инфраструктуры риск-менеджмента, политики и плана по менеджменту риска. Эти решения должны приводить к улучшениям риск-менеджмента и развитию его культуры в организации.

5 Процесс

5.1 Общие положения

Процесс риск-менеджмента должен быть:

- неотъемлемой частью менеджмента;

- частью культуры и практики организации;

- соответствовать бизнес-процессам организации.

Он включает деятельность, описанную в 5.2 - 5.6. Процесс риск-менеджмента показан на рисунке 3.

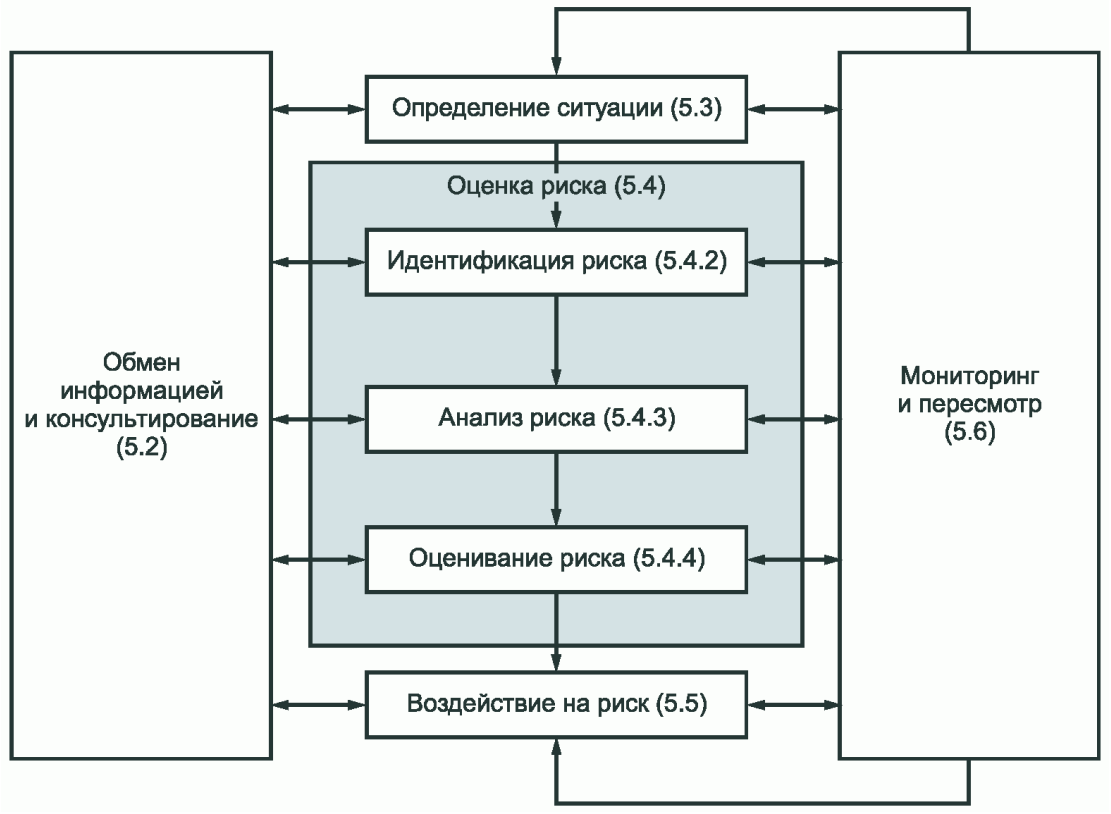

Рисунок 3 - Процесс риск-менеджмента

5.2 Обмен информацией и консультирование

Обмен информацией и консультирование с внешними и внутренними заинтересованными

сторонами осуществляются на всех этапах процесса риск-менеджмента.

Поэтому планы обмена информацией и консультирования должны быть разработаны на раннем этапе. Они должны рассматривать вопросы, касающиеся самого риска, его причин, его последствий (если они известны) и мер, предпринимаемых для воздействия на него. Должны осуществляться эффективный внешний и внутренний обмен информацией и консультирование, с тем чтобы гарантировать, что подотчетные лица, ответственные за процесс риск-менеджмента, и заинтересованные стороны представляют себе основу, на базе которой принимаются решения, и осознают причины того, почему требуются конкретные действия.

Подход на основе создания консультативной группы может:

- помочь должным образом установить ситуацию (контекст);

- гарантировать, что интересы заинтересованных сторон осознаются и рассматриваются;

- способствовать соответствующей идентификации рисков;

- объединять вместе различные области экспертизы для анализа рисков;

- гарантировать рассмотрение должным образом различных точек зрения при определении критериев риска и при оценивании рисков;

- обеспечивать одобрение и поддержку плана воздействия на риск;

- совершенствовать соответствующее управление изменениями во время процесса риск-менеджмента;

- разрабатывать соответствующий внешний и внутренний обмен информацией и план консультирования.

Обмен информацией и консультирование с заинтересованными сторонами являются важными аспектами, потому что с их помощью делают выводы о риске, основанные на их восприятиях риска. Эти восприятия могут отличаться вследствие различий в ценностях, потребностях, предположениях, понятиях и опасениях заинтересованных сторон. Поскольку их точки зрения могут иметь существенное влияние на принимаемые решения, то восприятия заинтересованных сторон необходимо идентифицировать, регистрировать, записывать и учитывать в процессе принятия решений.

Обмен информацией и консультирование должны способствовать обмену правдивой, существенной, точной и понятной информацией с учетом аспектов конфиденциальности и личной неприкосновенности.

5.3 Определение ситуации

5.3.1 Общие положения

Посредством установления ситуации (контекста) организация формулирует свои цели, определяет внешние и внутренние параметры, которые следует принимать во внимание при управлении рисками, и определяет область применения и критерии риска для оставшегося процесса. Поскольку многие параметры аналогичны тем, которые рассматриваются при разработке инфраструктуры риск-менеджмента (см. 4.3.1), в этом случае при установлении ситуации (контекста) для процесса риск-менеджмента их следует рассматривать более подробно и, в частности, как они связаны с областью применения конкретного процесса

риск-менеджмента.

5.3.2 Установление внешней ситуации

Внешняя ситуация (контекст) - это внешняя среда, в которой организация стремится к достижению своих целей.

Понимание внешней ситуации (контекста) является важным для обеспечения того, что цели и опасения внешних заинтересованных сторон рассматриваются при разработке критериев риска. Это основывается на ситуации (контексте) во всей организации, но с конкретными подробностями правовых и регулятивных требований, восприятия заинтересованных сторон и других аспектов рисков, специфических для области применения конкретного процесса риск-менеджмента.

Внешняя ситуация (контекст) организации может включать, но не ограничиваться этим:

a) социальную и культурную, политическую, правовую, регулирующую, финансовую, технологическую, экономическую, природную и рыночную среду на международном, национальном, региональном или местном уровнях;

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

c) взаимосвязи с внешними заинтересованными сторонами, их ценности и восприятие.

5.3.3 Установление внутренней ситуации

Внутренняя ситуация (контекст) - это внутренняя среда, в которой организация стремится к достижению своих целей.

Процесс риск-менеджмента должен соответствовать культуре, процессам, структуре и стратегии организации. Внутренняя ситуация (контекст) - это что-либо в масштабе организации, что может влиять на то, каким образом организация будет осуществлять риск-менеджмент. Внутреннюю ситуацию (контекст) необходимо определить в силу того, что:

a) риск-менеджмент имеет место в контексте целей организации;

b) цели и критерии конкретного проекта, процесса или деятельности следует рассматривать в свете целей организации в целом;

c) некоторые организации затрудняются распознать возможности достижения своих стратегических, проектных или коммерческих целей, и это влияет на текущие обязательства, возможности, доверие и ценность <2> организации.

<2> В контексте корпоративного и финансового риск-менеджмента для данного термина наиболее подходит понятие "стоимость".

Необходимо понимать внутреннюю ситуацию (контекст). Она может включать, но не ограничиваться этим, следующие составляющие:

- управление, организационную структуру, роли и обязанности;

- политики, цели и стратегии, необходимые для достижения этих целей;

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

- информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);

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

- культуру организации;

- стандарты, руководства и модели, принятые организацией;

- форму и содержание контрактных отношений.

5.3.4 Установление ситуации процесса менеджмента риска

Необходимо устанавливать цели, стратегии, область применения и параметры деятельности организации или тех ее частей, где применяется процесс риск-менеджмента. Риск-менеджмент следует проводить с полным рассмотрением необходимости обоснования ресурсов, используемых при его осуществлении. Следует также определять требуемые ресурсы, ответственность и полномочия, а также порядок учета.

Ситуация (контекст) процесса риск-менеджмента изменяется в зависимости от потребностей организации. Она может включать, но не ограничиваться этим:

- определение задач и целей деятельности по риск-менеджменту;

- определение ответственностей за процесс риск-менеджмента и в рамках этого процесса;

- определение области применения, а также глубины и широты деятельности по риск-менеджменту, которую необходимо осуществлять, включая особые включения и исключения;

- определение деятельности, процесса, функции, проекта, продукта, услуги или активов с учетом времени и расположения;

- определение взаимосвязей между конкретным проектом, процессом или деятельностью и другими проектами, процессами или видами деятельности организации;

- определение методологий оценки риска;

- определение способа оценки производительности и эффективности риск-менеджмента;

- определение и указание решений, которые необходимо принять;

- идентификацию, охват или объемы необходимого обучения, их уровни и цели, ресурсы, требуемые для такого обучения.

Внимание, уделяемое этим и другим соответствующим факторам, должно гарантировать, что принятый подход риск-менеджмента соответствует обстоятельствам, организации и рискам, воздействующим на достижение ее целей.

5.3.5 Определение критериев риска

Организация должна определить критерии, которые необходимо использовать для оценки значимости риска. Критерии должны отражать ценности, цели и ресурсы организации. Некоторые критерии могут основываться или возникать из правовых и регулятивных требований, а также других требований, которые взяла на себя организация. Критерии риска должны быть согласованы с политикой управления рисками организации (см. 4.3.2), должны быть определены в начале каждого процесса риск-менеджмента и должны постоянно рассматриваться.

При определении критериев риска факторы, которые необходимо рассматривать, должны включать следующее:

- характер и типы причин и последствий, которые могут возникать, и то, как их следует измерять;

- как следует определять возможность;

- временные рамки возможности и/или последствия(й);

- как должен быть определен уровень риска;

- точки зрения заинтересованных сторон;

- уровень, на котором риск становится приемлемым или допустимым;

- принимать ли во внимание множественные риски и если да, то каким образом и какие комбинации следует рассматривать.

5.4 Оценка риска

5.4.1 Общие положения

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

Примечание - Стандарт ИСО/МЭК 31010 предлагает руководство по методам оценки риска.

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 всеобъемлющего перечня рисков, основанных на тех событиях, которые могут создавать, повышать, предотвращать, снижать, ускорять или задерживать достижение целей. Важно идентифицировать риски, связанные с решением не использовать благоприятные возможности. Всеобъемлющая идентификация является критически важной, потому что риск, который не был идентифицирован на данном этапе, не будет включен в будущий анализ.

Идентификация должна включать риски независимо от того, контролирует ли организация их источник или нет, даже если их источник или причина могут быть неочевидными. Идентификация рисков должна включать рассмотрение эффекта домино, включая эффект каскада и кумулятивные эффекты. Также необходимо рассматривать широкий спектр последствий, даже если источник риска может быть не очевиден. Наряду с идентификацией, что может произойти, необходимо рассматривать возможные причины и сценарии, которые показывают, какие могут наступить последствия. Все существенные причины и следствия должны быть рассмотрены.

Организация должна применять инструменты и методы, которые соответствуют ее целям и возможностям, а также рискам, с которыми она сталкивается. На этапе идентификации рисков большое значение имеет соответствующая и актуализированная информация. Это по возможности должно включать соответствующую исходную информацию. Для идентификации рисков необходимо привлекать людей, обладающих соответствующими знаниями.

5.4.3 Анализ риска

Анализ риска включает дальнейшее осознание риска. Анализ риска обеспечивает входную информацию для оценивания риска и решений относительно необходимости дальнейшего воздействия на эти риски, а также наиболее подходящих стратегий и методов воздействия. Анализ риска может также предоставлять входную информацию для принятия решений, когда необходим выбор, и наличие альтернативных вариантов, включающих различные типы и уровни риска.

Анализ риска включает рассмотрение причин и источников риска, их положительных и отрицательных последствий и возможности того, что эти последствия могут произойти. Факторы, влияющие на последствия и возможность, должны быть идентифицированы. Риск анализируют посредством определения последствий и возможности, а также других характеристик риска. Событие может иметь множественные последствия и может воздействовать на различные цели. Необходимо также принимать во внимание существующие средства управления, их результативность и эффективность.

Способ, которым выражают последствия и возможности, и способ их комбинирования для определения уровня риска должны отражать тип риска, имеющуюся информацию и цель, для которой результат оценки риска должен быть использован. Все это должно согласовываться с критериями риска. Также важно рассматривать взаимозависимость различных рисков и их источников.

При анализе необходимо рассматривать достоверность в определении уровня риска и его чувствительность к предварительным условиям и допущениям и эффективно обмениваться информацией с теми, кто принимает решения, и, в случае необходимости, с другими заинтересованным сторонами. Такие факторы, как наличие разброса мнений экспертов, неопределенность, доступность, качество, количество, соответствие текущей информации или ограничения моделирования, необходимо констатировать и по возможности обращать на них особое внимание.

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

Последствия и вероятность (возможность) могут быть определены посредством моделирования исходов событий или ряда событий, или экстраполяцией данных экспериментальных исследований или имеющихся данных. Последствия могут быть выражены в виде материальных или нематериальных воздействий. В некоторых случаях требуется более одного численного значения или описывающий параметр для указания последствий и степени их осуществимости для различных моментов времени, местоположения, групп или ситуаций.

5.4.4 Оценивание риска

Цель оценивания риска заключается в том, чтобы способствовать принятию решений, основанных на исходных результатах анализа риска, относительно необходимости воздействия на риск и установления приоритета воздействия на риск.

Оценивание риска включает сравнение уровня риска, выявленного во время процесса анализа, с установленными критериями риска во время рассмотрения ситуации (контекста). Рассмотрение необходимости воздействия на риск должно основываться на этом сравнении.

Решения должны более широко учитывать ситуацию (контекст) риска и учитывать толерантность к риску не только организации, извлекающей из риска пользу, но и других сторон. Решения должны приниматься в соответствии с правовыми, регулятивными и другими требованиями.

При некоторых обстоятельствах оценивание риска может привести к решению провести дальнейший анализ. Оценивание риска также может привести к решению не воздействовать на риск каким-либо иным образом, кроме поддержания существующих средств управления. На это решение влияют отношение к риску самой организации и установленные критерии риска.

5.5 Воздействие на риск

5.5.1 Общие положения

Воздействие на риск включает выбор одного или более вариантов модифицирования рисков и применение этих вариантов. Будучи примененным, воздействие на риск устанавливает или изменяет средства управления.

Воздействие на риск включает циклический процесс, состоящий из следующих этапов:

- оценивания воздействия на риск;

- обсуждения, являются ли уровни остаточного риска допустимыми;

- если они недопустимы, то создания нового вида воздействия на риск;

- оценивания результативности этого воздействия.

Альтернативные варианты воздействия на риск не обязательно являются взаимоисключающими или подходящими для всех обстоятельств. Альтернативные варианты могут включать:

a) избежание риска посредством решения не начинать или не продолжать деятельность, в результате которой возникает риск;

b) принятие или увеличение риска для использования благоприятной возможности;

c) устранение источника риска (2.16);

d) изменение возможности (2.19);

e) изменение последствий (2.18);

f) разделение риска с другой стороной или сторонами (включая контракты и финансирование риска);

g) осознанное удержание риска.

5.5.2 Выбор вариантов воздействия на риск

Выбор наиболее подходящего варианта воздействия на риск включает уравновешивание затрат и усилий реализации с извлекаемыми выгодами с учетом правовых, регулятивных и других требований, таких как ответственность перед обществом и защита окружающей среды. Процесс принятия решений должен быть построен таким образом, чтобы обеспечить принятие мер по таким рискам, управление которыми не обосновано с экономической точки зрения, например значительные (со значительными негативными последствиями), но редкие (с низкой вероятностью или возможностью наступления) риски.

Количество вариантов воздействия на риск можно рассматривать и применять либо по отдельности, либо в комбинации. Организация может обычно извлекать выгоду из принятия комбинации вариантов воздействия на риск.

При выборе вариантов воздействия на риск организация должна рассматривать значения и восприятия заинтересованных сторон и наиболее подходящие способы обмена информации с ними. Если альтернативные варианты воздействия на риск могут влиять на риск где-либо еще в организации или в отношении заинтересованных сторон, то это следует учитывать при принятии решения. Будучи одинаково эффективными, некоторые варианты воздействия на риск могут быть более приемлемы для одних заинтересованных сторон, чем для других.

В плане воздействия на риск должен быть четко указан порядок приоритета, в соответствии с которым должны применяться отдельные воздействия на риск.

Воздействие на риск может само по себе вызывать риски. Существенным риском может быть отсутствие или неэффективность мер воздействия на риск. Мониторинг должен стать неотъемлемой частью плана воздействия на риск, с тем чтобы гарантировать, что меры остаются эффективными.

Воздействие на риск может также вызывать вторичные риски, которые необходимо оценивать, воздействовать на них, подвергать мониторингу и анализу. Такие вторичные риски должны включаться в тот же самый план воздействия на риск, что и первоначальный риск, и не рассматриваться как новый риск. Следует определить и учитывать связь между обоими этими рисками.

5.5.3 Подготовка и реализация планов воздействия на риск

Целью планов воздействия на риск является документирование того, как должны реализовываться выбранные альтернативные варианты воздействия. Информация, представленная в планах воздействия на риски, должна включать:

- причины выбора вариантов воздействия на риски, включая ожидаемые выгоды, которые необходимо извлечь;

- лиц, ответственных за утверждение плана, и лиц, ответственных за реализацию плана;

- предлагаемые действия;

- требования к ресурсам, включая возможные непредвиденные обстоятельства;

- показатели качества воздействия на риск и ограничения;

- требования к отчетности и мониторингу;

- сроки и график выполнения.

Планы воздействия на риски должны быть включены в процессы менеджмента организации и должны обсуждаться с соответствующими заинтересованными сторонами.

Лица, принимающие решения, и другие заинтересованные стороны должны быть ознакомлены с характером и степенью остаточного риска после воздействия на него. Остаточный риск должен быть документирован и подвергнут мониторингу, пересмотру и, где целесообразно, дальнейшему воздействию.

5.6 Мониторинг и пересмотр

Мониторинг и пересмотр должны быть планируемой частью процесса риск-менеджмента и включать регулярную проверку или надзор. Они могут быть периодическими, произвольными.

Должна быть четко определена ответственность за проведение мониторинга и пересмотра.

Процессы мониторинга и пересмотра, осуществляемые организацией, должны включать в себя все аспекты процесса риск-менеджмента в целях:

- гарантии того, что средства управления являются эффективными и результативными как при проектировании, так и при функционировании;

- получения дополнительной информации для улучшения оценки риска;

- анализа и извлечения уроков из случаев (включая риски без последствий), изменений, тенденций, успехов и неудач;

- выявление изменений во внешней и внутренней ситуации (контексте), включая изменения критериев риска, и сам риск, который может потребовать пересмотра способов воздействия на риск и приоритетов;

- идентификации новых или зарождающихся рисков.

Прогресс в реализации планов воздействия на риск обеспечивает достижение показателей эффективности. Результаты могут включаться в общее управление и оценку эффективности, внутреннюю и внешнюю отчетность организации.

Результаты мониторинга и пересмотра должны быть документированы и соответствующим образом зарегистрированы на внешнем и внутреннем уровнях, а также использованы в качестве входных данных для пересмотра инфраструктуры риск-менеджмента (см. 4.5).

5.7 Регистрация процесса менеджмента риска

Деятельность по риск-менеджменту должна быть прослеживаемой. В процессе риск-менеджмента регистрация обеспечивает основу для улучшения методов и инструментов, а также всего процесса.

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

- потребности организации в постоянном обучении;

- преимущества повторного использования информации в целях менеджмента;

- затраты и усилия, вовлеченные в создание и поддержку учета;

- правовые, регулятивные и оперативные потребности в учете;

- метод доступа, простоту восстановления и средства хранения информации;

- период хранения;

- проверку источников информации.

Приложение А
(справочное)

ПРИЗНАКИ УЛУЧШЕННОГО МЕНЕДЖМЕНТА РИСКА

А.1 Общие положения

Все организации должны стремиться достичь соответствующего уровня функционирования их инфраструктуры риск-менеджмента одновременно с критичностью решений, которые должны приниматься. Нижеприведенный перечень признаков представляет высокий показательный уровень риск-менеджмента. Чтобы помочь организациям измерить собственное качество управления рисками в соответствии с этими критериями, для каждого признака приводится несколько показателей.

А.2 Ключевые результаты

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

А.2.2. Риски организации находятся в пределах ее критериев риска.

А.3 Признаки

А.3.1 Постоянное улучшение

Акцент делают на постоянное улучшение риск-менеджмента через установление целей деятельности организации, измерение, пересмотр и последующую модификацию процессов, систем, ресурсов, возможностей и навыков.

Это может подтверждаться наличием определенных целей деятельности, согласно которым измеряют деятельность организации и каждого отдельного менеджера. Данные о деятельности организации могут публиковаться и доводиться до сведения. Обычно проводят, как минимум, годовой пересмотр деятельности и затем ревизию процессов и осуществляют установление целей деятельности на следующий период.

Оценка качества риск-менеджмента является неотъемлемой частью оценки всей деятельности организации и системы измерения качества работы подразделений и отдельных работников.

А.3.2 Полная ответственность за риски

Улучшенный риск-менеджмент включает всестороннюю, полностью определенную и

принятую отчетность и ответственность за риски, средства управления и задачи воздействия на риск. Назначенные лица, которые полностью принимают ответственность, обладают необходимыми навыками и ресурсами для того, чтобы проверять эти мероприятия, осуществлять мониторинг рисков, совершенствовать мероприятия по управлению рисками и эффективно доносить информацию о рисках и управлению ими до внешних и внутренних заинтересованных лиц.

Это может подтверждаться всеми членами организации, которые осведомлены в полном объеме о рисках, средствах управления и задачах, за которые они несут ответственность. Обычно это должно быть отражено в должностных инструкциях, содержаться в информационных базах данных или системах. Распределение ролей в менеджменте рисков, ответственности и обязательств должно быть частью всех ознакомительных программ организации.

Организация должна гарантировать, что ответственные лица оснащены всем необходимым для выполнения своей роли и им предоставлены полномочия, время, обучение, ресурсы и навыки, достаточные для того, чтобы взять на себя ответственность.

A.3.3 Применение менеджмента риска при принятии всех решений

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

Это может быть указано в записях собраний и обсуждений, подтверждающих, что подробные обсуждения рисков имели место. Необходимо обеспечить возможность увидеть, что все элементы риск-менеджмента представлены в ключевых процессах принятия решений, осуществляемых в организации, например, обсуждений размещения капитала по крупным проектам, реструктуризации и организационных изменений. По этим причинам четко обоснованный риск-менеджмент должен просматриваться в масштабах организации как обеспечивающий основу для результативного руководства.

A.3.4 Постоянный обмен информацией

Улучшенный риск-менеджмент включает постоянный обмен информацией с внешними и внутренними заинтересованными сторонами, включая всестороннее и периодическое представление информации о деятельности по риск-менеджменту как части надлежащего управления.

Это может быть подтверждено обменом информации с заинтересованными сторонами как неотъемлемым и важным элементом риск-менеджмента. Обмен информацией правильно рассматривать как двусторонний процесс, такой, что правильно обоснованные решения могут приниматься в отношении уровня рисков и потребности в воздействии на риск в соответствии с установленными должным образом и всесторонними критериями риска.

Всестороннее и периодическое внешнее и внутреннее представление информации о значительных рисках и о результатах деятельности по риск-менеджменту способствует в значительной мере результативному руководству в масштабах организации.

A.3.5 Полная интеграция в структуру руководства организации

К риск-менеджменту относятся как к центральному процессу менеджмента организации, а риски рассматривают с точки зрения воздействия неопределенности на цели. Структура руководства и процесс основываются на риск-менеджменте. Менеджеры считают

результативный риск-менеджмент существенным для достижения целей организации.

Это может подтверждаться формулировками менеджеров и в важных письменных материалах в организации с использованием термина "неопределенность" в отношении рисков. Этот признак также обычно отражается в заявлениях организации, касающихся политики, в частности той, которая относится к управлению рисками. Как правило, этот признак может проверяться посредством интервью с менеджерами и на основе их действий и заявлений.

Библиография

[1] ISO Guide 73:2009, Risk management - Vocabulary (Руководство ИСО 73:2009. Словарь) <*>

[2] ISO/IEC 31010:2009, Risk management - Risk assessment techniques (ИСО/МЭК 31010 Менеджмент риска. Методы оценки риска) <*>

<*> Официальный перевод этого стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.