ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 51901.7— 2017/ ISO/TR 31004:2013

МЕНЕДЖМЕНТ РИСКА

Руководство по внедрению ИСО 31000

(ISO/TR 31004:2013 Risk management — Guidance for the implementation of ISO 31000, IDT)

Издание официальное

Москва
Стандартинформ
2017

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Открытым акционерным обществом «Научно-исследовательский центр контроля и диагностики технических систем» (АО «НИЦ КД») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 12 сентября 2017 г. № 1060-ст

4 Настоящий стандарт идентичен международному документу ISO/TR 31004:2013 «Менеджмент риска. Руководство по внедрению ИСО 31000» (ISO/TR 31004:2013 «Risk management — Guidance for the implementation of ISO 31000», IDT).

Международный стандарт разработан Техническим комитетом ISO/TC 262.

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2017

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Внедрение ИСО 31000 1
Приложение А (справочное) Основные концепции и принципы 6
Приложение В (справочное) Применение принципов ИСО 31000 8
Приложение С (справочное) Способы выражения полномочий и обязательств 16
Приложение D (справочное) Мониторинг и анализ 19
Приложение Е (справочное) Интегрирование менеджмента риска в общую систему менеджмента . . 26
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 28
Библиография 29

Введение

0.1 Общие положения

Организации используют для достижения поставленных целей различные методы менеджмента риска (выявление, обнаружение, понимание и, при необходимости, обработку риска).

Настоящий стандарт может помочь организациям повысить результативность менеджмента риска в соответствии с ИСО 31000, устанавливающим общий подход к менеджменту риска организации.

Настоящий стандарт предназначен для лиц, ответственных за принятие решений, воздействующих на достижение целей организации, включая ответственных за менеджмент риска, экспертов в области риска и специалистов отделов по управлению риском. Настоящий стандарт предназначен для использования всеми заинтересованными лицами, связанными с деятельностью в области риска, включая преподавателей, студентов, а также лиц, участвующих в разработке законодательных и обязательных требований.

Настоящий стандарт следует применять вместе с ИСО 31000, стандарт применим к организациям всех типов и размеров. Основные концепции и определения, необходимые для понимания ИСО 31000, приведены в приложении А. Общие методы, направленные на приведение в соответствие существующих методов менеджмента риска организации требованиям ИСО 31000, приведены в разделе 3. Настоящий стандарт обеспечивает также динамическое регулирование в соответствии с изменением внутренней и внешней среды организации.

В приложениях приведены дополнительные объяснения и примеры внедрения ИСО 31000.

Примеры, описанные в настоящем стандарте, приведены только для иллюстрации.

0.2 Основные положения и принципы

Некоторые понятия и концепции являются фундаментальными для понимания ИСО 31000 и настоящего стандарта, их объяснение приведено в разделе 2 ИСО 31000:2009 и приложении А.

В ИСО 31000 установлено одиннадцать принципов эффективного менеджмента риска. Принципы являются информационной и руководящей основой во всех аспектах менеджмента риска организации. Принципы устанавливают характеристики эффективного менеджмента риска. Организация должна не просто внедрить принципы менеджмента риска, а включить эти принципы во все аспекты менеджмента. Они служат показателями выполнения менеджмента риска и повышают значение эффективной организации менеджмента риска. Принципы менеджмента риска воздействуют на все элементы процесса в переходный период, описанные в настоящем стандарте, возникающие при этом технические проблемы описаны в приложениях. Более детальные рекомендации приведены в приложении В.

В настоящем стандарте использованы термины «высшее руководство» и «контролирующий орган». Термин «контролирующий орган» относят к лицу или группе лиц, которые направляют деятельность организации и управляют организацией на высшем уровне. Термин «контролирующие организации» относят к лицу или группе лиц, которые дают руководящие указания и проверяют деятельность высшего руководства.

Примечание — Во многих организациях функции «контролирующего органа» могут быть возложены на совет директоров, попечительский совет, наблюдательный совет и т. д.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ РИСКА

Руководство по внедрению ИСО 31000

Risk management. Guidance for the implementation of ISO 31000

Дата введения — 2018—12—01

1 Область применения

В настоящем стандарте приведены руководящие указания по внедрению в организации эффективного менеджмента риска на основе применения требований ИСО 31000. В стандарте приведены:

- структурированный подход, направленный на приведение менеджмента риска организации в соответствии с требованиями ИСО 31000 с учетом особенностей деятельности организации;
- разъяснение основных положений ИСО 31000;
- руководящие указания по внедрению принципов и структуры менеджмента риска, приведенных в ИСО 31000.

Настоящий стандарт может быть использован государственными, частными и/или общественными организациями, ассоциациями, группой лиц или отдельными лицами.

Примечание — Для удобства различные пользователи настоящего стандарта далее объединены общим термином «организация».

Настоящий стандарт может быть применен ко всем видам деятельности и всем подразделениям организации.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ISO 31000:2009 Risk management — Principles and guidelines (Менеджмент риска — Принципы и руководящие указания)

3 Внедрение ИСО 31000

3.1 Общие положения

В данном разделе приведено руководство по приведению существующего менеджмента риска организации в соответствие с принципами и требованиями ИСО 31000, при этом необходимо обеспечить непрерывность соответствия менеджмента риска организации этим требованиям.

Приведенная в стандарте общая методология применима при плановом подходе всеми организациями независимо от особенностей мероприятий менеджмента риска организации и включает в себя следующее:

- сравнение существующей деятельности с требованиями ИСО 31000;
- идентификацию необходимых изменений и подготовку плана внедрения этих изменений;
- выполнение непрерывного мониторинга и анализа для обеспечения постоянного улучшения.

Осуществление этих действий позволит организации достичь понимания своего риска и обеспечить соответствие риска критериям и отношению организации к риску.

Издание официальное

Независимо от причин внедрения ИСО 31000 применение его положений и требований может позволить организации лучше управлять своими рисками и эффективно достигать поставленных целей. Все организации до некоторой степени управляют риском. Стратегия внедрения ИСО 31000 должна отражать способ управления риском в организации.

Процесс внедрения, описанный в 3.2, позволяет провести сравнительную оценку существующего менеджмента риска организации с требованиями ИСО 31000 и, в случае необходимости, адаптировать и внести необходимые изменения.

В ИСО 31000 идентифицированы различные элементы структуры менеджмента риска. Если эти элементы интегрированы в управление, функции и процессы организации, она может достичь целого ряда преимуществ в работе, связанных со скоростью принятия решений, результативностью и эффективностью работы. Ниже перечислены основные преимущества такой интеграции.

a) Менеджмент риска может быть встроен в общую систему менеджмента и принятия решений организации; независимо от того, является система формальной или неформальной; существующие процессы менеджмента могут быть улучшены в соответствии с ИСО 31000.

b) Понимание неопределенности при управлении организацией становится неотъемлемой частью системы менеджмента, при этом могут быть установлены общие принципы менеджмента организации.

c) Внедрение процесса менеджмента риска учитывает особенности, размер и требования организации.

d) Управление политикой, структурой и процессом(ами) в области менеджмента риска может быть интегрировано в существующие системы менеджмента организации.

e) Отчетность в области менеджмента риска может быть интегрирована в общую отчетность организации.

f) Выполнение действий менеджмента риска становится неотъемлемой частью общего подхода к работе организации.

g) Взаимодействие и связь между отдельными областями менеджмента риска организации (например, менеджмент риска подразделения, финансовый менеджмент риска, менеджмент риска проекта, менеджмент безопасности, обеспечение непрерывности бизнеса, страховой менеджмент) могут быть достигнуты и/или улучшены путем учета риска при достижении целей и урегулировании проблем организации.

h) Организация может улучшить обмен информацией о неопределенности и риске между группами, участвующими в менеджменте риска и различными уровнями управления организации.

i) Направление действий в области менеджмента риска организации могут быть сосредоточены на достижении целей и приняты за общее направление работы организации. Организация может получить косвенные социальные выгоды, поскольку внешние заинтересованные лица организации могут быть мотивированы на улучшение их деятельности в области менеджмента риска.

j) Обработка риска, средства и методы контроля риском могут стать неотъемлемой частью ежедневной деятельности организации.

3.2 Способы внедрения ИСО 31000

В стандарте ИСО 31000 приведено разъяснение способов эффективного менеджмента риска, однако способы интеграции менеджмента риска в процессы менеджмента организации в стандарте рассмотрены недостаточно. Существуют различные организации с разными отправными точками в области менеджмента риска, однако общий и систематический подход к внедрению применим во всех случаях. Организация должна определить необходимость внесения изменений в существующую структуру менеджмента риска, спланировать и внедрить эти изменения и затем проводить непрерывный мониторинг результативности. Это позволит организации:

- привести существующий в организации менеджмент риска в соответствие с принципами и требованиями, установленными в ИСО 31000, пункт 3;
- применять процесс менеджмента риска, описанный в ИСО 31000, пункт 5;
- установить признаки улучшенного менеджмента риска в соответствии с А.3 приложения А ИСО 31000;
- достигнуть ключевых результатов (см. ИСО 31000, пункт 2).

Данный подход также применим к организациям, в которых достигнуто соответствие требованиям ИСО 31000, для выполнения требований ИСО 31000, пункты 4.6 и 5.6, относительно постоянного улучшения структуры и процессов менеджмента риска.

При внесении изменений в менеджмент риска организации рекомендовано использовать опыт других организаций по управлению аналогичными типами риска или аналогичными процессами.

3.3 Интеграция требований ИСО 31000 в процессы менеджмента организации

3.3.1 Общие положения

Стандарт ИСО 31000 устанавливает структуру и основной процесс менеджмента риска организаций всех типов и их отдельных частей. Рекомендации данного подраздела помогают интегрировать элементы ИСО 31000 в общий менеджмент организации, включая действия, процессы и функции. Организации могут интегрировать положения ИСО 31000 в существующие процессы и/или разработать и внедрить новый подход, основанный на ИСО 31000. В данном подразделе установлены основные элементы структуры, процесса и действий, необходимых для успешной интеграции этих элементов и достижения целей организации. Существует много способов внедрения стандарта ИСО 31000 в организации. Выбор и порядок внедрения элементов должны соответствовать потребностям организации и ее заинтересованным сторонам. Необходимо учесть, что менеджмент риска должен поддерживать общую стратегию управления бизнесом, т. е. помогать организации в достижении цели, защите бизнеса и создании дополнительной ценности организации. Следует также учитывать особенности культуры организации, а также методы управления изменениями и проектами.

Внедрение стандарта ИСО 31000 является динамическим итеративным процессом. Внедрение структуры связано с процессом менеджмента риска, описанным в пункте 5 ИСО 31000. Преимущества от внедрения можно получить от интеграции и постоянного улучшения менеджмента риска во всей организации.

Интеграцию следует рассматривать в условиях динамического изменения среды организации. Организация должна проводить мониторинг изменений, которые вызваны процессом внедрения, а также изменений внутренней и внешней среды. При этом может возникнуть потребность в изменении критериев риска.

3.3.2 Полномочия и обязательства

Все действия по управлению бизнесом обычно начинают с анализа их целесообразности, разработки этапов процесса и оценки экономической эффективности. Эти действия обычно основаны на решении высшего руководства и контролирующего органа о внедрении, выделении необходимых ресурсов и наделении ответственных лиц необходимыми полномочиями.

Обычно процесс внедрения включает следующее:

a) получение необходимых полномочий и принятие обязательств;

b) анализ слабых мест;

c) индивидуальную адаптацию и определение масштаба работ, на основе потребностей, культуры, создания и защиты ценности организации;

d) сравнительную оценку риска, связанную с переходом;

e) разработку бизнес-плана:

- установление целей, приоритетов и показателей;
- разработка экономического обоснования ситуации, включая соответствие целям организации;
- определение области применения, подотчетности, графика работ и ресурсов;

f) идентификацию условий внедрения менеджмента риска, включая обмен информацией с заинтересованными сторонами.

3.3.3 Проектирование и разработка структуры

3.3.3.1 Организация должна оценить существующие подходы к менеджменту риска, включая область применения, среду и культуру.

a) Необходимо провести анализ всех законодательных и обязательных требований, требований потребителей и требований сертификации, исходя из применяемых организацией стандартов. Цель этого этапа состоит в том, чтобы при проектировании и разработке структуры и плана внедрения менеджмента риска учесть индивидуальные особенности организации и адаптировать их в соответствии со структурой, культурой и общей системой менеджмента организации.

b) Важно рассмотреть процесс менеджмента риска и аспекты существующей структуры менеджмента риска, обеспечивающей этот процесс.

c) Необходимо установить соответствующие критерии риска. Критерии риска должны быть совместимы с целями и отношением организации к риску. При изменении целей необходимо соответственно изменять критерии риска.

Для проектирования и разработки новой структуры необходимо провести сравнительную оценку:

- принципов и альтернативных характеристик в соответствии с ИСО 31000;
- предыдущей структуры, оценка которой должна помочь сравнить особенности существующей практики менеджмента риска с требованиями следующих подразделов ИСО 31000:
  - 4.3.2 (политика в области менеджмента риска);
  - 4.3.3 (распределение ответственности и полномочий);
  - 4.3.4 (интеграция в процессы организации);
  - 4.3.5 (ресурсы);
  - 4.3.6 и 4.3.7 (внутренний и внешний обмен информацией и отчетность);
- процесса менеджмента риска, путем сравнения элементов существующих процессов с требованиями пункта 5 ИСО 31000 и анализа основных принципов, которые лежат в основе и обеспечивают целесообразность процесса с точки зрения принципов, установленных в ИСО 31000, пункт 3 (например, применим ли данный процесс к принятию решений на всех уровнях и во всех подразделениях организации). Необходимо оценить:
  - обеспечивает ли текущий процесс лицам, принимающим решения, необходимую информацию о риске, чтобы принятые решения были качественными и соответствовали целям организации или превышали их;
  - достаточен ли существующий подход к менеджменту риска для управления связанными рисками и рисками, возникающими в нескольких местах.

3.3.3.2 Требования к проектированию и разработке структуры должны быть идентифицированы.

Организация должна на основе сравнительной оценки (см. 3.3.3.1) принять решение о том, какие аспекты текущего менеджмента риска:

a) можно использовать в будущем (распространить на другие типы принятия решений);

b) требуют исправления и улучшения;

c) больше не увеличивают ценность и должны быть исключены.

Организация должна разрабатывать, документировать способы управления риском и проводить обмен информацией о них. Объем и содержание внутренних стандартов, руководящих принципов и моделей, связанных с менеджментом риска, должны отражать культуру и среду организации.

В документах может быть определено следующее:

- риск, которым необходимо последовательно управлять во всей организации;
- разные уровни ответственности в области менеджмента риска;
- требования к компетентности и обязанностям всех лиц, ответственных за менеджмент риска;
- вовлеченные внутренние и внешние заинтересованные стороны посредством всестороннего обмена информацией и консультаций;
- информация о риске и результатах применения процесса менеджмента риска, которые должны быть последовательно и безопасно зарегистрированы, с соответствующим доступом к этой информации.

Организация должна проводить анализ требований менеджмента риска, необходимых методов, обучения и ресурсов через запланированные интервалы времени, при значимых изменениях организации и/или ее среды или в ситуации, когда в результате мониторинга и анализа идентифицированы пробелы или неэффективность работы.

3.3.3.3 Должны быть определены область применения, цели, задачи, ресурсы, показатели результативности и критерии мониторинга и анализа.

3.3.3.4 Должны быть установлены методы внутреннего и внешнего обмена информацией и отчетности.

3.3.4 Внедрение менеджмента риска

Необходимо разработать детальный план внедрения менеджмента риска, чтобы обеспечить осуществление последовательных изменений и требуемые ресурсы. План должен быть поддержан ресурсами, необходимыми для его выполнения, при этом бюджетирование должно стать частью процесса планирования.

План внедрения менеджмента риска необходимо проанализировать в соответствии с ИСО 31000:2009, пункт 5.4 результаты сравнения должны быть переведены в действия по обработке риска.

План должен помочь прослеживать действия по внедрению менеджмента риска и помочь обмену информацией с высшим руководством и контролирующим органом. План необходимо анализировать и пересматривать через запланированные интервалы времени.

План должен обеспечить:

- детальное описание конкретных действий, их последовательности, исполнителей и срока завершения. Эти действия могут включать внесение изменений во внутренние стандарты и руководства, возможности для разъяснения и обучения, внесение изменений в распределение ответственности и полномочий и отчетность;
- идентификацию всех действий, выполняемых как часть широкомасштабных действий, связанных с развитием организации, или действий, которые связаны иным способом (например, разработку учебного материала и требований к обучающим лицам);
- определение обязанностей по выполнению плана;
- способы обмена информацией о завершении, продвижении и проблемах в процессе работы;
- идентификацию и регистрацию критериев анализа плана.

Внедрение плана менеджмента риска может занять некоторое время до его завершения, поэтому план должен быть реализован последовательно. Целесообразно уделять первостепенное значение тем изменениям, которые оказывают наибольшее влияние на достижение поставленных целей. Внедрение плана менеджмента риска может быть проведено в различных подразделениях организации и на различных стадиях зрелости организации в области менеджмента риска. Внедрение плана менеджмента риска может быть выполнено более эффективно, если его выполнение объединить с другими программами изменений.

3.3.5 Мониторинг и анализ

Организация должна проводить прослеживание, анализ и регулярный (ежемесячный, ежеквартальный и т. п.) обмен информацией с высшим руководством о продвижении внедрения плана менеджмента риска.

Отчеты о выполнении плана менеджмента риска и предпринимаемых действиях необходимо регулярно валидировать после непредубежденного и объективного рассмотрения и анализа. Результаты анализа должны включать экспертизу структуры, процессов, риска и воздействия на окружающую среду.

Организация должна проводить периодический анализ стратегии выполнения, измерения продвижения и последовательности выполнения плана менеджмента риска, а также идентификации отклонений от этого плана. Анализ должен быть инициирован в случае, если идентифицированы критерии анализа, изложенные в плане.

Необходимо провести сравнительную оценку результативности изменений и управления риском, а также идентифицировать полученный опыт и возможности для улучшений.

О существенных проблемах при проведении мониторинга необходимо незамедлительно информировать ответственных лиц.

Полученные результаты необходимо заново рассмотреть на этапе определения области применения и других ранних этапах. Необходимо идентифицировать новые виды риска, изменения существующего риска, которые были обнаружены. Текущий статус структуры должен быть зарегистрирован для внедрения улучшений (см. ИСО 31000:2009, 4.6 и 5.7).

3.4 Постоянное улучшение

Структура менеджмента риска и процесс менеджмента риска должны быть проанализированы для оценки соответствия их структуры и содержания, а также оценки их влияния на повышения ценности организации в соответствии с поставленными целями. Если результаты анализа и мониторинга показывают, что могут быть осуществлены улучшения, то они должны быть внедрены как можно скорее.

Организации, внедрившие ИСО 31000, должны быть ориентированы на постоянный поиск и внедрение возможностей для улучшения. Действия, используемые в процессе перехода, также могут быть полезны для осуществления периодических проверок отклонений от процесса.

Существуют различные способы внедрения постоянного улучшения, включая следующие:

- обычный мониторинг и анализ структуры менеджмента риска и процесса менеджмента риска, которые идентифицируют возможности улучшения;
- новые знания, к которым получен доступ;
- существенные изменения во внутренней и внешней среде организации.

Приложение А
(справочное)

Основные концепции и принципы

А.1 Общие положения

В настоящем приложении приведено объяснение некоторых терминов и концепций (например, «риск»), применяемых в ежедневной практике, которые имеют особое значение в ИСО 31000 и настоящем стандарте.

ИСО 31000 определяет риск как «влияние неопределенности на цели».

Примечание — Целесообразно, чтобы пользователи настоящего стандарта ознакомились с терминами и определениями в данном приложении.

А.2 Риск и цели

Организации всех типов сталкиваются в своей работе с внутренними и внешними факторами и воздействиями, которые могут повлиять на срок и степень достижения поставленных целей. Воздействие неполной информации об этих факторах на цели организации является риском.

Цели, упомянутые в ИСО 31000 и настоящем стандарте, — это результаты, к которым стремится организация. Как правило, эти цели выражают намерения и стремления организации и отражают ее явные и неявные задачи, ценности и приоритеты с учетом социальных обязательств, законодательных и обязательных требований. Обычно управление риском становится более простым, если цели выражены в измеримых величинах. Часто бывает, что организация устанавливает разнообразные цели, при этом несогласованность целей может стать дополнительным источником риска.

Вероятность (шанс) — это не только возможность появления события, но и реализации последствий события, а также значимость последствий (положительных и/или отрицательных). Как правило, существует диапазон возможных последствий события, и каждому из них соответствует собственная вероятность. Уровень риска может быть выражен как вероятность возникновения особых последствий (включая диапазон). Последствия связаны непосредственно с целями и возникают, когда какие-то события происходят или не происходят.

Риск — это влияние неопределенности на достижение цели независимо от конкретной области или обстоятельств, поэтому событие или опасность (или другой источник риска) не должны быть описаны как риск. Риск должен быть описан как комбинация вероятности возникновения события (или опасности, или источника риска) и его последствий.

Понимание того, что у риска могут быть положительные или отрицательные последствия, является центральной и жизненно важной концепцией, которая должна быть понята руководством организации. Риск может принести организации опасности и/или возможности.

Риск может быть создан или изменен после принятия решения. Поскольку почти всегда существует некоторая неопределенность, связанная с принятием решений, то почти всегда существует риск. Ответственные за достижение целей должны понимать, что риск является неизбежной частью работы организации, при этом риск может возникнуть или измениться после принятия решения. Риск, связанный с принятием решений, должен быть понят при принятии решения, такой риск является преднамеренным. Это становится возможным при использовании процесса менеджмента риска, описанного в ИСО 31000.

А.3 Неопределенность

Неопределенность, которая вместе с целями вызывает риск, возникает во внутренней и внешней среде работы организации. Неопределенность может быть вызвана:

- последствиями основных социологических, психологических и культурных факторов, связанных с поведением человека;
- воздействиями естественных (природных) процессов, которые характеризуются присущей им изменчивостью, например, погоды, изменениями наблюдений в совокупностях;
- результатом неполной или неточной информации, например, из-за утерянных, измененных, ненадежных, внутренне противоречивых и/или недоступных данных;
- изменениями во времени, например, из-за конкуренции, трендов, новой информации, изменений основополагающих факторов;
- разным восприятием воздействия неопределенности в различных подразделениях организации и заинтересованных лиц.

А.4 Обработка и управление риском

Обработка риска — это действия, выполняемые организацией для изменения риска, которые позволяют достичь поставленных целей.

Обработка риска может изменить риск путем изменения источника опасного события (например, применение методов управления позволяет более точно определить вероятность реализации события) или изменения диа-

пазона возможных последствий и места, где они могут произойти. Обработка риска в соответствии с ИСО 31000 является процессом, который направлен на изменение и/или разработку средств управления и включает сохранение риска.

А.5 Структура менеджмента риска

Структура менеджмента риска связана с действиями в рамках системы менеджмента организации (включая методы, процессы, системы, ресурсы и культуру), которые позволяют управлять риском.

Характеристики структуры менеджмента риска и степень ее интеграции в систему менеджмента организации в конечном счете определяют эффективность менеджмента риска.

Структура должна включать четкие заявления со стороны высшего руководства о намерении организации относительно менеджмента риска (описанные в ИСО 31000 как полномочия и обязательства) и поддержке (ресурсы и возможность), направленной на достижение этого намерения.

Возможности не существуют как единичная система или элемент. Возможности включают многочисленные элементы, интегрированные в общие процессы менеджмента организации. Они могут быть уникальными с точки зрения задач управления риском (например, создание специализированной информационной системы) и/или могут быть аспектами системы менеджмента организации (например, применение методов управления человеческими ресурсами).

А.6 Критерии риска

Критерии риска — это параметры, установленные организацией, которые позволяют описывать риск и принимать решения относительно уровня риска с учетом отношения организации к риску. Эти решения позволяют оценить риск и выбрать способы его обработки.

А.7 Менеджмент, менеджмент риска и управление риском

Менеджмент включает скоординированные действия, которые позволяют руководить и управлять организацией для достижения поставленных целей.

Менеджмент риска — это составной компонент менеджмента организации, поскольку включает скоординированные действия, связанные с воздействием неопределенности на поставленные цели. Именно поэтому для обеспечения результативности менеджмента риска необходима максимальная интеграция этого процесса в систему менеджмента и процессы организации.

Приложение В
(справочное)

Применение принципов ИСО 31000

В.1 Общие положения

Все организации управляют риском в той или иной степени, поэтому в стандарте ИСО 31000:2009 установлены одиннадцать принципов, которые необходимо внедрить для обеспечения эффективности менеджмента риска. В принципах менеджмента риска приведены:

a) разъяснения относительно эффективного управления риском (например, менеджмент риска создает и защищает ценность организации);

b) характеристики менеджмента риска, которые позволяют менеджменту риска быть эффективным (например, принцип b), который определяет, что менеджмент риска — неотъемлемая часть всех процессов организации).

В стандарте ИСО 31000 каждый принцип представлен в виде двух частей: краткого заголовка и его подробного разъяснения.

При разработке целей менеджмента риска организации необходимо учитывать все одиннадцать принципов, однако, значение отдельных принципов может быть изменено в соответствии с особенностями применения их в конкретной ситуации.

Успешное внедрение этих принципов влияет на результативность и эффективность менеджмента риска в организации. Всегда должны быть учтены все одиннадцать принципов, даже при том, что значение отдельных принципов менеджмента риска может быть изменено исходя из особенностей рассматриваемой части структуры и ее применения.

Несмотря на то, что принципы изложены кратко, значение каждого из них должно быть понято, чтобы обеспечить их непрерывное выполнение.

В дальнейшем результаты этого вида анализа должны быть учтены при разработке и/или улучшении структуры менеджмента риска (например, при распределении ответственности и полномочий, предоставлении обучения, обмене информацией с заинтересованными лицами, разработке и проведении непрерывного мониторинга и анализа реализации менеджмента риска).

В данном приложении приведено описание способов применения каждого принципа, при этом для некоторых из них приведены практические рекомендации по их применению.

В.2 Принципы

В.2.1 Менеджмент риска создает и защищает ценность

В.2.1.1 Принцип

a) менеджмент риска создает и защищает ценность

Менеджмент риска 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.

В.2.1.2 Как применять принцип

Данный принцип помогает понять, что цель менеджмента риска состоит в создании и защите ценности организации, и помочь в реализации ее целей. Внедрение этого принципа необходимо, чтобы помочь организации идентифицировать факторы (внутренние и/или внешние), которые инициируют и создают неопределенность, воздействующую на достижение целей организации и управлять ими.

Взаимосвязь между результативностью менеджмента риска и достижением успеха организации необходимо явно продемонстрировать и довести до сведения всех вовлеченных сторон. Данный принцип разъясняет, что риском нельзя управлять ради него самого, но необходимо управлять ради достижения поставленных целей организации и их превышения.

Некоторые показатели и их значения трудно измерить (например, в денежном выражении), но они могут в значительной степени способствовать повышению производительности, улучшению репутации и соответствию законодательным и обязательным требованиям. Человеческие, социальные и экологические ценности особенно важны при управлении безопасностью и обеспечением здоровья людей и связанным риском, а также при управлении нематериальными активами, поэтому для описания таких ценностей необходимо использовать качественные, а не количественные показатели.

B.2.2 Менеджмент риска — неотъемлемая часть всех процессов организации

B.2.2.1 Принцип

b) Менеджмент риска — неотъемлемая часть всех процессов организации.

Менеджмент риска — не автономное действие, которое является отдельным от основных видов деятельностей и процессов организации. Менеджмент риска — часть обязанностей менеджмента и неотъемлемая часть всех организационных процессов, включая стратегическое планирование и процессы управления проектом и управления изменениями.

B.2.2.2 Как применять принцип

Действия организации, включая принимаемые решения, вызывают риск. Изменения во внешней среде, которые неподконтрольны организации, могут инициировать появления нового риска. Все действия и процессы организации происходят во внутренней и внешней среде, в которой присутствует неопределенность. Из этого следует, что:

a) структура менеджмента риска должна быть реализована путем интеграции ее компонентов в общую систему менеджмента и в процесс принятия решений организации, независимо от того, является система менеджмента организации документированной или нет; существующие процессы менеджмента могут быть улучшены путем внедрения положений стандарта ИСО 31000;

b) процесс менеджмента риска должен быть неотъемлемой частью действий, создающих риск; если риск понят организацией после принятия решения, то необходимо изменить принятое решение;

c) если документированной системы менеджмента организации не существует, то структура менеджмента риска может служить основой для ее создания.

Если менеджмент риска не интегрирован в другую деятельность и процессы менеджмента, то эта деятельность может быть воспринята как дополнительная административная задача или бюрократическое нововведение, которое не создает и/или не защищает ценность.

Существует два основных метода применения принципа:

- в процессе разработки (включая поддержку и улучшение) структуры менеджмента риска;
- при применении процесса менеджмента риска к принятию решений и связанным действиям.

Метод выражения намерений организации (т. е. полномочий и обязательств) в области менеджмента риска должен быть аналогичен выражению других намерений (см. приложение С). Везде, где применимо, компоненты структуры менеджмента риска должны быть включены в компоненты существующих систем менеджмента (см. приложение Е и ИСО 31000).

Аудиторские компании могут играть важную роль при анализе способов принятия решения руководством, а также анализа применения процесса менеджмента риска.

B.2.3 Менеджмент риска — часть принятия решений

B.2.3.1 Принцип

c) Менеджмент риска — часть принятия решений.

Менеджмент риска помогает лицам, принимающим решения, сделать информированный выбор, расположить по приоритетам действия и сделать выбор между альтернативными планами действий.

B.2.3.2 Как применять принцип

Данный принцип показывает, что менеджмент риска лежит в основе принятия обоснованного решения. Менеджмент риска должен быть интегрирован в действия, поддерживающие достижение целей, и процесс принятия решений. В процессе принятия решений следует последовательно оценивать риск и, если необходимо, его обрабатывать. Принятие или непринятие решений включает риск и важно осознавать риск в обеих ситуациях.

Менеджмент риска должен быть частью принятия решения. Риск следует учитывать заранее (превентивно) до принятия решения, а не по факту принятия решения. Например, следующим образом:

- решения о стратегических проблемах должны учитывать неопределенность при изменениях факторов внешней среды и изменений ресурсов организации;
- процесс инноваций должен не только учитывать неопределенность, которая определяет успех инноваций, но также риск, связанный с человеческими, социальными, экологическими аспектами инноваций, требованиями безопасности и соответствия законодательным и обязательным требованиям (например, безопасность товаров);
- в планах относительно большого объема инвестиций должны быть определены этапы принятия решений, на которых следует проводить оценку риска.

В политике организации в области менеджмента риска и обмена информацией о нем должен быть отражен данный принцип.

В других частях структуры организации следует учитывать способ принятия решения, так чтобы процесс на всех этапах принятия решения был эффективным и последовательным, например, при управлении проектом, инвестиционной оценке или закупках.

Ответственные за принятие решений на всех уровнях и во всех подразделениях организации должны понимать политику в области менеджмента риска организации и должны обладать необходимой компетентностью, чтобы эффективно применять процесс менеджмента риска при принятии решений. При этом необходимо четко распределить ответственность и полномочия, обеспечить профессиональное обучение и проводить анализ выполнения работы.

Практическая помощь

Для достижения максимального эффекта от применения данного принципа необходимо с самого начала подробно ответить на следующие вопросы:

Как принцип может помочь создать и защитить ценность?

Как и где в организации принимают решения?

Кто вовлечен в принятие решений?

Какие знания и навыки необходимы для тех, кто принимает решения, чтобы сделать менеджмент риска частью принятия решений?

Как лица, принимающие решения, приобретают знания и навыки, в которых они нуждаются?

Какое руководство и поддержка необходимы для существующего персонала?

Как будущий персонал при введении в должность будет обучен методу принятия решений?

Как будут затронуты интересы внешних заинтересованных лиц?

Что необходимо изменить в процессах принятия решений в организации?

Как проводить мониторинг прогресса в реализации этого принципа?

B.2.4 Менеджмент риска явным образом связан с неопределенностью

B.2.4.1 Принцип

d) Менеджмент риска явным образом связан с неопределенностью.

Менеджмент риска четко учитывает неопределенность, характер этой неопределенности и способы ее обработки

B.2.4.2 Как применять принцип

Процесс менеджмента риска уникален среди других типов менеджмента тем, что связан с воздействием неопределенности на поставленные цели. Риск можно оценить и успешно обработать только в случае, если поняты особенности и источник неопределенности.

Организация должна рассмотреть неопределенность всех типов, при этом нельзя ее недооценивать или переоценивать.

Направленность на анализ неопределенности важна также при выборе способов обработки риска, анализе воздействия и надежности методов управления. Также следует учитывать неопределенность, связанную с поддержкой процесса менеджмента риска, например, оценки успешности передачи информации при проведении консультаций с заинтересованными сторонами или оценки достаточности выбранных интервалов мониторинга для выявления изменений.

Лица, вовлеченные в управление риском, должны понимать значение неопределенности, типы и источники неопределенности. Количество и виды методов оценки риска, направленных на снижение неопределенности, должны соответствовать важности принимаемого решения, при этом предпочтительно применять разнонаправленные методы.

Предположения, на основе которых приняты решения, должны быть зарегистрированы в процессе менеджмента риска (ИСО 31000:2009, пункт 5.7). Предположения обычно отражают некоторую форму неопределенности. Неопределенность, выявленная на различных этапах процесса, должна быть учтена.

При оценке риска важно оценить неопределенность, связанную с оценкой и ранжированием вероятности и последствий.

В процессе анализа риска и предполагаемой обработки риска необходимо исследовать чувствительность, т. е. фактическое влияние неопределенности на риск.

Практическая помощь

Лица, принимающие решения, должны, прежде всего, выяснить: «Каковы предположения в данном случае?» и «Как неопределенность связана с предположениями?». Эта практика не должна быть ограничена формальными оценками риска, например, она может быть применена при прогнозировании.

- При анализе внутренней и внешней среды организации при определении области применения, необходимо исследовать и учесть все особенности, связанные с высокой изменчивостью. Это источники неопределенности. Следует определить способы непрерывного мониторинга и анализа этих особенностей.

Если неопределенность существует только в пределах известного диапазона, то необходимо следить за значением неопределенности в данном диапазоне.

В.2.5 Менеджмент риска является систематическим, структурированным и своевременным

В.2.5.1 Принцип

e) Менеджмент риска является систематическим, структурированным и своевременным.

Систематический, регулярный и структурированный подход к менеджменту риска способствует эффективности и устойчивым, сравнимым и надежным результатам.

В.2.5.2 Как применять принцип

Последовательный подход к управлению риском в процессе принятия решения помогает обеспечить эффективность работы и создает атмосферу доверия и успеха в организации. Для этого необходимо применение организационных методов, которые позволяют учитывать риск, связанный со всеми принятыми решениями, и использовать последовательные критерии риска, связанные с достижением целей организации и соответствием области применения ее деятельности.

Своевременный подход показывает, что процесс менеджмента риска применен в оптимальной точке в процессе принятия решений. Частично, это зависит от разработанной структуры, к которой также применяют этот принцип. Если соображения относительно риска сделаны слишком рано или слишком поздно, а также если возможности, связанные со снижением риска, упущены, то могут потребоваться существенные затраты, связанные с пересмотром решения. Необходимо оценить и понять зависимость от времени учета риска, чтобы определить наиболее эффективный подход к менеджменту риска.

Структурированный подход подразумевает применение процесса менеджмента риска так, как описано в ИСО 31000:2009, пункте 5, включая подготовку к этим действиям. В зависимости от своих потребностей организация должна совместить принятые методы управления риска с методами менеджмента (например, метод снизу вверх или сверху вниз на соответствующем уровне менеджмента организации).

В.2.6 Менеджмент риска основан на наилучшей доступной информации

В.2.6.1 Принцип

f) Менеджмент риска основывается на наилучшей доступной информации.

Входные данные для процесса менеджмента риска основаны на таких источниках информации, как исторические данные, опыт, обратная связь от заинтересованных сторон, наблюдения, прогнозы и экспертные оценки. Однако лица, принимающие решения, должны принимать во внимание любые ограничения данных и моделирования, а также возможности расхождений мнений среди экспертов.

В.2.6.2 Как применять принцип

Для организации важно получить наилучшую доступную информацию, чтобы иметь правильное понимание риска. Следовательно, мероприятия менеджмента риска должны включать методы (например, исследование) сбора и генерирования информации. Однако, несмотря на предпринимаемые усилия, иногда доступная информация может быть ограничена, например, ожидания относительно будущих событий могут быть ограничены использованием методов статистического прогнозирования.

Организация должна понять чувствительность решений по отношению к неопределенности информации. Достоверность оценки риска зависит, частично, от точности и прецизионности критериев риска. Сбор данных, связанных с риском, (например, данных о возникновении инцидентов и другой информации, полученной на фактических данных) может помочь при статистическом прогнозировании.

На практике основной целью часто становится принятие решений на основе фактических данных, хотя это не всегда возможно по времени или доступным ресурсам. В таких ситуациях выводы на основе экспертных оценок необходимо объединять с доступной информацией. При этом необходимо избегать смещения в сторону экспертных оценок. Кроме того, на основе прошлых данных не всегда возможен точный прогноз. В ситуациях с потенциально высокими последствиями отсутствие информации может иметь немедленное действие, если есть доказательства возможного вреда, а не безусловного доказательства наличия вреда.

Этот принцип также применим при разработке (или улучшении) структуры менеджмента риска, поскольку существуют аспекты структуры, которые могут определить успех использования этого принципа. Например, аспекты, связанные с обеспечением возможности исследования или связанные со сбором, анализом, обновлением и доступностью информации, необходимой для осуществления процесса.

Достоверность и точность информации необходимо регулярно анализировать для обеспечения ее адекватности, своевременности и достоверности в соответствии с зарегистрированными предположениями. Необходимо обеспечить периодический анализ, а также пересмотр или коррекцию структуры менеджмента риска по проблемным вопросам.

Практическая помощь

При разработке и проектировании способов обмена информацией об инцидентах необходимо сначала тщательно рассмотреть цели использования информации. Определить, при решении каких вопросов может помочь эта информация, кто настоящие и будущие ее конечные пользователи, как необходимо сортировать информацию, как повысить степень совместимости информации, как можно получить доступ к информации. После ответа на эти вопросы целесообразно разработать форму отчетности с учетом воздействий изменений на качество полученной информации в долгосрочном периоде.

Необходимо описать область применения информации (включая регистрацию даты разработки или изменения), которая должна стать частью более подробных и документированных описаний ключевых рисков (например, реестра риска). Это позволяет пользователям реестра риска учесть изменения области применения, которые могут произойти впоследствии при возникновении изменений риска.

Если при оценке используют предположения, то пояснения относительно этих предположений, включая все ограничения, должны быть точно зарегистрированы и поняты.

При разработке способов обработки риска необходимо определить, как будет проводиться мониторинг применения средств контроля методов управления, как результаты мониторинга могут стать доступны лицам, принимающим решения и использующим такие средства.

B.2.7 Менеджмент риска является адаптируемым

B.2.7.1 Принцип

g) Менеджмент риска является адаптируемым.

Менеджмент риска должен соответствовать внешней и внутренней области применения (среде) и профилю риска.

B.2.7.2 Как применять принцип

В стандарте ИСО 31000 изложен общий подход к созданию менеджмента риска, применимый ко всем типам организаций и всем типам риска. Каждая организация имеет культуру, показатели, критерии риска и область применения деятельности. Менеджмент риска должен учитывать особенности организации и удовлетворять ее потребностям.

Нет никакого единственно правильного способа разработки и реализации структуры и процессов менеджмента риска, поскольку необходимы гибкость и адаптация для каждой организации. При разработке следует учитывать многие аспекты, включая размер, культуру, сферу деятельности, конфигурацию и стиль управления организации.

Различные виды риска могут потребовать разработки и применения различных специализированных процессов в организации. Процессы менеджмента риска должны соответствовать требованиям ИСО 31000, при этом могут быть различия в системах, моделях и уровне применяемых оценок риска (например, при оценке риска, связанного с информационными технологиями (ИТ), инвестиционного риска или риска, связанного с конкурентами). Каждый процесс должен быть адаптирован для определенной цели.

Основная цель структуры состоит в обеспечении применимости процесса менеджмента риска к принятию решений наиболее эффективным способом, который отражает политику организации. При этом в разработанной структуре необходимо отразить место и способы принятия решений, учесть законодательные требования или другие внешние обязательства организации.

Важно иметь в виду, что адаптация не подразумевает различия в элементах структуры (см. пункт 5 ИСО 31000:2009) или этапах процесса (см. пункт 5 ИСО 31000:2009). Все они важны для эффективного менеджмента риска.

Данный принцип важен во время разработки и улучшения структуры менеджмента риска, а также при определении способов структурирования аспектов процесса.

Данный принцип может также показать, что организация должна исследовать внутренние проблемы, например, текучесть кадров (если этот показатель высокий, то может потребоваться применение соответствующих средств корректировок, чтобы обеспечить выполнение всеми новыми работниками требований менеджмента риска).

Адаптивность структуры необходима для достижения интеграции с процессами принятия решений организации. При этом необходимо изменение процессов принятия решений, чтобы соответствовать модифицированной структуре менеджмента риска.

Практическая помощь

При разработке структуры менеджмента риска необходимо определить вовлеченных лиц и учесть их требования и потребности.

- Работа над более глубоким пониманием основных понятий ИСО 31000 может помочь обеспечить необходимые охват, структуру и процесс менеджмента риска в соответствии с альтернативными признаками эффективного менеджмента риска, приведенными в ИСО 31000:2009, приложение А. Наоборот, поверхностное понимание не приведет к этой цели.

В.2.8 Менеджмент риска учитывает человеческие и культурные факторы

В.2.8.1 Принцип

h) Менеджмент риска учитывает человеческие и культурные факторы.

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

В.2.8.2 Как применять принцип

Данный принцип помогает учесть представления и потребности заинтересованных лиц. При этом необходимо понимать, что на такие представления и потребности могут оказывать влияние социальные, культурные и иные характеристики. Анализируемые факторы должны включать социальные, политические и культурные аспекты, а также концепцию времени. Общие типы ошибок включают следующее:

a) отказ обнаружить ранние признаки опасности и реагировать на них;

b) безразличие к мнениям людей или отсутствие знаний о них;

c) использование упрощенных стратегий обработки информации и не желание работать со сложными вопросами;

d) отказ признать сложность проблемы.

При разработке структуры и применении всех аспектов процесса менеджмента риска необходимо установить требования, чтобы понять и использовать в работе человеческие и культурные факторы.

Разработка структуры и обмен информации о риске должны учитывать культурные характеристики и уровни знаний аудитории.

Практическая помощь

Руководители должны своими действиями показывать, что они способствуют и поддерживают уважение и понимание индивидуальных различий людей.

Люди ценят, когда спрашивают их мнение.

Как правило, организации вознаграждают за то, что для них ценно. Если выбор, поощрение и вознаграждение работников напрямую не связаны с фактическим выполнением работ в области менеджмента риска, то маловероятно, что такая работа будет соответствовать стандартным требованиям к менеджменту риска. Усилия людей должны быть признаны и оценены.

Как правило, неблагоразумно полагаться только на единоличное управление, необходимо привлечение различных мнений, чтобы работать с риском.

Для транснациональных корпораций благоразумно признать значение культуры при определении поведения людей.

Практическая помощь

Ниже приведены примеры полезных вопросов относительно человеческих и организационных факторов:

Структура организации соответствует потребностям организации?

Формально ответственные лица точно идентифицированы?

Все должностные инструкции содержат точный перечень ответственности и полномочий работников?

Действительно ли все каналы обмена информацией точны и эффективны?

Иногда необходимо проверить правильность понимания и интерпретации обмена информацией на всех уровнях в организации?

Проводят ли в организации мониторинг морального климата ?

Проводят ли анализ форм взаимодействия между командами?

Существуют ли способы получения и признания слухов, а также способы реагирования на них в организации, достаточно ли этих способов, чтобы не допустить отрицательного воздействия слухов?

Существует ли четкое определение, пересмотр и содействие политике?

Если в политике есть проблемы, необходим ли анализ процесса?

Придерживается ли организация политики и процедур? Если нет, необходим ли дополнительный анализ? Они внедрены в жизнь?

Привлекают ли внутренних и внешних аудиторов к выявлению опасного или неэтичного поведения работников в организации?

В.2.9 Менеджмент риска является прозрачным и учитывает интересы заинтересованных сторон

В.2.9.1 Принцип

i) Менеджмент риска является прозрачным и учитывает интересы заинтересованных сторон.

Соответствующее и своевременное вовлечение заинтересованных сторон и, в частности, лиц, принимающих решения, на всех уровнях организации обеспечивает, что менеджмент риска 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.

B.2.9.2 Как применять принцип

Данный принцип может воздействовать на разных уровнях. Этот принцип может быть отражен в политике в области менеджмента риска организации (например, «Мы будем информировать и консультироваться с заинтересованными сторонами везде, где возможно, чтобы они понимали наши цели и могли выразить свои знания и представления, которые могут помочь при принятии решений нашей организации»).

Консультации с заинтересованными сторонами являются частью этапа внедрения процесса менеджмента риска и их необходимо планировать и относиться к этому очень аккуратно. Именно здесь доверие может быть построено или разрушено. Для обеспечения эффективности и повышения уверенности в результатах, соответствующие заинтересованные стороны должны быть вовлечены во все аспекты процесса менеджмента риска, включая разработку процесса консультаций и обмена информацией.

При внедрении данного принципа необходимо учитывать проблемы, связанные с конфиденциальностью, безопасностью и частной жизнью, например, доступ к отдельным пунктам реестра риска может быть ограничен.

Практическая помощь

При обучении менеджменту риска могут быть использованы ролевые игры, связанные с обучением обмену информацией и консультациям по подготовке кадров в области менеджмента риска.

Необходимо оценить самочувствие лиц, получающих информацию.

Необходимо обеспечить регулярную обратную связь, чтобы продемонстрировать эффективность процесса на практике.

Необходимо поощрять выявление новых мнений, эти мнения и представления следует поощрять, признавать, ценить, и везде, где применимо, необходимо обеспечить обратную связь о них.

B.2.10 Менеджмент риска является динамичным, итеративным и реагирующим на изменения

B.2.10.1 Принцип

j) Менеджмент риска является динамичным, итеративным и реагирующим на изменения.

Менеджмент риска непрерывно распознает изменения и реагирует на них. Как только происходит внешнее или внутреннее событие, область применения или знания изменяются, необходимо проводить мониторинг и пересмотр рисков, при этом новые риски появляются, некоторые изменяются, другие исчезают.

B.2.10.2 Как применять принцип

Все изменения в целях организации или аспектах внутренней или внешней среды неизбежно влияют на риск (например, внутреннее изменение структуры, появление нового главного поставщика или изменение в законодательстве). Аналогично изменения в области деятельности организации (например, приобретение другой компании, или заключение нового основного контракта) могут потребовать изменений в структуре менеджмента риска (например, в обучении). Процессы менеджмента риска должны быть разработаны с учетом динамики изменений организации (например, скорости изменения).

В стандарте ИСО 31000 изложено два режима мониторинга и анализа (для структуры и процесса). Каждый из них предназначен для своей цели и каждый требует осмысления и реализации.

Организация должна проводить мониторинг и анализ структуры для обеспечения соответствия принципам менеджмента риска, политике в области менеджмента риска и поддержки применения процесса принятия решений.

Необходимо включать мониторинг и анализ в каждый из основных этапов процесса менеджмента риска.

Организация должна проводить анализ своих методов управления риском, чтобы обеспечить их непрерывную результативность при реагировании на изменения. Например, эффективность методов управления зависит от их применения квалифицированными специалистами, поэтому при значимых изменениях в составе персонала такие средства могут стать неэффективными.

Организация должна тщательно адаптировать процессы мониторинга и анализа, в особенности они должны быть чувствительны к факторам изменения, которые могут оказать наибольшее воздействие. В процессе мониторинга и анализа необходимо оценить значения контролируемых показателей. При этом необходимо актуализировать такие показатели при возникновении изменений или новых обстоятельств.

Мониторинг и анализ — это уникальные виды деятельности (см. ИСО 31000:2009, пункты 4.5 и 5.6). Мониторинг связан с непрерывным наблюдением за основными параметрами для определения их соответствия установленным требованиям. Анализ проводят периодически, он должен быть структурирован относительно его цели и предназначен для определения актуальности предположений, на основе которых были приняты решения (т. е. разработана структура). Анализ должен также учесть внедрение новых знаний и технологий.

Практическая помощь

При применении процесса менеджмента риска и разработке заявления об области применения этого процесса, компоненты, которые наиболее вероятно подвергнутся изменению (например, особенности внешней среды), должны быть идентифицированы, следует также проводить мониторинг их изменения. Выявленные изменения могут потребовать переоценки отдельных или всех документированных рисков.

Работников необходимо поощрять, сообщать о беспокойстве по поводу существующего положения вещей (включая информацию о разоблачениях).

Даже небольшие организации должны учитывать глобальные изменения, например, глобальный финансовый кризис 2008 глубоко повлиял на некоторых небольших поставщиков, главными потребителями которых были организации, связанные прямо или косвенно с банкротством банка. Такие внешние события или обстоятельства могут потребовать превентивных изменений структуры менеджмента риска.

В.2.11 Менеджмент риска способствует постоянному улучшению организации

В.2.11.1 Принцип

k) Менеджмент риска способствует постоянному улучшению организации.

Организации должны разрабатывать и применять стратегии улучшения менеджмента риска одновременно с улучшением других аспектов своей деятельности.

В.2.11.2 Как применять принцип

Постоянное улучшение эффективности работы организации взаимосвязано с постоянным улучшением процесса менеджмента риска. Усовершенствованный процесс менеджмента риска, который основан на оценке риска принимаемых решений, может помочь снизить неопределенность в достижении целей, минимизировать изменчивость и повысить адаптивность организации. Однако необходимо следить, чтобы процесс менеджмента риска не был переусложнен. Менеджмент риска не должен проводиться на грани возможностей и гибкости реагирования.

Данный принцип особенно важен для организаций, которые опасаются использовать новые возможности для улучшения деятельности. Такие возможности могут возникнуть внутри (например, опыт реагирования на инциденты) или вне (например, появление новых инструментов и знаний, способных улучшить менеджмент риска) организации.

Данный принцип связан с непрерывным поиском возможностей повышения эффективности менеджмента риска, например, внедряя новые информационные технологии при принятии решений.

Цели постоянного улучшения должны быть установлены в политике в области менеджмента риска организации. Необходимо проводить непрерывный формальный и неформальный обмен информацией об этих целях. Постоянное улучшение может включать следующее:

- улучшение степени интеграции деятельности в области менеджмента риска в общую деятельность организации;
- повышение качества оценки риска;
- улучшение структуры, например, повышение качества и улучшение доступности информации;
- повышение скорости принятия решений.

Постоянное улучшение основано на использовании качественных и количественных показателях улучшения. Если в работе использованы поэтапные подходы и модели зрелости, то необходимо разработать показатели постоянного улучшения, которые основаны на ресурсах и культуре организации. Необходимо признать, что зачастую в основе успеха лежат многочисленные попытки человека добиться улучшения. Цели эффективного менеджмента риска направлены исключительно на повышение вероятности того, что организация полностью достигнет своих целей. Чем быстрее организация сможет достигнуть эффективного менеджмента риска, тем более эффективно она сможет достичь поставленных целей.

На практике, для достижения некоторых улучшений может потребоваться время, например, может возникнуть необходимость в дополнительном бюджетировании и планировании. При планировании улучшений необходимо расставить приоритеты, ранжировать выгоды и организовать проведение мониторинга реализации улучшений в организации.

Практическая помощь

При использовании мониторинга и анализа элементов структуры необходимо проводить ежегодный анализ выполнения принципов менеджмента риска и внедрения улучшений.

Организация должна оценить и проанализировать соответствие, пригодность и эффективность структуры менеджмента риска.

Необходимо использовать систему отчетности об инцидентах, чтобы провести анализ их причины. При этом необходимо исследовать не только текущие причины инцидента, но также провести анализ особенностей структуры менеджмента риска, которая позволила инциденту произойти.

Организация должна проводить мониторинг достижений (например, проект выполнен вовремя в рамках выделенного бюджета), чтобы понять, какие особенности структуры менеджмента риска позволили добиться успеха и могут быть использованы для укрепления успеха в будущем.

Приложение С
(справочное)

Способы выражения полномочий и обязательств

С.1 Общие положения

В данном приложении приведены руководящие указания и стратегии реализации полномочий и обязательств, а также способы обмена информацией о них в организации.

Для того чтобы полномочия и обязательства были эффективными, высшее руководство и контролирующие органы организации должны четко описать заинтересованным сторонам свой подход к менеджменту риска, документированию и обмену информацией о соответствующих полномочиях и обязательствах. Полномочия в области менеджмента риска, как правило, приводит к изменению в деятельности, культуре, политике, процессах и способах выполнения работ в области менеджмента риска, которые должны быть отражены в структуре менеджмента риска. Полномочия и обязательства могут быть изложены в кратком заявлении, которое должно быть широко распространено.

Разработка полномочий включает принятие решения о направлении действий и определение ответственных за их выполнение. В существующих организациях разработка полномочий влечет за собой изменения. При идентификации направления действий одновременно необходимо определить обязательства по их выполнению.

Полномочия и обязательства — это фундаментальная часть структуры менеджмента риска. Полномочия и обязательства должны быть частью менеджмента организации и структуры и должны быть учтены при их разработке.

Полномочия и обязательства должны отражать одиннадцать принципов менеджмента риска, изложенных в ИСО 31000:2009, пункт 3.

На практике полномочия и соответствующие обязательства организации могут быть выражены и восприняты явным и неявным способом. Неявные способы выражения (например, ежедневные действия высшего руководства и контролирующих органов, и способы действий, преобладающие в культуре организации), как правило, обеспечивают более сильный стимул, чем явные способы выражения (например, документированная политика в области менеджмента риска).

С.2 Методы представления полномочий и обязательств

С.2.1 Ключевые характеристики

Полномочия и обязательства должны соответствовать следующим критериям:

a) быть совместимыми со стратегическим планом, целями, политиками, способами обмена информацией и системой менеджмента организации;

b) быть совместимыми с критериями риска, определенными контролирующими органами;

c) соответствовать принципам ИСО 31000 и быть направленными на улучшение менеджмента риска в соответствии с ИСО 31000:2009 (приложение А);

d) обеспечивать простоту обмена информацией и проверку на понимание внутри и вне организации;

e) иметь обоснованные ожидания успешного выполнения;

f) быть ориентированными на обязанности владельцев риска.

Если существующие полномочия и обязательства организации в области менеджмента риска уже не соответствуют перечисленным критериям, следует провести явные и неявные необходимые изменения.

Пример — Если контролирующим органом или высшим руководством принято решение, в отношении которого была проведена оценка риска, это является признаком того, что организация приняла на себя обязательства по пониманию этого риска.

Существенной частью адаптации пересмотренных полномочий является разработка плана по изменению понимания требований. Цель этого плана состоит в обеспечении того, что полномочия и преимущества от их выполнения широко поняты, в них верят, а также то, что организация последовательно добивается осуществления этих полномочий. Действия организации, их сравнение с заявлениями о полномочиях имеют наибольшее воздействие на принятие их различными заинтересованными сторонами.

С.2.2 Установление политики и обязательств в области менеджмента риска и обмен информацией о них

Одним из основных способов выражения полномочий и обмена информацией о них явным способом является установление политики в области менеджмента риска и обмен информацией о ней. В ИСО 31000:2009, пункт 4.3.2 определено, что организация должна не только точно установить свою политику в области менеджмента риска, но также проводить обмен информацией о ней внутри и вне организации. В ИСО 31000:2009, пункт 4.3.2 также идентифицированы специальные положения, которые обычно отражены в политике в области менеджмента риска.

Способы выражения политики должны соответствующим образом учитывать принцип менеджмента риска g) (менеджмент риска должен быть адаптируемым) и быть совместимы с общим направлением развития органи-

зации. В противном случае политика в области менеджмента риска не может рассматриваться как часть общей системы, в которой работает организация.

Для более крупных организаций принятие политики обычно подразумевает разработку формального заявления о полномочиях в области менеджмента риска. Такая политика входит составной частью в общий набор политик и утверждается высшим руководством. Обмен информацией о политике в области менеджмента риска и усиление этой политики необходимо проводить посредством системы менеджмента организации.

Практическая помощь

Вовлечение высшего руководства и контролирующих органов и принятие ими соответствующих обязательств являются ключевыми факторами для успеха программ менеджмента риска. Организация должна рассмотреть следующие вопросы, которые помогают установить соответствующие полномочия и обязательства в области менеджмента риска:

Каковы стратегические цели организации? Действительно ли они ясны? Что является явным и неявным в этих целях?

Насколько высшее руководство понимает природу и значимость рисков, решение по которым оно готово взять на себя, и возможностей, которые оно готово использовать для достижения стратегических целей организации?

Готово ли высшее руководство установить ясное и понятное управление риском в организации?

Какие шаги высшее руководство сделало для обеспечения надзора за менеджментом риска?

При принятии решений руководители и работники понимают степень, до которой им (индивидуально) разрешено представлять организацию с учетом последствий события или ситуации? Отношение к риску должно быть основано на опыте, позволяющем принимать обоснованные решения с учетом риска.

Понимают ли руководители свой суммарный и связанный уровень риска и соответственно могут ли определить приемлемость риска?

Понимают ли высшее руководство и исполнительное руководство суммарный и связанный уровень риска для организации в целом?

Действительно ли специалистам и исполнительному руководству ясно, что отношение к риску не является постоянным? Оно может быть изменено под воздействием изменения конъюнктуры рынка и среды. При одобрении высшим руководством риска необходимо предусмотреть до некоторой степени гибкое отношение к его применению.

При принятии решения полностью ли исследованы последствия? Структура риска должна помочь руководителям, при этом руководители принимают на себя соответствующий уровень риска бизнеса с учетом потенциального вознаграждения.

Какие существенные риски высшее руководство готово принять на себя и какие возможности оно готово использовать? Какие существенные риски высшее руководство не готово принять на себя? Вне зависимости от политики в области менеджмента риска, эта политика должна действовать наравне с другими политиками организации.

Политика должна быть поддержана явными и неявными способами, правильно выражена и соответствовать шести критериям, установленным в С.2.1.

С.2.3 Укрепление приверженности

Высшее руководство и контролирующие органы должны продемонстрировать и укреплять приверженность организации полномочиям и обязательствам в области менеджмента риска с помощью соединения явных и неявных действий, включая следующие:

- прояснение того, что цели в области менеджмента риска могут быть связаны или не связаны с других целями менеджмента;
- прояснение того, что эффективность менеджмента риска связана с постановкой целей организации;
- обеспечение интеграции действий в области менеджмента риска, выполняемых в соответствии с полномочиями, в существующие процессы менеджмента, в том числе процессы стратегического менеджмента, проектирования и оперативной деятельности;
- требование проведения регулярного мониторинга и отчетности о структуре и процессах менеджмента риска организации, обеспечивающих их соответствие и эффективность;
- мониторинг адекватности понимания организацией видов своих рисков, соответствующих установленным критериям, и предпринятых действий по ликвидации последствий в случае несоответствия этим критериям;
- обеспечение принципа лидерства руководства, когда руководитель показывает пример своими действиями;
- возобновление обязательств и полномочий при изменениях сроков, событий и состава высшего руководства.

Стандарт ИСО 31000 может быть внедрен во всей организации или в ее части, например, во вспомогательных подразделениях.

С.3 Руководство по разработке полномочий и обязательств

Установленные полномочия в области менеджмента риска должны быть обдуманными и учитывать стратегические перспективы и результаты консультаций с контролирующими органами и высшим руководством. Это поможет обеспечить осуществление полномочий организацией.

Полномочия и обязательства необходимо анализировать на тактическом и стратегическом уровнях. Организация должна определить и оценить требования к компетентности, навыкам и опыту персонала, провести экспертизу их достижения.

Необходимо внимательно следить за изменениями, происходящими в соответствии с полномочиями в области менеджмента риска. Следить за тем, кто руководит изменениями, и кто нуждается в руководстве и/или поддержке. Иногда изменения могут быть радикальными (например, изменения в требованиях к работе, мониторинге функционирования и процессах управления), поэтому способность организации к изменениям может быть снижена. Изменения необходимо рассматривать в связи с другими изменениями, которые находятся на стадии реализации, и учитывать необходимость их интеграции.

Необходимо проводить консультации с работниками, которые будут в значительной степени затронуты изменениями, в особенности, лицами ответственными за отдельные направления менеджмента риска организации (например, обеспечение здоровья и безопасности людей, менеджмент безопасности). Смысл изменений должен быть понятен персоналу.

Полномочия должны быть четко сформулированы в программном заявлении, которое демонстрирует обязательства организации.

Практическая помощь

Некоторые способы достижения соответствия представлены ниже:

- рассмотрение способов разъяснения полномочий организации и того, как они подкрепляются дальнейшими действиями;
- рассмотрение сроков, влияющих на полномочия (необходимо уважать наравне с другими аспектами деятельности) организации, хотя до тех пор, пока структура менеджмента риска полностью не реализована, преимущества ее внедрения не будут полностью поняты, менеджмент риска не будет столь же эффективен, как мог бы быть);
- идентификация ключевых лиц, ответственных за инициирование необходимых изменений в подходе к менеджменту риска, руководство и внедрение действий по менеджменту риска;
- определение аспектов структуры и действий в области менеджмента риска, для которых необходим мониторинг со стороны высшего руководства, управление мониторингом и сбором и представлением такой информации;
- включение выполнения менеджмента риска в качестве регулярной повестки дня во все ключевые совещания и встречи высшего руководства;
- разработка эффективных методов обмена информацией о работе менеджмента риска (например, публикации информационного бюллетеня для персонала в стиле отчета по менеджменту риска);
- исследование критериев для начала проведения анализа полномочий со стороны руководства.

Приложение D
(справочное)

Мониторинг и анализ

D.1 Общее

D.1.1 Общие положения

Приложение содержит рекомендации по мониторингу и анализу структуры и процессов менеджмента риска в соответствии с ИСО 31000:2009, пункты 4.5, 4.6 и 5.6.

Мониторинг и анализ — два типа действий, направленных на определение достоверности предположений и решений. Эти методы используют для поддержки эффективности функционирования общей структуры менеджмента риска и отдельных этапов процесса менеджмента риска.

Мониторинг включает в себя наблюдение фактического выполнения и сравнение полученных результатов с ожидаемым или требуемым выполнением. Мониторинг включает непрерывную проверку или исследование, экспертное наблюдение, критическое обследование или непрерывное определение статуса, необходимое для идентификации отклонений от уровня выполнения (требуемого или ожидаемого), а также изменений области определения.

Анализ включает периодическую или внезапную проверку текущей ситуации, направленную на выявление изменений в среде, производственных и организационных методах работы. Анализ — это действие, предпринятое для определения пригодности, соответствия и результативности структуры и процесса для достижения поставленных целей. В процессе анализа необходимо рассмотреть результаты, полученные в процессе мониторинга.

Аудит — процесс систематического анализа на основе фактических данных на соответствие установленным критериям. Каждый аудит — это анализ, но не каждый анализ — аудит.

Мониторинг и анализ совместно помогают установить соответствие функционирования менеджмента риска ожидаемым показателям, необходимость улучшений, внедрение изменений, необходимость регулирования или пересмотра структуры или отдельных элементов процесса.

Мониторинг и анализ направлены на обеспечение разумной гарантии того, что риском соответственно управляют, идентифицируют недостатки менеджмента риска и возможности его улучшения. Мониторинг и анализ необходимы для обеспечения понимания организацией своих рисков в соответствии с критериями риска и отношением к риску. Мониторинг и анализ требуют применения системного интегрированного подхода к системе менеджмента организации в целом.

Действия по мониторингу и анализу, а также по результатам мониторинга и анализа, часто используют как систему, способную помочь обнаружить и исправить слабые места, прежде чем произойдут отрицательные воздействия или обеспечить уверенность в том, что уровень текущего риска соответствует критериям риска организации. Эти действия могут также быть использованы для предоставления внутренним и внешним заинтересованным сторонам разумной гарантии эффективности организации.

Риск может стать дополнительным фактором изменений во внутренней и внешней среде организации. Аналогично, мониторинг внешней среды может повысить готовность организации к изменениям, которые могут предоставить дополнительные возможности для улучшения работы или нововведений. При внимательном отношении к таким изменениям, выполнению работ, несоответствиям и ошибкам организация сможет идентифицировать возможности для улучшения структуры менеджмента риска и работы организации в целом.

Необходимо разработать на местах всестороннюю программу мониторинга и регистрации показателей риска при выполнении работ, которые должны быть интегрированы с другими показателями работы организации.

Программа должна помочь в создании системы раннего обнаружения неблагоприятных трендов, которые могут потребовать внедрения предупреждающих действий.

Мониторинг и анализ по отдельности могут быть направлены на индивидуальный риск или несколько связанных рисков. Они могут помочь фокусироваться на риске и/или методах его обработки или управления.

D.1.2 Ответственность за мониторинг и анализ

Общую ответственность за действия по мониторингу и анализу несут контролирующие органы и высшее руководство, а не органы контроля, например, подразделения по внутреннему аудиту. Полезным дополнением к процессу отчетности системы менеджмента могут стать функции обеспечения качества, независимый функциональный анализ и мониторинг выполнения обязательных требований, потому что эти действия обеспечивают альтернативные данные о процессе.

Действия по мониторингу и анализу могут быть рассмотрены с точки зрения иерархической структуры. При этом необходимо регулярно проводить действия по мониторингу и анализу на высших уровнях, что, при должной организации, обеспечивает самый высоких уровнях результативности. Однако программа мониторинга и анализа должна включать все три элемента.

Программа мониторинга и анализа должна верифицировать внедрение и эффективность выполнения политики в области менеджмента риска. Способ реагирования высшего руководства на результаты программы мо-

ниторинга может повлиять на поведение работников. Очень важно, чтобы высшее руководство действовало как образец для подражания.

D.1.3 Независимость анализа

Независимость анализа, проводимого внутренними или внешними сторонами, вытекает из отношений проверяющего (аудитора) и нанимающей стороны.

Независимость — основа беспристрастности анализа и объективности выводов. Проверяющие и аудиторы должны быть независимы от проверяемых (контролируемых) настолько, насколько возможно. При этом аудиторы не должны допускать в работе предвзятости и конфликта интересов.

Для целей внутреннего аудита аудиторы должны быть независимы от руководителей проверяемых подразделений. Проверяющие и аудиторы должны стараться быть объективными на всех этапах процесса аудита, чтобы гарантировать, что результаты и заключения базируются только на доказательствах.

В небольших организациях часто достаточно трудно обеспечить полную независимость проверяющих и аудиторов от руководителей проверяемых подразделений, но необходимо приложить максимальные усилия, чтобы избежать предвзятости и конфликта интересов.

Независимость проверяющих и аудиторов помогает сделать проверки и аудиты эффективным и надежным методом поддержки политики в области менеджмента риска и методов управления. Это помогает организации получить необходимую информацию, на основе которой могут быть внедрены необходимые улучшения.

Такие проверки часто ориентированы на проверку соответствия стандартам (внутренним и/или внешним), процедурам или законодательным требованиям. В процессе проверок также рассматривают пригодность, результативность и эффективность методов управления, например, проверка действий в области менеджмента риска на соответствие принципам ИСО 31000.

Во многих организациях проводят анализ со стороны руководства и консультирование (например, силами советников по вопросам менеджмента риска, сотрудников службы контроля и менеджеров по качеству), в рамках которых проводят проверки. При этом о результатах внутреннего аудита, как правило, сообщают контролирующему органу и высшему руководству. Целью проведения анализа и проверок является обеспечение гарантий контролирующему органу и высшему руководству организации в том, что:

- критерии риска совместимы с целями и условиями работы организации;
- использован соответствующий систематический процесс для идентификации, оценки и обработки риска, и этот процесс непрерывно функционирует;
- проводят необходимую обработку недопустимого риска;
- применяют подходящие и эффективные способы управления для обработки недопустимого риска;
- планы обработки риска успешно внедряются.

Проведение независимого анализа не снимает и не снижает ответственности и обязанностей руководителей по проведению мониторинга и анализа на соответствующем уровне.

D.1.4 Получение необходимой информацию

Как и для других аспектов менеджмента риска, в процессе мониторинга и анализа необходимо использование наилучшей имеющейся информации [см. принцип f),]. Чтобы информация соответствовала цели, информация должна относиться к работе пользователей и быть достоверна. Полноценность информации повышается, если она сопоставима, поддается проверке, своевременна и понятна. Информация может быть получена из двух типов источников:

a) прямых данных: наблюдения и измерения фактических показателей или результатов процесса;

b) косвенных данных: измерения, полученные в процессе или в результате анализа.

Сочетание измерений из различных источников необходимо выбирать исходя из потребностей (в зависимости от доступности) или удобства (своевременность, стоимость и т. д.).

D.1.5 Отчетность о процессе анализа

Отчетность должна предоставить информацию контролирующим органам, высшему руководству и заинтересованным сторонам организации о соответствии риска критериям риска и наличии планов обработки риска, которые помогут достичь поставленных целей в области риска. Дополнительно отчетность может предоставить информацию о новых видах риска.

Весь набор информации о риске (например, в реестре риска) необходимо периодически обновлять. Тип и частота создания отчетов зависит от характера, размера и области применения оценки риска в организации.

В результате процесса анализа или аудита должен быть разработан отчет, в котором необходимо подвести итоги и сделать заключение об оценке соответствия установленным критериям. В отчете могут быть представлены рекомендации относительно улучшения системы на основе наблюдений проверяющих. Иногда проверяющий может дать предложения непосредственно по критериям риска. Действия по результатам анализа должны быть сосредоточены на улучшении системы и направлены на первопричины проблем.

D.1.6 Корректирующие действия и постоянное улучшение

Организация должна установить соответствующие процессы, чтобы обеспечить активное рассмотрение рекомендаций руководством организации и инициирование внедрения необходимых мероприятий. Необходимо довести до сведения контролирующих органов и заинтересованных сторон информацию предпринимаемых ответных действий и проводить мониторинг этих действий до их полного внедрения.

D.2 Мониторинг и анализ структуры

D.2.1 Общие положения

Целью мониторинга и анализа является поддержание структуры менеджмента риска в актуализированном состоянии. Структура направлена на элементы и процессы системы менеджмента организации, которые позволяют управлять риском.

В ИСО 31000:2009, пункт 4, приведено руководство о необходимых элементах структуры и их взаимосвязи с внутренней и внешней областью применения и средой организации.

Изменения могут происходить во внутренней или внешней области применения и среде организации, поэтому необходимо постоянно адаптировать структуру менеджмента риска, чтобы обеспечить ее постоянную эффективность.

Даже при отсутствии внутренних или внешних изменений, которые требуют изменений структуры, все равно необходимо обеспечить, чтобы в любое время структура функционировала, как запланировано. Для организаций, переходящих к применению ИСО 31000, может возникнуть необходимость проверки элементов структуры плана внедрения, чтобы обеспечить его корректное осуществление. Для организаций, которые уже внедрили ИСО 31000, необходимо обеспечить проверку наличия и непрерывного функционирования компонентов структуры, как запланировано.

D.2.2 Ответственность

При распределении обязанностей в области менеджмента риска руководители, ответственные за обеспечение регулярного анализа и мониторинга структуры на соответствие установленным показателям, ответственное лицо (например, руководитель высшего звена) или подразделение организации (например, отдел менеджмента риска) должны стать хранителями структуры, их ключевая ответственность должна состоять в том, чтобы обеспечить постоянную эффективность структуры.

D.2.3 Установление базового уровня

Организация должна установить базовый уровень менеджмента риска в организации. Этот уровень может быть описан различными способами, но должен включать:

a) элементы структуры (см. ИСО 31000:2009, пункт 4.3), которые обеспечивают возможность достижения поставленных целей;

b) степень поддержки, оказываемой контролирующими органами и высшим руководством, которая выражена через полномочия и обязательства в области менеджмента риска (которая часто выражается в форме политики в области менеджмента риска).

Предназначенная форма и архитектура структуры менеджмента риска должны быть зарегистрированы после разработки, а информация о них доступна, например, в виде таблицы (см. таблицу D.1). Это помогает создать основу или ориентир для сравнений, который может быть использован в процессе мониторинга и анализа.

Таблица D.1 — Пример таблицы перечня элементов структуры

Элемент	Область применения	Цели	Ключевые действия	Ответственность и график работ	Меры по внедрению	Статус выполнения
Ответственность	Уровень ответственности	Поддержка текущей политики организации в области менеджмента риска	- Определение критериев; - создание отчетных документов; - делегирование полномочий	- Издание политики; - разработка графика и матрицы ответственности; - дата следующего анализа	...	...
Ресурсы: Обучение	Организационный уровень	Обеспечение элементов менеджмента риска для процесса обучения. Обеспечение доступности обновлений в процессе обучения	- Разработка рекомендаций; - разработка программы обучения; - обеспечение обучения преподавателей	- Разработка: менеджмента риска организации; - детализация: менеджмента подразделений - дата следующего анализа: хх/хх/хх	- Действие: ежемесячный отчет; - качество: опрос или аудит обучения	...

Организация должна установить показатели выполнения работ, которые связаны с целями организации и являются признаком результативности общей структуры менеджмента риска. Показатели выполнения, иногда называемые остаточными показателями, включают:

- инциденты, аварии и ошибки;
- фактические потери;

- несоответствия;
- жалобы потребителей;
- неуплаченный долг;
- готовность системы;
- степень достижения целей организации;
- степень достижения целей менеджмента риска.

D.2.4 Оценка изменений характеристик и среды организации

Организация должна установить наличие материальных изменений внутренней или внешней среды и области применения с момента разработки или изменения структуры менеджмента риска.

Практическая помощь

Внутренние характеристики, которые могут измениться, включают:

- структуру;
- методы управления и требования;
- политику, внутренние стандарты и модели;
- договорные требования;
- стратегические и операционные системы, затронутые внутренними или внешними факторами (например, изменение законодательных и обязательных требований);
- возможности и ресурсы (например, финансовый капитал, репутация, капитал, время, люди, процессы, системы и технологии);
- знания, навыки и интеллектуальная собственность;
- информационные системы и потоки;
- социальное, экологическое и культурное поведение;
- другие приоритеты и постулаты организации, которые могут быть восприняты как конкурирующие с намерениями организации в области менеджмента риска.

Ведущие показатели, которые могут указать на изменения во внешней среде и области применения, обычно определяют по отчетам и обзорам, которые отражают изменения и тренды в сфере промышленности, в которой работает организация.

Примеры включают:

- товарную оценку, показатели банковского процента, бонусы, обменные курсы, индексы фондового рынка, индекс потребительских цен (тренд);
- индекс (тренд);
- уровень или инциденты мошенничества в подобных организациях;
- объем рынка и потенциал роста, а также внезапные изменения в объемах заказов;
- политическую и социальную стабильность, социальное недовольство и активность.

Если область применения и среда организации изменились, то необходимо пересмотреть существующую структуру менеджмента риска с учетом выявленных изменений. Целью этого является подтверждение пригодности структуры и процессов установленным целям и приоритетам организации.

В результате анализа организация может изменить базовый уровень структуры менеджмента риска.

Пример 1 — Изменения в структуре организации могут потребовать пересмотра политики в области менеджмента риска и перераспределения ответственности и ресурсов для эффективного управления. Если размер организации увеличился, например, из-за слияния или приобретения компаний, то необходимо пересмотреть объем ресурсов, выделяемых на менеджмент риска, и провести подробный анализ всех различий в подходе к менеджменту риска между организациями. Может возникнуть необходимость разработать переходный план, который позволит внедрить все необходимые изменения, выявленные в результате анализа.

Пример 2 — Если появились новые законодательные требования, то аспекты структуры, связанные с ответственностью, обучением, получением информации или созданием отчетов, возможно, потребуют пересмотра или расширения.

D.2.5 Анализ структуры

Если в организации однажды уже проведена оценка характеристик, внешней среды и области применения, то необходимо провести более широкий, всесторонний анализ структуры, чтобы определить:

a) что выполнение плана менеджмента риска происходит как запланировано;

b) принятые структура и процессы работают как запланировано;

c) уровень риска находится в пределах установленных критериев;

d) менеджмент риска положительно влияет на основные цели организации;

e) соответствующие вовлеченные стороны получают достаточно отчетов, что позволяет им эффективно исполнять свои функции и обязанности в структуре управления;

f) персонал организации обладает достаточными навыками, знаниями и компетентностью в области менеджмента риска, чтобы выполнять возложенные обязанности;

g) ресурсов, выделенных на менеджмент риска, достаточно;

h) опыт, извлеченный из фактических результатов работ, включая потери, ошибки и возможности, изучен и из него сделаны необходимые выводы;

i) достигаются цели, установленные в области менеджмента риска.

Организация должна утвердить регулярный график анализа. Если обстоятельства изменяются, то график анализа необходимо изменить исходя из текущих целей, например, если последствия риска появляются внезапно или они очень серьезные.

Результаты такого анализа должны включать в себя:

- полный отчет о функционировании структуры менеджмента риска;
- отчет об этапах и прогрессе выполнения плана менеджмента риска (включая анализ всех задержек);
- общий отчет о зрелости организации в области риска в соответствии с передовым опытом;
- рекомендации о необходимых изменениях для улучшения качества менеджмента риска и его результативности в организации;
- актуализацию политики, целей и планов в области менеджмента риска по мере необходимости;
- актуализацию описания области применения и среды работы организации;
- отчет о трендах ключевых показателей риска;
- план действий по работе с изменениями, направленный на достижение целей в области менеджмента риска.

D.3 Мониторинг и анализ процесса

D.3.1 Общие положения

Цель мониторинга и анализа процесса менеджмента риска состоит в обеспечении того, что этот процесс:

- соответствует бизнесу организации;
- работает как запланировано.

Риски и соответствующие методы управления и обработки риска могут изменяться на протяжении длительного периода, ответственные за менеджмент риска должны знать о значении этих изменений. Отказ от обработки может привести к недопустимому риску. Кроме того, методы управления, цель которых состоит в выявлении недостатков и модификации риска, могут быть изменены с точки зрения их пригодности и результативности. Это связано с тем, что если не поводить регулярный мониторинг и анализ риска, то его значение может стать недопустимым в соответствии с критериями приемлемого риска организации, а, следовательно, у организации, возможно, нет понимания ее рисков.

На основе результатов мониторинга и анализа необходимо вернуться к этапу установления области применения и среды и пересмотреть их. При этом следует сохранить основу для возобновления оценки риска путем обеспечения повторяющегося и динамического характера процесса менеджмента риска и разработки структуры менеджмента риска.

D.3.2 Ответственность

Мониторинг должен стать неотъемлемой частью менеджмента. Риск и методы его обработки должны быть подконтрольны ответственным за их мониторинг. Эта ответственность должна быть зарегистрирована в должностных инструкциях и соответствующих документах.

Организация должна разработать единые корпоративные показатели эффективности менеджмента риска, которые должны отражать диапазон ключевых критериев, на основе которых работники могут проводить документальный анализ, например показателей, которые могут учесть финансовые аспекты, требования заинтересованных сторон, внутреннюю эффективность, а также задачи по обучению и росту. Фактическая эффективность работ по отношению к перечню показателей может быть измерена на всех уровнях организации и результаты измерений направлены ответственным лицам.

Организация должна проводить мониторинг планов обработки риска, чтобы удостовериться в их успешной и своевременной реализации.

D.3.3 Изучение полученного опыта

Организация должна учиться на своих ошибках, включая потери, отклонения, несоответствия и возможности, которые были идентифицированы заранее, но на них не отреагировали.

При таком анализе необходимо ответить на следующие вопросы:

Что произошло?

Как и почему получен такой результат?

Нужно ли пересмотреть изначальные предположения?

Какие ответные меры были предприняты (или не предприняты)?

Вероятность повторного получения такого результата?

Каковы все дополнительные ответные меры или предпринятые действия?

Ключевые пункты, которые должны быть изучены и лица, которые должны быть информированы о них.

D.3.4 Мониторинг

D.3.4.1 Существуют следующие типичные подходы к мониторингу:

a) Владельцы риска могут исследовать среду для наблюдения за изменениями в области применения и среды. Частота таких исследований зависит от уровня риска и динамики изменений среды. В некоторых случаях

достаточно разработать отчетность по отклонениям от установленных показателей. Владелец риска сравнивает соответствующие внешние или внутренние факторы с областью применения, чтобы определить, произошли ли изменения. При этом необходимо обеспечить регулярный обмен информацией и консультации с заинтересованными сторонами, чтобы определить, не изменились ли их взгляды или цели.

b) Владельцы риска проводят мониторинг планов обработки риска на предмет своевременности действий и адекватного реагирования на изменения среды.

c) Владельцы средств контроля несут ответственность за мониторинг состояния средств контроля и проводят их периодическую проверку или непрерывный мониторинг. Наибольшей эффективности менеджмента риска можно добиться тогда, когда он полностью интегрирован в процесс принятия решений и систему менеджмента организации. Необходимо использовать управление эффективностью, чтобы проводить мониторинг риска и результативности процесса менеджмента риска. Показатели эффективности должны отражать диапазон ключевых целей организации, установленных в начале процесса менеджмента риска при определении области применения менеджмента риска. Такие показатели эффективности могут быть разработаны в отношении определенных видов риска, методов управления и применения процесса менеджмента риска.

Примечание — При работе с риском желательно, чтобы средства контроля также принадлежали ответственному за их работу. Обычно владелец или оператор, работающий со средством контроля не является владельцем риска. Это не затрагивает общую ответственность владельца риска по обработке риска и разработке, внедрению, применению, мониторингу и оценке соответствующих средств контроля.

D.3.4.2 Показатели эффективности могут помочь измерению результатов (например, определять потери или доходы) или показателей процессов (например, своевременное завершение планов обработки риска). Обычно используют набор различных показателей, но показатели эффективности обычно не указывают причины изменений. Поэтому в условиях быстро изменяющейся среды показатели процесса могут стать более полезными.

При выборе показателей важно проверить, что:

- они измеримы;
- их использование эффективно с точки зрения требований своевременности, усилий и ресурсов;
- процесс измерений или наблюдений поощряет или облегчает желательные действия и не мотивирует к нежелательным действиям (например, фальсификацию данных);
- вовлеченные лица понимают процесс и ожидаемую выгоду, а также имеют возможность участвовать в разработке показателей;
- результаты измерены, работа проанализирована и доведена до заинтересованных лиц в форме, которая облегчает изучение опыта и улучшение организации.

D.3.4.3 При применении управления эффективностью к процессу менеджмента риска, нужно отметить, что:

- измерение эффективности требует ресурсов, которые должны быть идентифицированы и выделены при разработке показателей эффективности;
- некоторые действия в области менеджмента риска трудно измерить, но это не делает их менее важными. В этом случае можно использовать замещающие показатели, например, ресурсы, выделенные на деятельность в области менеджмента риска, могут быть заместительной мерой приверженности эффективному менеджменту риска;
- разница между данными измерений по показателям эффективности и инстинктивным представлениям о фактическом состоянии очень важна и должна быть исследована, например, если руководители не заинтересованы в менеджменте риска из-за низкого (по оценкам) уровня риска, то все равно проблему необходимо исследовать и не отклонять;
- внезапное ухудшение показателей обычно привлекает внимание, однако прогрессивное ухудшение показателей может быть столь же проблематичным, поэтому необходимо проводить мониторинг и анализ трендов показателей эффективности.

D.3.5 Анализ со стороны руководства

Необходимо регулярно проводить анализ со стороны руководства процессов, систем и действий для обеспечения того, чтобы:

a) новые риски не возникали;

b) методы управления и обработки риска оставались соответствующими и эффективными.

Такой анализ со стороны руководства необходимо проводить в соответствии с утвержденной программой (например, на основе подхода, установленного в ИСО 19011).

В процессе анализа со стороны руководства могут быть использованы методы, аналогичные непрерывному мониторингу, при этом целесообразно, чтобы для обеспечения более объективного анализа их проводило лицо, непосредственно не вовлеченное в процесс. Периодичность анализа может быть установлена исходя из уровня риска, цикла бизнес-планирования, динамики изменения среды или совещаний контролирующего органа, ответственного за менеджмента риска.

Если обнаружены проблемы, организация должна рассмотреть, как они появились и почему они не были обнаружены ранее.

Обеспечение средствами контроля лежит на ответственных руководителях (владельцах риска) и является частью их обычных функций и обязанностей. Выделение специальных средств контроля владельцам средств кон-

троля облегчает их внедрение, но применение специальных средств контроля может потребовать дополнительного обучения персонала. Если запланированы изменения в организации или обнаружены внешние изменения, то могут произойти изменения:

- во внешней или внутренней среде, заинтересованных сторонах и их взглядах;
- области применения менеджмента риска, целях и критериях риска организации;
- видах и уровнях риска;
- необходимости обработки риска;
- влиянии и результативности методов управления риском.

При разработке или пересмотре бизнес-планов или стратегических планов для организации очень важно проводить анализ со стороны руководства видов риска, обработки риска и методов управления риском. В этом случае могут быть разработаны или пересмотрены цели организации, поэтому целесообразно использовать процесс оценки риска для анализа предварительных вариантов планов, чтобы обеспечить достижимость целей и определить соответствующие мероприятия по обработке риска. Лица, ответственные за выполнение процесса менеджмента риска, должны регулярно проводить анализ событий, продукции и результатов, чтобы идентифицировать возможности для улучшения.

Приложение Е
(справочное)

Интегрирование менеджмента риска в общую систему менеджмента организации

Е.1 Общие положения

Менеджмент риска — неотъемлемая часть системы менеджмента организации. В стандарте ИСО 31000 организациям рекомендовано разработать, внедрить и непрерывно улучшать структуру менеджмента риска, целью которой является объединение менеджмента риска в систему менеджмента организации (включая управление и стратегию). Интеграция должна обеспечить, чтобы информация о риске использовалась для принятия решений на всех уровнях организации. Люди и организации управляют риском каждый день, когда они принимают решения. Менеджмент риска уже естественно присутствует в ситуации, когда мы решаем сделать что-то. Кто-то это делает лучше, кто-то хуже, но все могут улучшить качество менеджмента риска и принятия решений, что приводит к улучшению способов достижения целей и повышению доверия. Если целью интеграции менеджмента риска является повышение ценности, то вполне логично воздействовать на то, что уже существует вместо того, чтобы заменять существующее чем-то другим. При этом нелогично добавлять что-то или принуждать к иному способу действий, если что-то уже происходит как естественная функция принятия решений.

Интеграция не просто включает внедрение установленных и стандартизированных методов и процессов менеджмента риска в существующую систему(ы) менеджмента, а требует адаптации и изменений методов и процессов для удовлетворения потребностей лиц, принимающих решения, и подстроить их под существующие процессы принятия решений.

В настоящем приложении приведены некоторые практические примеры того, как менеджмент риска может быть интегрирован в существующую систему(ы) менеджмента.

Е.2 Что такое система менеджмента?

Все организации используют определенную систему менеджмента. Недавно формализованные системы менеджмента, состоящие из множества требований, были созданы, чтобы служить основой, в соответствии с которой организация может установить практику и процедуры управления работой. Существует много международных и национальных стандартов, которые описывают систему менеджмента в целом или ее отдельные элементы.

Система менеджмента — это ряд взаимосвязанных или взаимодействующих элементов организации, направленных на установление политики и целей, а также процессов достижения этих целей. С точки зрения управления бизнесом, достичь большей эффективности возможно при внедрении интегрированной системы менеджмента.

Например, менеджмент качества, описанный в ИСО 9001, содержит эффективный подход к удовлетворенности потребителя, в то время как менеджмент риска работает с воздействиями неопределенности на цели, которые могут относиться не только к потребителям, но также и другим заинтересованным лицам. Многие организации внедрили систему менеджмента качества, основанную на требованиях ИСО 9001, поэтому менеджмент риска может быть интегрирован в такую систему менеджмента путем разработки совместных действий, избегая дублирования.

Е.3 Интегрированная система менеджмента и менеджмент риска

Кроме интеграции менеджмента риска в процессы основного бизнеса, существует потребность в разработке взаимодействия между всеми подходами системы менеджмента, например, менеджментом качества, экологическим менеджментом, системой техники безопасности, менеджментом безопасности, оценкой соответствия, финансовым менеджментом и даже со страховым менеджментом, связанным с событиями, которые могут быть в финансовом отношении переданы другим организациям.

Отдельные системы менеджмента должны сформировать интегрированную систему менеджмента, основанную на политике и стратегии всей организации. Если организация имеет отдельные системы менеджмента для управления особыми рисками, структура менеджмента риска должна быть распространена и на другие системы.

Такой подход к менеджменту риска может помочь:

a) повысить ориентированность высшего руководства на стратегические цели организации;

b) обеспечить обработку всех рисков в интегрированной системе менеджмента в соответствии с принципами и руководящими указаниями ИСО 31000.

Этот подход может включать следующее:

- применение в системе менеджмента качества методов менеджмента риска, связанных с менеджментом риска проекта и продукции;
- работу с неопределенностью в экологическом менеджменте, например, работу с инцидентами и потенциальными авариями, деятельность в опасном помещении, утилизацию опасных материалов и веществ;
- интегрирование обработки риска в функциональную деятельность, такую как обеспечение безопасности работ;
- обработку риска, связанного с угрозой безопасности, например насильственными действиями против организации, ее служащих или потребителей;

- работу с рисками, связанными с информационными технологиями (ИТ), например, прерывания ИТ-операций, потери данных, нарушения конфиденциальности и обеспечения непрерывности бизнеса;

- управление риском, связанным с обеспечением непрерывности бизнеса, гарантирующим быстрое реагирование на опасные события и инциденты;

- установление средств контроля, направленных на защиту активов организации, обеспечение правильной отчетности, обеспечение соответствия законодательным и обязательным требованиям или управление страховым риском для снижения страховой премии.

Е.4 Внедрение менеджмента риска в структуру системы менеджмента качества

Е.4.1 Общие положения

Процесс менеджмента риска должен быть интегрирован в процессы принятия решений организации, независимо от уровня и функционального подразделения, в которых приняты эти решения.

Е.4.2 Идентификация и понимание принятия решения

Следующие методы помогают понять, когда и где решения принимают, в соответствии с циклом «Планируй — Делай — Проверяй — Действуй» (PDCA).

a) Идентификация всех форм формализованных методов принятия решений, существующих в организации. В крупных организациях используют многочисленные процедуры, которые требуют формального одобрения широкого диапазона решений, например, одобрения ежегодного стратегического плана, капиталовложений, нового штата, модификации управлений процессом, перемещение штата.

b) Использование блок-схем или других методов, позволяющих нанести на карту основные методы принятия решений и последовательности их реализации, применяемых к определенным проектам и ко всем аспектам бизнеса. Этот метод позволяет рассмотреть процесс принятия решений по подразделениям или по основным функциям и должен быть применен при разработке проекта принимаемого решения. Если в организации существуют действия, управление которыми осуществляется с применением формализованной системы менеджмента (например, руководства по применению ИСО 9001), то принятие решения в таких системах должно стать частью этого анализа. Точно так же, если в организации существует делегирование полномочий по принятию решений, то такое делегирование должно быть включено в анализ. В результате должна сложиться последовательная и документированная система того, где решения приняты, кто принимает решения, и какие существуют процессы, вовлеченные в такие решения.

Сочетание вышеупомянутых методов должно повысить степень организационного и личного понимания процесса принятия решений.

Е.4.3 Оценка риска

При принятии некоторых решений (например, разработка и реализация новой продукции или планирование и внедрение основного проекта) уместно включать формальную оценку риска в различные стадии проекта. Например, в большинстве проектов существует много точек принятия решений, таких как выполнение, экономическое обоснование, бюджетирование, планирование, внедрение и передача. В каждой из этих точек формальная оценка риска необходима при выборе варианта принятия решений. Это увеличивает вероятность успешного выполнения проекта и повышает его эффективность. Для оценки риска производственных решений для использования вовлеченным персоналом могут быть разработаны простые стандартизированные формы процесса менеджмента риска. Такие методы особенно подходят в ситуациях, где персонал работает без непосредственного контроля. Ключевым компонентом этих методов принятия решений является понимание использованных предположений. По определению, предположения — источник неопределенности.

Такие стандартизированные процессы менеджмента риска могут быть определены для различных типов принятия оперативных решений, отдельных групп работников, выполняющих особую задачу и конкретной среды, где они происходят. Простые системы могут быть закодированы в карманном, проверочном контрольном листе и выданы вовлеченному персоналу.

Е.4.4 Внедрение в структуру менеджмента риска

Выполнение методов, приведенных ниже, требует регулирования и пересмотра структуры менеджмента риска, например:

- внесения поправок в политику в области менеджмента риска организации;

- организации мероприятий, направленных на выполнение первоначального анализа и картографии практики принятия решений;

- внесения поправок в руководящие процедуры;

- обучения менеджеров и вовлеченного персонала;

- специального обучения персонала, выполняющего работу в соответствии с определенной системой менеджмента (например, персонала, работающего с особыми типами риска);

- регулирования гарантийной системы организации и системы информирования о менеджменте риска;

- обеспечения результативного внутреннего обмена информацией и консультаций.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 31000:2009	IDT	ГОСТ Р ИСО 31000—2010 «Менеджмент риска. Принципы и руководство»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичный стандарт.		

Библиография

[1] ISO 9000, Quality management systems — Fundamentals and vocabulary
[2] ISO 9001, Quality management systems — Requirements
[3] ISO 19011, Guidelines for auditing management systems
[4] ISO Guide 73:2009, Risk management — Vocabulary
[5] IEC 31010, Risk management — Risk assessment techniques

УДК 658.562.012:006.354 ОКС 03.100.01 Т59

Ключевые слова: менеджмент риска, риск, управление риском, принципы менеджмента риска, процесс менеджмента риска, мониторинг риска, неопределенность

БЗ 8—2017/1

Редактор *И.В. Львова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 13.09.2017. Подписано в печать 05.10.2017. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,79. Тираж 26 экз. Зак. 1689.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru