ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70350— 2022

МЕНЕДЖМЕНТ РИСКА

Оценивание качества менеджмента риска организации

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Ассоциацией риск-менеджмента «Русское Общество Управления Рисками» (АРМ «РусРиск»)

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 12 сентября 2022 г. № 914-ст

4 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

© Оформление. ФГБУ «РСТ», 2022

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 Термины и определения 1
4 Менеджмент риска в организации 2
5 Оценка менеджмента риска 3
6 Методы сбора информации и доказательств 7
7 Формирование интегральной оценки менеджмента риска и рекомендаций по улучшению 8

Введение

Менеджмент риска как часть сильного корпоративного управления организации получает все большее признание и внимание. Требования и запросы со стороны заинтересованных сторон, включая регуляторов, поставщиков, потребителей, партнеров, финансовые организации и т. д., стимулируют организации идентифицировать существенные бизнес-риски, с которыми они сталкиваются, — социальные, корпоративные, этические и экологические, а также стратегические, финансовые, операционные и иные — и объяснять, как они ими управляют, почему предпринятых ими действий достаточно для достижения поставленных целей.

Использование инфраструктуры менеджмента риска расширилось, поскольку многие организации признали преимущества скоординированных подходов к менеджменту риска и согласны с тем, что эффективный менеджмент риска должен быть полностью интегрирован с управлением организацией и применяться на всех уровнях организации (корпоративном, процессном уровне, уровне бизнес-единицы, проекта и т. д.). В свою очередь, это влечет за собой потребность в оценке эффективности менеджмента риска, так как согласно ГОСТ Р ИСО 31000—2019 (подраздел 5.1) она будет зависеть от степени интеграции в управление организацией, включая процедуры принятия решений.

Инфраструктура менеджмента риска должна быть разработана таким образом, чтобы подходить организации, ее внутренней и внешней среде. Для того чтобы менеджмент риска был эффективным, инфраструктура в любой организации, независимо от ее размера или цели, должна содержать определенные существенные компоненты, включая компонент «Оценка эффективности». Отправной точкой для улучшения подхода организации к менеджменту риска должен быть анализ текущего состояния, который подводит итоги и оценивает, какие из остальных компонентов присутствуют сейчас. Если какая-либо из основных частей отсутствует, маловероятно, что менеджмент риска станет эффективным. Оценка деятельности организации по менеджменту риска является критически важным элементом в этих усилиях.

Анализ текущего состояния также позволяет определить степень надежности менеджмента риска, т. е. те характерные для конкретной организации ограничения, которые могут оказывать влияние на его эффективность, включая ограниченность ресурсов, знаний и достоверности информации, ограничения технологий и способов их применения, предубеждения, допущения и убеждения вовлеченных лиц и др.

Настоящий стандарт описывает три подхода к оценке качества менеджмента риска организации: через элементы процесса менеджмента риска, на основе ключевых принципов менеджмента риска и на основе модели зрелости менеджмента риска. Используемый подход (или комбинация подходов) оценки качества должен быть адаптирован к потребностям организации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ РИСКА

Оценивание качества менеджмента риска организации

Risk management.
Quality assessment of the organization's risk management

Дата введения — 2023—01—01

1 Область применения

В настоящем стандарте содержатся руководящие указания по оцениванию качества менеджмента риска. Эти руководящие указания могут быть адаптированы для любой организации вне зависимости от рода ее деятельности. При этом законодательством Российской Федерации, органами регулирования и надзора в рамках отдельных направлений деятельности организации и/или отраслью могут быть установлены отдельные требования к организации и оцениванию качества менеджмента риска. Организациям следует применять настоящий стандарт с учетом специального регулирования в части, не противоречащей требованиям такого регулирования.

Настоящий стандарт описывает общие подходы к оцениванию качества менеджмента риска и не ограничивается конкретной отраслью или видом деятельности.

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

2 Нормативные ссылки

ГОСТ Р ИСО 31000—2019 Менеджмент риска. Принципы и руководство
ГОСТ Р 51897 (ISO Guide 73:2009) Менеджмент риска. Термины и определения

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 51897, а также следующие термины с соответствующими определениями:

3.1 **оценщик**[1)]: Сотрудник/подразделение либо привлеченный эксперт, выполняющие оценивание качества менеджмента риска в организации.

Примечание — Основным внутренним оценщиком является внутренний аудитор или подразделение внутреннего аудита организации (в случае его наличия).

3.2 **качество менеджмента риска:** Характеристика менеджмента риска, отражающая надежность и эффективность его функционирования в организации.

3.3 **зрелость менеджмента риска:** Состояние развития менеджмента риска в организации относительно обобщенного состояния иных организаций, включая применение принципов и процесса, внедрение и развитие инфраструктуры менеджмента риска.

[1)] Термин распространяется на настоящий стандарт в трактовке, устанавливаемой его определением, и не имеет связи с Федеральным законом № 135-ФЗ от 29 июля 1998 г. «Об оценочной деятельности в Российской Федерации».

Издание официальное

3.4 **инфраструктура менеджмента риска:** Набор компонентов, формирующих основы и организационные меры, применяемые при проектировании, разработке, внедрении, мониторинге, пересмотре и постоянном улучшении менеджмента риска во всей организации.

Примечания

1 Основы отражают политику, цели, полномочия и обязательства в области менеджмента риска.

2 Организационные меры включают планы, взаимоотношения, подотчетность, ресурсы, процессы и действия.

3 Инфраструктура менеджмента риска интегрирована в стратегические и операционные политики и практики всей организации.

3.5 **комплаенс-обязательства:** Применимые внешние требования (законодательство Российской Федерации, а также иные нормативно-правовые акты, регламентирующие деятельность и ответственность организации), требования внутренних политик и процедур и иные требования, на которые организация ориентируется в рамках своей деятельности (договорные отношения, хартии и т. д.).

3.6 **разумная уверенность:** Степень предоставления гарантий, которая основана на объективности и полноте информации, необходимых и достаточных для принятия обоснованных управленческих решений и формирования выводов, заключений в части менеджмента риска.

Примечание — Разумная уверенность может отличаться и определяться отдельно в каждой конкретно взятой ситуации.

4 Менеджмент риска в организации

4.1 Организация инфраструктуры менеджмента риска

Инфраструктура менеджмента риска неотъемлемо встроена в общую стратегию, политику и практическую деятельность организации. Организационные меры включают планы, взаимоотношения, подотчетность, ресурсы, процессы и действия. Схема инфраструктуры менеджмента риска, приведенная на рисунке 1 ГОСТ Р ИСО 31000—2019, показывает концептуальную модель, которую можно использовать для анализа качества данных взаимосвязей.

Ответственность за определение отношения организации к риску несет ее высшее руководство, а совет директоров/наблюдательный совет (далее — Совет) отвечает за определение того, соответствует ли отношение к риску наилучшим интересам акционеров (участников) и других высших органов управления организации в зависимости от организационно-правовой формы.

Совет обеспечивает общий надзор за менеджментом риска организации и должен понимать компоненты менеджмента риска, спрашивать высшее руководство о рисках и согласовывать ключевые управленческие решения. Заинтересованным сторонам следует предоставлять информацию, достаточную для понимания отношения к риску высшего руководства и Совета, чтобы принимать решения в соответствии с их толерантностью к потенциальному изменению результатов деятельности организации. Организации раскрывают информацию о менеджменте риска посредством периодической публичной управленческой отчетности, пресс-релизов, по запросам заинтересованных сторон и иными, не запрещенными политикой организации, способами, а также организуют работу по получению обратной связи от заинтересованных сторон.

Совет также несет общую ответственность за обеспечение менеджмента риска и наличие адекватной инфраструктуры менеджмента риска. Совет возлагает работу по организации и поддержанию инфраструктуры менеджмента риска на высшее руководство; при этом в организации может быть создано отдельное функциональное подразделение со специальными навыками и знаниями, которое координирует данную деятельность, однако важную роль в обеспечении успешного менеджмента риска в масштабах всей организации играет каждый ее сотрудник. Основная ответственность за идентификацию рисков и воздействие на них остается на высшем руководстве.

4.2 Мониторинг

Функционирование менеджмента риска в организации со временем меняется. Отношение к риску может измениться из-за факторов внутренней или внешней среды, эффективные в прошлом меры воздействия на риск могут стать неактуальными, а контрольные процедуры — менее эффективными или больше не выполняться. Изменения могут быть вызваны приходом нового персонала, изменениями в структуре организации или внедрением новых процессов. Кроме того, изменяются цели организации,

а также характер потенциальных событий или условий, которые могут повлиять на достижение этих целей. Менеджмент риска должен предвосхищать, обнаруживать, признавать и реагировать на изменения рисков и событий соответствующим и своевременным образом. Поэтому высшему руководству необходимо определить, остаются ли элементы менеджмента риска актуальными и способны ли они справляться с новыми рисками.

Важнейшим элементом надежного менеджмента риска является мониторинг, обеспечивающий его правильное функционирование. Мониторинг может осуществляться двумя способами: в рамках текущей деятельности или посредством отдельных оценок. Такое сочетание непрерывного мониторинга и отдельных оценок обеспечит сохранение эффективности менеджмента риска с течением времени.

Чем больше полнота и выше эффективность непрерывного мониторинга, тем меньше необходимость в отдельных оценках. Частота проведения отдельных оценок, необходимых для получения высшим руководством разумной уверенности в эффективности менеджмента риска, является предметом суждения высшего руководства, а также требований применимого регулирования (в случае их наличия). При принятии решения о проведении оценки учитываются характер и степень изменений, компетентность и опыт людей, реализующих меры воздействия на риски и соответствующие контрольные процедуры, характер рисков, на которые осуществляется воздействие, их существенность для бизнеса, результаты непрерывного мониторинга.

Непрерывный мониторинг встроен в обычную, повторяющуюся операционную деятельность организации. Он может быть более эффективным, чем отдельные оценки, потому что он выполняется в режиме реального времени, динамически реагируя на изменяющиеся условия, и глубоко внедрен в организацию. Часто проблемы быстрее всего выявляются с помощью непрерывного мониторинга, поскольку отдельные оценки проводятся постфактум. Некоторые организации, осуществляющие надежный непрерывный мониторинг, тем не менее проводят периодическую отдельную оценку менеджмента риска или его элементов, так как воспринимаемый уровень объективности у отдельных оценок будет выше, чем у самопроверок.

Организация, которая осознает необходимость частых отдельных оценок, должна сосредоточить внимание на способах усиления своего непрерывного мониторинга и таким образом сделать упор на встраивание мониторинга в свою деятельность, а не на его дополнение.

Поскольку ответственность за непрерывный мониторинг и отдельные оценки, как правило, распределяется между различными сторонами внутри организации, включая линейное руководство, внутренний аудит, функцию управления рисками, функцию обеспечения соответствия комплаенс-обязательствам и иные функции, важно, чтобы деятельность по обеспечению разумной уверенности была скоординирована для обеспечения наиболее эффективного и результативного использования ресурсов. В организациях часто бывает несколько отдельных групп, выполняющих различные функции по консультированию, соблюдению комплаенс-обязательств и обеспечению разумной уверенности по менеджменту риска независимо друг от друга. Без эффективной координации и отчетности работа может дублироваться или ключевые риски могут быть упущены (не выявлены и не проанализированы) или неправильно оценены.

5 Оценка менеджмента риска

Органы управления должны обладать разумной уверенностью в менеджменте риска. Для определения степени соответствия менеджмента риска потребностям организации, а также степени соответствия общепринятой передовой практике органы управления могут назначить (привлечь) оценщика.

Оценщик должен иметь способ измерения качества управления рисками в организации. Этого можно достичь путем изучения критериев, отражающих аспекты менеджмента риска. Используемые критерии должны быть актуальными, надежными, понятными и полными. Совокупность наблюдений должна позволить оценщику сделать вывод о надежности и эффективности менеджмента риска в организации.

Одной из ключевых групп критериев, которые оценщику следует учитывать при каждой оценке, является наличие подходящей инфраструктуры для организации и развития общекорпоративного и систематического подхода к менеджменту риска.

Оценщик должен проанализировать, учитывает ли и определяет ли инфраструктура:

- отношение организации к риску (в т. ч. путем определения риск-аппетита и толерантности к риску);
- ответственность и взаимодействие участвующих сторон;

- поддержание и развитие навыков и компетенций в области менеджмента риска среди участников;
- политику и план менеджмента риска;
- ограничения, которые могут оказывать влияние на эффективность менеджмента риска.

Оценщик также анализирует, позволяют ли компоненты инфраструктуры обеспечить риск-ориентированный подход к управлению организации в рамках ключевых направлений деятельности, включая (но не ограничиваясь) долгосрочное и краткосрочное планирование, операционную, инвестиционную, финансовую и проектную деятельность.

Результаты любой проверки документов в рамках оценки должны быть подтверждены путем анализа того, эффективно ли работает менеджмент риска на практике. Это означает, что данный тип деятельности по обеспечению разумной уверенности не должен ограничиваться инфраструктурой менеджмента риска и всегда должен рассматривать следующие вопросы:

- риски эффективно идентифицируются и надлежащим образом анализируются;
- имеется адекватное и соответствующее воздействие на риски;
- высшее руководство осуществляет эффективный мониторинг и пересмотр для выявления изменений в рисках и мерах по воздействию/контрольных процедурах.

Исходя из этого в дополнение к оценке инфраструктуры выделяются три подхода по достижению разумной уверенности, которые могут использоваться при оценке менеджмента риска:

- подход через элементы процесса менеджмента риска;
- подход на основе ключевых принципов менеджмента риска;
- подход на основе модели зрелости менеджмента риска.

Хотя подходы являются самодостаточными, каждый из них предлагает разные точки зрения на эффективность менеджмента риска в организации. Часто использование комбинации всех подходов может дать наиболее информативные и объективные результаты. Менеджмент риска должен быть соответствующим образом адаптирован к организации, ее размеру, целям культуры и профилю рисков. Следовательно, процесс подтверждения разумной уверенности также должен быть адаптирован к потребностям организации.

5.1 Подход через элементы процесса менеджмента риска

Данный подход проверяет наличие и реализацию каждого элемента процесса менеджмента риска согласно ГОСТ Р ИСО 31000. Нередко руководители склонны считать, что выполнение процесса менеджмента риска обеспечивается в любом случае, поэтому ключевым условием применения подхода является получение достаточного документального подтверждения соответствующих заявлений высшего руководства о выполнении каждого из элементов на практике.

Элемент 1. Обмен информацией и консультирование

К критериям данного элемента относятся закрепление порядка обмена информацией и консультирования и их фактическое выполнение, использование ИТ-средств для обмена информацией и консультирования, а также информационных и технологических систем для поддержки процесса менеджмента риска организации в целом и др.

Элемент 2. Область применения, среда и критерии

К критериям данного элемента относится определение области применения процесса менеджмента риска с учетом понимания внешней и внутренней среды организации, а также критериев для оценки значимости риска и поддержки процессов принятия решений (шкал оценок, уровней эскалации риска) и др.

Элемент 3. Идентификация риска

К критериям данного элемента относятся разработка и внедрение методов по идентификации рисков применительно к целям организации исходя из области применения процесса менеджмента риска и среды организации, идентификация как угроз, так и возможностей, и др.

Элемент 4. Анализ риска

К критериям данного элемента относятся определение и применение подхода к формулированию и документированию риска, включая его источники, последствия, вероятность и сценарии реализации, взаимосвязь с другими рисками, использование ключевых индикаторов риска и др.

Элемент 5. Оценивание риска

К критериям данного элемента относятся наличие формализованного подхода к оцениванию риска, включая как качественные (экспертные), так и количественные методы, определение величины текущего и остаточного риска на основе выбранных методов, подхода к ранжированию рисков исходя из установленных критериев и др.

Элемент 6. Воздействие на риск

К критериям данного элемента относятся определение подходов к выбору способов воздействия на риск и формированию мероприятий по воздействию на риски/плана воздействия на риск (разработке, реализации, контролю сроков, стоимости и эффективности), проведение анализа затрат и результатов от выполнения мероприятий по воздействию на риски и др.

Элемент 7. Мониторинг и пересмотр

К критериям данного элемента относятся наличие установленного порядка постоянного мониторинга и периодического пересмотра процесса менеджмента риска и его результатов (включая анализ причин и последствий риска в случае его реализации, пересмотр мероприятий по управлению риском и др.).

Элемент 8. Документирование и отчетность

К критериям данного элемента относятся регламентация форм и сроков формирования отчетности по рискам, доведение информации по деятельности по менеджменту риска и ее результатах по всей организации, предоставление необходимой информации для принятия решений.

К преимуществам данного подхода можно отнести:

- возможность последовательного проведения оценки процесса менеджмента риска на примере конкретного риска;
- относительную простоту сбора документального подтверждения для каждого элемента процесса менеджмента риска;
- достаточный уровень объективности и конкретности критериев;
- возможность проведения сравнительного анализа (бенчмаркинга) с другими компаниями на основе открытых данных.

К ограничениям данного подхода можно отнести продолжительность и сложность оценки для крупных организаций ввиду большого количества направлений деятельности, в которых должен быть внедрен процесс менеджмента риска.

5.2 Подход на основе ключевых принципов менеджмента риска

Концепция данного подхода определяет, что эффективный менеджмент риска в целом должен удовлетворять необходимому и достаточному набору принципов или характеристик в соответствии с ГОСТ Р ИСО 31000—2019 (раздел 4). Оценка, основанная на этих принципах, позволит проанализировать, насколько они соблюдаются в организации:

- интегрированность. Интегрированный менеджмент риска является неотъемлемой частью всей деятельности организации;
- структурированность и комплексность. Структурированный и комплексный подход к менеджменту риска способствует согласованным и сопоставимым результатам;
- адаптированность. Инфраструктура и процесс менеджмента риска настраиваются и соразмерны внешней и внутренней среде организации, ее целям;
- вовлеченность. Заключается в надлежащем и своевременном участии причастных сторон, что позволяет учитывать их знания, взгляды и мнения. Это приводит к повышению осведомленности и информативности в рамках менеджмента риска;
- динамичность. Риски могут возникать, меняться или исчезать по мере изменения внешней и внутренней среды организации. Менеджмент риска предвосхищает, обнаруживает, признает и реагирует на эти изменения и события соответствующим и своевременным образом;
- базирование на наилучшей доступной информации. В качестве исходных данных используются исторические и текущие данные, а также прогнозные ожидания. Менеджмент риска последовательно анализирует и учитывает любые ограничения и неопределенности, связанные с исходными данными и ожиданиями. Информация должна быть актуальной, ясной и доступной для всех причастных сторон;
- учет поведенческих и культурных факторов. Поведение и культура человека существенно влияют на все аспекты менеджмента риска на каждом уровне и этапе;
- непрерывное улучшение. Менеджмент риска постоянно улучшается благодаря обучению и накоплению опыта.

К преимуществам данного подхода можно отнести:

- возможность оценки менеджмента риска в организациях, которые не акцентируют внимание на полной формализации процесса менеджмента риска;
- возможность формирования выводов о менеджменте риска на основе закрытого перечня принципов.

К ограничениям данного подхода можно отнести относительно высокий уровень субъективности восприятия принципов и отсутствие универсальных способов документального подтверждения их применения.

5.3 Подход на основе модели зрелости менеджмента риска

Подход на основе модели зрелости менеджмента риска исходит из утверждения, что качество менеджмента риска организации должно со временем улучшаться и часто занимает как минимум несколько лет, а менеджмент риска на низком уровне зрелости приносит очень небольшую отдачу от вложенных в него ресурсов и нередко может восприниматься как расходы на соблюдение применимых комплаенс-обязательств или как обязательная надстройка, скорее направленная на формирование отчетности по рискам, чем на эффективное воздействие на них. Эффективный менеджмент риска развивается с течением времени, при этом дополнительная польза создается на каждом новом этапе развития. Данный подход направлен на анализ положения менеджмента риска организации на общей кривой зрелости менеджмента риска сопоставимых организаций, чтобы Совет и высшее руководство могли оценить, соответствует ли он текущим потребностям организации и достигает ли он ожидаемой зрелости.

Фактическая деятельность в рамках менеджмента риска оценивается по выбранным критериям с использованием выбранной системы измерения зрелости, в которой в том числе учитываются намерения и заявления участвующих сторон по организации менеджмента риска, но высокий балл может быть получен только при полном внедрении и практическом применении менеджмента риска. Возможная модель измерения зрелости показана ниже в таблице 1.

Таблица 1 — Пример модели измерения зрелости

Уровни зрелости				
Базовый	Развивающийся	Устоявшийся	Продвинутый	Эталонный
Менеджмент риска находится на начальном уровне развития, непоследовательно применяется в рамках всей организации. Остаются значительные возможности для улучшения	Менеджмент риска применяется более развернуто, но используется непоследовательно и понимается в основном только Советом, высшим руководством организации и соответствующими сотрудниками, имеющими к этому непосредственное отношение. Сохраняются значительные возможности для улучшения	Менеджмент риска определен и закреплен, но не всегда применяется Советом, высшим руководством организации, а также сотрудниками в отдельных ключевых областях/сферах деятельности. Сохраняются умеренные возможности для улучшения	Менеджмент риска в значительной мере хорошо понимается и последовательно применяется Советом, высшим руководством и сотрудниками в рамках всей организации. Сохраняются ограниченные возможности по улучшению	Менеджмент риска соответствует ведущим практикам, последовательно, комплексно применяется и внедряется в рамках всей организации. Данная сфера деятельности рассматривается как ведущая практика и может быть использована как для внутреннего, так и внешнего сравнения

Ключевым аспектом подхода на основе модели зрелости является увязка результатов менеджмента риска и прогресса в выполнении плана менеджмента риска с системой измерения и управления эффективностью организации. Результаты работы данной системы могут быть представлены высшему руководству и Совету как свидетельство развития менеджмента риска.

К преимуществам данного подхода можно отнести:

- возможность адаптации критериев оценки на основе модели измерения зрелости в зависимости от запроса заинтересованных сторон или необходимости глубины проводимого анализа без прямой привязки к принципам или элементам процесса менеджмента риска;
- возможность учета дополнительных факторов (например, внешних требований к менеджменту риска в организациях отдельных секторов экономики) в рамках используемой модели измерения зрелости.

К ограничениям данного подхода можно отнести следующие:

- направленность на понимание зрелости не в полной мере отвечает цели по оценке эффективности менеджмента риска, т. к. зрелый менеджмент риска с высоким уровнем формализации не всегда подтверждает его эффективность;

- сопоставимость полученных результатов при использовании универсальной модели измерения зрелости ограничена.

6 Методы сбора информации и доказательств

Объем документации менеджмента риска организации будет варьироваться в зависимости от ее размера и комплексности. В более крупных организациях обычно есть формализованные руководства и инструкции, раскрывающие и дополняющие политику менеджмента риска, организационные схемы, должностные инструкции, блок-схемы информационных систем и т. д. Организации меньших размеров обычно имеют значительно меньше документации.

В таких случаях отдельные аспекты менеджмента риска могут быть неформальными и недокументированными, но при этом выполняться регулярно и эффективно. Подобные действия можно тестировать так же, как и задокументированные действия. Тот факт, что элементы менеджмента риска не задокументированы, не обязательно означает, что они неэффективны или не могут быть оценены. В то же время соответствующий потребностям организации уровень документации, как правило, делает мониторинг более эффективным. Это полезно и в других отношениях: документирование облегчает сотрудникам понимание того, как работает процесс, и их конкретные роли, а также упрощает внесение изменений при необходимости.

Принимая решение задокументировать сам процесс оценки, оценщик обычно опирается на существующее документирование менеджмента риска организации. Существующее документирование обычно дополняется наблюдениями, подготовленными оценщиком, включая доказательства проверок и анализов, выполненных в процессе оценки. Для получения доказательств оценщик может использовать различные методы, в том числе:

- очные наблюдения — например присутствуя при реализации деятельности по менеджменту риска на разных уровнях организации: от заседаний Совета до программ и проектов, работы отдельных подразделений и сотрудников;
- интервью;
- изучение документов — например, повесток заседаний, подтверждающих документов и протоколов Совета, коллегиального исполнительного органа и других коллегиальных органов организации, стратегических планов и подтверждающих документов по решениям о выделении ресурсов;
- изучение и использование результатов предыдущих оценок;
- аналитические методы — например, анализ первопричин обнаруженных областей для совершенствования;
- построение карты процесса;
- статистический анализ — например, анализ типов происшествий или предаварийных ситуаций;
- верификация и оценка моделей рисков;
- проведение опросов/анкетирования;
- анализ самооценки контрольных процедур.

Нередко в рамках сбора достаточной информации и доказательств для формирования заключения также используется комбинация различных методов. Оценщик выбирает наиболее подходящие для выполняемой оценки методы. Оценщик также оценивает наличие достаточных ресурсов и навыков для выполнения всей работы, необходимой для обеспечения достаточного обоснования заключения. Оценщик должен проанализировать, может ли быть разумным отказаться от выражения мнения или добавить оговорку за счет исключения определенных областей или рисков из объема мнения, если у него отсутствуют достаточные ресурсы или навыки.

Выводы оценщика должны быть фактическими, объективными и подкрепляться достаточными доказательствами. Достаточность подразумевает, что доказательства являются фактическими, адекватными и убедительными, чтобы разумный, информированный человек пришел к тем же выводам, что и оценщик. Свидетельства оценки должны быть надлежащим образом задокументированы и организованы.

В случае если высшее руководство намеревается сделать заявление внешним сторонам об эффективности менеджмента риска, ему следует рассмотреть возможность разработки и сохранения документации в поддержку этого заявления. Характер и объем документирования оценщика обычно более существенны, когда результаты оценки будут раскрываться внешним сторонам. Такая документация может быть полезна, если результаты оценки впоследствии будут оспорены.

7 Формирование интегральной оценки менеджмента риска и рекомендаций по улучшению

Вне зависимости от выбранного подхода к оценке, по результатам ее проведения оценщик формулирует общий вывод (мнение) о качестве менеджмента риска, который должен быть доведен до сведения Совета, высшего руководства и, при необходимости, иных заинтересованных сторон. Данный вывод представляет собой интегральную оценку по выбранной шкале измерения, отражающей степень эффективности и надежности менеджмента риска (например, «менеджмент риска в целом эффективен и надежен» — «менеджмент риска эффективен с ограничениями» — «менеджмент риска неэффективен»). Структура и описание шкалы измерения определяются оценщиком и должны быть в достаточной степени понятны, конкретны и информативны для исключения недопониманий, расхождения во взглядах о положении интегральной оценки на ней. Оценщику рекомендуется документировать вывод и выбранную шкалу измерения.

Вместе с общим выводом оценщик также формулирует и документирует рекомендации по дальнейшему улучшению менеджмента риска. Высшему руководству организации следует на основе данных рекомендаций разработать план (программу) развития улучшения менеджмента риска либо включить их в существующий план и назначить ответственных за их реализацию с последующим мониторингом их выполнения. После внедрения эти улучшения должны способствовать совершенствованию менеджмента риска.

УДК 658.5.011 ОКС 03.100.01

Ключевые слова: риск, менеджмент риска, качество менеджмента риска, эффективность менеджмента риска, надежность менеджмента риска, процесс менеджмента риска, инфраструктура менеджмента риска, принципы менеджмента риска, зрелость менеджмента риска

Редактор *З.А. Лиманская*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 14.09.2022. Подписано в печать 28.09.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,24.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru