

«Одобрено»
Комитетом ПАРТАД по внутреннему контролю,
внутреннему аудиту и управлению рисками
(протокол № 4/2018 от 21.12.2018)

РУКОВОДСТВО ПО УПРАВЛЕНИЮ РИСКАМИ

2018

СОДЕРЖАНИЕ:

РАЗДЕЛ 1. Область применения	3
РАЗДЕЛ 2. Методы оценки рисков	4
РАЗДЕЛ 3. Порядок признания рисков значимыми	9
РАЗДЕЛ 4. Ключевые индикаторы рисков	11
РАЗДЕЛ 5. Методы определения ограничений рисков (определение риск – аппетита организации)	12
РАЗДЕЛ 6. Проведение самооценки	13
РАЗДЕЛ 7. Способы оценки эффективности системы управления рисками	15
РАЗДЕЛ 8. Обмен информацией о рисках. Отчетность по системе управления рисками	21
Приложения:	
1. Пример классификации рисков организации	22
2. Пример выбора методов оценки риска в зависимости от вида риска	27
3. Примеры шкал оценки размера потенциального ущерба и вероятности наступления риска	31
4. Пример оценки и признания кредитного риска значимым с использованием Матрицы рисков	33
5. Пример ключевых индикаторов рисков	35
6. Пример определения риск – аппетита в балльном эквиваленте	42
7. Пример проведения самооценки	43
8. Пример оценки соответствия системы управления рисками принципам и компонентам COSO ERM	50
9. Пример состава отчетности и иных внутренних документов организации в рамках системы управления рисками	62
10. Пример Реестра рисков	67

РАЗДЕЛ 1. Область применения

Настоящее Руководство по управлению рисками (далее - Руководство) разработано в развитие Внутреннего стандарта ПАРТАД по управлению рисками и внутреннего контроля в целях методологической поддержки членов ПАРТАД по вопросам управления рисками.

Особый акцент в Руководстве сделан на практических примерах организации системы управления рисками.

Руководство не является обязательным для применения членами ПАРТАД (далее по тексту – организация) и может быть использовано при разработке внутренних документов организации по системе управления рисками.

РАЗДЕЛ 2. Методы оценки рисков

Оценка рисков позволяет организации учитывать, в какой степени события могут оказать влияние на достижение ее целей.

Оценка риска состоит из идентификации риска, его анализа и сравнительной оценки риска¹.

Для этого используется количественные или качественные методы оценки, либо их сочетание.

Методы качественной оценки часто используются в случаях невозможности количественного определения рисков, а также в случаях, когда достаточно надежные данные, требуемые для количественной оценки, либо нельзя получить, либо получение и анализ таких данных оказываются слишком дорогостоящими. Методы количественной оценки, как правило, требуют большей точности и используются в отношении более сложных и комплексных видов деятельности в дополнение к качественным методам. Качественные методы являются наиболее подходящими в отношении рисков, данными об истории проявления и частоте изменчивости которых располагает организация и которые, вследствие этого, можно надежно спрогнозировать.

К основным методам оценки рисков можно отнести следующие:

Качественные методы оценки:

Мозговой штурм

Метод «мозгового штурма» (brainstorming) – это метод коллективной генерации идей, применяемый при решении ряда задач, требующих нетривиальных подходов. Относится к методам экспертных оценок, так как предполагает участие группы лиц, являющихся специалистами в определенной области.

Как правило, участниками «мозговых штурмов», проводимых для целей управления рисками, выступают представители топ-менеджмента, хотя возможно привлечение экспертов, особенно при идентификации и оценке специфических рисков. Рекомендуемое количество участников – 8-10 человек. Малое число участников может привести к вялости дискуссии и низкой эффективности процесса, большое – к сложностям регулирования дискуссии и фиксации идей.

«Мозговой штурм» может быть использован в сочетании с другими методами оценки рисков, или самостоятельно как метод стимулирования креативного мышления на любом этапе процесса управления рисками.

Структурированные или частично структурированные интервью

¹ В соответствии со стандартом ИСО/МЭК 31010:2009 «Менеджмент риска. Методы оценки риска» (ISO/IEC 31010:2009 «Risk management — Risk assessment techniques»).

Представляет собой риск-интервью – опрос владельцев рисков с целью выявления и оценки рисков, входящих в сферу их компетенции. Метод является одним из наиболее понятных и доступных, но, тем не менее, достаточно сложным в применении.

Структурированные и частично структурированные интервью полезны в ситуациях, когда трудно собрать людей для обсуждения или когда свободное обсуждение в группе невозможно. Данные виды интервью чаще всего используют как часть процесса анализа риска для идентификации опасностей или оценки эффективности средств управления. Структурированные и частично структурированные интервью могут быть использованы при сборе входных данных для оценки риска причастными сторонами.

Структурированное риск-интервью – это опрос, проводимый с помощью специально разработанной анкеты. Вопросы, не включенные в анкету или опросный лист, не задаются. Вопросы в основном закрытого типа.

Полуструктурированное риск-интервью содержит перечень вопросов для ответов в свободной форме либо список тем, которые необходимо охватить. Порядок вопросов может быть заданным или произвольным.

Неструктурированное риск-интервью – свободная беседа на заданную тему. Может использоваться на начальных этапах построения системы управления рисками, для определения контекста и знакомства с организацией.

Метод Дельфи

Метод Дельфи – процедура, предназначенная для получения согласованного мнения группы экспертов. В процессе управления рисками может применяться для идентификации и оценки рисков, когда требуется обоснованная и согласованная экспертная оценка. Экспертная оценка – это не частное мнение профессионала в определенной области, а результат, полученный с применением формальной процедуры, позволяющей не только получить единое мнение целой группы экспертов, но и вычислить степень согласованности отдельных точек зрения. Метод Дельфи – самая распространенная и известная из таких процедур.

Общая схема проведения экспертизы по методу Дельфи состоит в следующем. На первом туре эксперты дают ответы на поставленные вопросы, как правило, без аргументации. Ответы обрабатываются, определяются их статистические характеристики (средняя, среднеквадратическое отклонение, крайние значения ответов) и результаты обработки сообщаются экспертам. После этого проводится второй тур опроса, в ходе которого эксперты должны объяснить, почему они изменили или не изменили своего мнения. Данные обработки результатов второго тура опроса и аргументация ответов с сохранением анонимности снова сообщаются экспертам перед проведением третьего тура опроса. Последующие туры проводятся по такой же схеме. Подобная организация экспертизы позволяет экспертам учесть в своих ответах

новые для них обстоятельства и в то же время избавляет их от какого бы то ни было давления при отстаивании своей позиции.

Контрольные листы

Контрольные листы – это списки опасностей, рисков и сбоев в управлении. Они составляются на основе опыта работы, либо как результат предшествующей оценки рисков, либо по результатам сбоев, которые случались раньше.

Контрольные списки могут применяться для идентификации опасностей и рисков, или для оценки эффективности управления рисками. Они могут являться дополнением другого метода оценки рисков, и наиболее полезны для проверки, все ли было охвачено при применении более творческих методик, выявляющих новые проблемы (например, для определения, все ли риски были идентифицированы в процессе «мозгового штурма», не выпали ли из рассмотрения «стандартные» риски при поиске рисков новых).

Анализ воздействия на бизнес

Метод анализа воздействия на бизнес (BIA) позволяет исследовать, как ключевые виды отказов/нарушений/разрушений могут повлиять на ключевые виды деятельности и процессы организации, а также идентифицировать и количественно определить необходимые возможности для управления организацией в этих условиях. Процесс метода BIA обеспечивает согласование и понимание:

- идентификации и критичности ключевых бизнес-процессов, функций, связанных ресурсов и ключевых взаимосвязей, существующих в организации;
- влияния отказов/нарушений/разрушений на возможности организации достигать установленных целей бизнеса;
- необходимых возможностей управления воздействием отказов/нарушений/разрушений и восстановлением нормального хода деятельности организации.

Количественные методы оценки:

Метод Value at Risk (Var)

Var – это выраженная в денежных единицах оценка величины, которую не превысят ожидаемые в течение данного периода времени потери с заданной вероятностью.

Для точного вычисления необходимо знать функции распределения портфельной прибыли в течение определенного временного промежутка. Чаще всего вычисление величины VaR осуществляется для периода от одного до десяти дней. При этом уровень достоверности очень высок – до 99%.

Анализ чувствительности

Сводится к исследованию зависимости некоторого результирующего показателя от вариации значений показателей, участвующих в его определении. Иными словами, этот метод позволяет получить ответы на вопросы вида: что будет с результирующей величиной, если изменится значение некоторой исходной величины.

Например, анализ чувствительности применяется в исследовании влияния изменения основных параметров проекта на его экономическую эффективность и в расчёте критических значений этих параметров.

Анализ чувствительности проводится для определения степени влияния варьируемых факторов на финансовый результат проекта, который характеризует рассмотренные выше показатели эффективности инвестиций. В качестве варьируемых можно принять следующие факторы: уровень инфляции, ставки налогов, объем инвестиций, задержки платежей, потери при продажах, прямые издержки, отсрочки оплаты прямых издержек, общие издержки, заработная плата персонала, ставки по депозитам и по кредитам, ставка дисконтирования.

В процессе анализа чувствительности может изменяться в определенном диапазоне значение одного из варьируемых факторов при фиксированных значениях остальных и определяется зависимость показателей эффективности от этих изменений. Максимальный диапазон изменений лежит в пределах от -100% до +100%.

Сценарный анализ

Основной принцип действия данного метода заключается в моделировании возможных ситуаций и последующей количественной оценке рисков на основе выводов, сделанных по результатам моделирования, т.е. какая-либо конкретная ситуация сравнивается с другой (обычно выборы «плохих» и «хороших» обстоятельств сравниваются с наиболее вероятными обстоятельствами).

Он позволяет оценить потенциальное одновременное воздействие ряда факторов риска на деятельность организации в случае наступления экстремального, но вместе с тем вероятного события.

Анализ начинается с оценки базового случая (наиболее вероятные значения входящих переменных), затем подбираются показатели, характерные для «плохого» стечения обстоятельств (высокие переменные затраты и т.д.) и для «хорошего». При этом отклонения параметров рассчитываются с учетом корреляции между ними.

Стресс-тестирование

Стресс-тестирование (Stress Testing) является методом количественной оценки риска, который заключается в определении величины несогласованной позиции, которая подвергает организацию риску и в определении шоковой величины изменения внешнего фактора — валютного курса, процентной ставки и тому подобное. Сочетание этих величин дает представление о том, какую сумму убытков или доходов получит организация, если события будут развиваться по заложенным предположениям.

При выборе сценария стресс-тестирования организация может исходить из следующего:

- стресс-тестирование должно охватывать все значимые для организации риски и направления деятельности;
- сценарии стресс-тестирования должны учитывать события, которые могут причинить максимальный ущерб организации или повлечь потерю деловой репутации.

В международной практике используются различные методики стресс-тестирования. В настоящее время наиболее распространенной методикой является сценарный анализ (на основе исторических или гипотетических событий). Также проводится анализ чувствительности портфеля активов к изменению факторов риска и рассчитываются максимальные потери.

Смешанные методы оценки

Матрица последствий и вероятностей

Данный метод предполагает расположение ранжированных показателей последствий и вероятностей в виде таблицы (матрицы). При заранее сформированной матрице последствий и вероятностей предполагается отнесение в одну из ячеек матрицы. В зависимости от места оцененного риска в матрице делается вывод о его допустимости либо недопустимости.

Формат, строки и колонки матрицы зависят от области применения, при этом очень важно, чтобы разработанная матрица соответствовала специфике деятельности организации.

Приведенный перечень методов оценки рисков не является исчерпывающим. По усмотрению организации могут применяться иные методы оценки рисков².

В Приложении 2 приведены варианты применения методов оценки рисков в зависимости от вида рисков.

² Подробно Методы оценки рисков рассматриваются в стандарте ИСО/МЭК 31010:2009 «Менеджмент риска. Методы оценки риска» (ISO/IEC 31010:2009 «Risk management — Risk assessment techniques»).

РАЗДЕЛ 3. Порядок признания рисков значимыми

В целях проведения оценки рисков, а также их последующего ранжирования по уровню значимости может использоваться Матрица последствий и вероятностей (Матрица рисков). Матрица рисков учитывает как вероятность наступления рискового события, так и последствия от реализации рисков.

Матрица рисков может быть организована в табличной форме, где строки и столбцы представляют шкалы значений оценок последствий и вероятностей, а их пересечение позволяет количественно оценить тот или иной вид риска. В таблице 1 приведен пример Матрицы рисков.

Таблица 1

Матрица рисков

Размер потенциального ущерба	Критический	2	2	3	3	3
	Высокий	2	2	2	3	3
	Средний	1	2	2	2	3
	Низкий	1	1	2	2	2
	Незначительный	1	1	1	2	2
		Невероятно	Редко	Маловероятно	Возможно	Вероятно
	Вероятность					

Примеры Шкал оценки размера потенциального ущерба и вероятности реализации риска в организации приведены в Приложении 3. Если к какому-то виду риска применимы несколько видов ущерба, для окончательной оценки риска может быть использован тот вид ущерба, величина которого окажется выше.

В Матрице рисков (Таблица 1) выделяются три области:

- риски высокого уровня (3);

Комитет ПАРТАД по внутреннему контролю, внутреннему аудиту и управлению рисками

- риски среднего уровня (2);
- риски низкого уровня (1).

Внутренними документами организации в области управления рисками определяется, какие риски в соответствии с проводимой оценкой являются значимыми для организации.

В Приложении 4 приведен пример оценки и признания кредитного риска значимым с использованием Матрицы рисков.

РАЗДЕЛ 4. Ключевые индикаторы рисков

Для определения источников (факторов) риска организация может использовать количественные или качественные показатели, характеризующие концентрацию рисков. Данные показатели именуются ключевыми индикаторами рисков (КИР).

КИР позволяют оценить эффективность системы управления рисками и качество принятых мер в рамках системы управления рисками. Появление негативных сигналов от КИР, как правило, свидетельствует о возрастании вероятности реализации риска. Соответственно, предотвратить такую опасность можно через усиление контроля над ситуацией.

Все КИР проходят этап адаптации и тестирования. В процессе функционирования системы управления рисками КИР могут корректироваться. КИР могут разрабатываться Должностным лицом, ответственным за организацию системы управления рисками, совместно с руководителями структурных подразделений и утверждаться руководителем организации.

Тестирование КИР может проводиться с помощью системы внутренних рейтингов (например, путем присвоения баллов от 1 до 5). При этом КИР, относящиеся к определенному структурному подразделению, оцениваются сотрудниками именно этого подразделения. Средний балл по каждому КИР соотносится со шкалой, установленной в организации. Например, КИР, набравшие средний балл менее 3, исключаются из дальнейшего анализа.

В результате проведенного анализа КИР для каждого вида риска можно определить 1-2 КИРа. Для мониторинга каждого КИР может назначаться ответственное лицо.

Для КИР, как правило, устанавливается пороговое значение, при превышении которого требуется изменение меры реагирования на данный риск.

Пример ключевых индикаторов рисков приведен в Приложении 5.

РАЗДЕЛ 5. Методы определения ограничений рисков (определение риск – аппетита организации)

В целях определения ограничений рисков можно выделить качественные и количественные методы. Организацией могут определяться ограничения рисков, как по каждому виду риска, так и по совокупному риску (риск – аппетит).

Наиболее информативным является количественный метод определения ограничений рисков (в денежном эквиваленте), однако его применение возможно только в том случае, если есть возможность оценить финансовый ущерб от реализации рисков, в том числе потенциальный.

Нефинансовые риски, включающие операционные риски, как правило, невозможно свести к величине денежного эквивалента. Поэтому в случаях, когда оценить финансовый ущерб не представляется возможным, применяется качественный метод определения ограничений рисков.

Риск – аппетит организации также может быть определен как в денежном эквиваленте (например, в процентном отношении от размера собственных средств, в процентном отношении от размера прибыли или иного финансового показателя), так и в форме балльной оценки либо иным способом, принятым в организации. При этом сведение воедино ограничений финансовых и нефинансовых рисков может проводиться, в том числе следующим образом:

1. приведение нефинансовых рисков к денежному эквиваленту;
2. приведение денежного эквивалента оценки финансового риска к балльным эквивалентам.

Пример определения риск – аппетита в балльном эквиваленте приведен в Приложении 6.

РАЗДЕЛ 6. Проведение самооценки

Основными целями самооценки являются:

- Идентификация основных операционных рисков, характерных для финансовых услуг, бизнес - процессов и систем, относящихся к основной деятельности организации;
- Выполнение оценки в рамках операционных рисков для каждого из выявленных рисков;
- Выявление отсутствующих, несовершенных либо устаревших процедур контроля в разрезе бизнес - процессов структурных подразделений и разработка плана корректирующих мероприятий по ограничению/снижению выявленных операционных рисков;
- Формирование инструментов управления операционными рисками.

Подготовка к проведению самооценки может состоять из следующих шагов:

- Разработка форм документов для проведения самооценки;
- Определение уполномоченных сотрудников структурных подразделений, ответственных за проведение самооценки (далее – ответственные сотрудники);
- Разработка порядка взаимодействия структурных подразделений с должностным лицом/структурным подразделением, ответственным за организацию системы управления рисками, в процессе проведения самооценки;
- Консультация ответственных сотрудников и/или руководителей структурных подразделений, которые могут быть определены в качестве лиц, ответственных за проведение самооценки в рамках подчиненного подразделения.

Объектами самооценки являются операционные риски, применяемые в отношении них контрольные процедуры и ограничения операционных рисков (ключевые индикаторы риска) (при необходимости).

В процессе проведения самооценки могут участвовать: должностное лицо/структурное подразделение, ответственное за организацию системы управления рисками; руководители и ответственные сотрудники структурных подразделений, иные сотрудники организации.

Роль должностного лица/структурного подразделения, ответственного за организацию системы управления рисками, в процессе проведения самооценки может состоять в следующем:

- Разработка методологии (порядка) проведения самооценки;
- Разработка структуры и формы Анкеты для проведения самооценки (далее – Анкета)/иного документа, применяемого в организации в целях проведения самооценки;

Комитет ПАРТАД по внутреннему контролю, внутреннему аудиту и управлению рисками

- Определение сроков проведения самооценки и перечня структурных подразделений, в которых планируется проведение самооценки;
- Подготовка перечня ответственных сотрудников структурных подразделений;
- Консультирование ответственных сотрудников по вопросам заполнения Анкеты/иного документа, применяемого в организации в целях проведения самооценки;
- Анализ агрегированных результатов самооценок структурных подразделений организации и разработка рекомендаций по операционным рискам по итогам самооценки;
- Подготовка соответствующей отчетности по проведению самооценки;
- Информирование заинтересованных подразделений о результатах самооценки;
- Иное.

Роль руководителя структурного подразделения в процессе проведения самооценки может состоять в следующем:

- Определение ответственного сотрудника структурного подразделения, либо самостоятельное исполнение функций данного сотрудника;
- Визирование/подписание Анкеты либо иного документа подразделения, формируемого по итогам проведения самооценки;
- Иное.

Роль ответственного сотрудника структурного подразделения в процессе проведения самооценки может состоять в следующем:

- Заполнение форм документов по проведению самооценки;
- Отправка заполненных Анкет(Анкеты подразделения)/иного документа, предназначенного для целей проведения самооценки, должностному лицу/структурному подразделению, ответственному за организацию системы управления рисками, в установленные сроки;
- Разработка планов мероприятий по ограничению/снижению операционных рисков;
- Контроль за исполнением в подразделении мероприятий по ограничению/снижению операционных рисков.
- Иное.

Если ответственный сотрудник в структурном подразделении не определен, то его функции выполняет руководитель соответствующего структурного подразделения.

В Приложении 7_ приведен пример порядка проведения самооценки организации.

РАЗДЕЛ 7. Способы оценки эффективности системы управления рисками

Проведение оценки системы управления рисками для целей ее совершенствования обязательно для профессионального участника рынка ценных бумаг. Периодичность такой оценки, а также критерии оценки нормативными актами Банка России не регламентируются.

Хорошей практикой считается ежегодная оценка системы управления рисками функцией внутреннего/внешнего аудита, а также периодическая оценка системы управления рисками с привлечением внешних экспертов (например, один раз в три года).

Среди способов оценки эффективности системы управления рисками организацией может применяться один или в комплексе несколько из нижеперечисленных способов:

- Оценка соответствия системы управления рисками принципам и компонентам COSO ERM.
- Оценка эффективности системы управления рисками на основе показателей системы управления рисками, разработанных организацией.
- Оценка эффективности посредством анализа результативности деятельности по выявлению нарушений ограничений рисков и их устранению.
- Оценка эффективности управления путем сопоставления выявленных рисков с установленными допустимыми уровнями рисков или по установленным организацией простым критериям эффективности, например, по количеству в течение года однотипных ошибок сотрудников организации – реализовавшихся рисков.
- Оценка эффективности системы управления рисками, включая такие элементы как оценка затрат на финансирование системы управления рисками; фактических убытков от реализации рисков и возможных потенциальных убытков.
- Оценка эффективности системы управления рисками, построенная на анализе NPV (чистая приведенная стоимость), учитывая ее изменение в зависимости от функционирования системы управления рисками (эффективность внедрения системы управления рисками определяется как разница между NPV, рассчитанной с учетом и без учета функционирования системы управления рисками).
- Иные способы.

Оценка эффективности управления рисками посредством анализа результативности деятельности по выявлению нарушений ограничений рисков и их устранению

В рамках данного метода организация:

Комитет ПАРТАД по внутреннему контролю, внутреннему аудиту и управлению рисками

- сопоставляет выявленные риски с установленными предельными размерами рисков (допустимыми уровнями по видам рисков);
- анализирует перечень мероприятий по снижению рисков или их исключению на предмет его достаточности;
- анализируется исполнение мероприятий по снижению рисков или их исключению.

Организацией может быть установлено как предельное значение отклонения от допустимых уровней по каждому виду риска, так и предельное значение отклонения от установленного риск – аппетита.

Также оценивается уровень исполнения перечня мероприятий по снижению рисков или их исключению.

По итогам проведенной оценки дается заключение об эффективности управления рисками.

Оценка соответствия системы управления рисками принципам и компонентам COSO ERM

Методологической основой данного метода оценки управления рисками, является **методология COSO ERM** – «Управление рисками организации – интегрированная модель», позволяющая выявить проблемные блоки, устранить некорректные процедуры, получить достаточно полную характеристику системы управления рисками.

В качестве критерия эффективности используют соответствие основных элементов систем управления рисками «лучшей практике». В соответствии с предлагаемой методологией эффективность процесса управления рисками является предметом субъективного суждения, которое формируется в результате оценки наличия и функционирования восьми компонентов управления рисками:

- внутренняя среда;
- постановка целей;
- определение событий;
- оценка рисков;
- реагирование на риски;
- средства контроля;
- информация и коммуникация;
- мониторинг.

Необходимо, чтобы все компоненты присутствовали и эффективно функционировали, а риск должен находиться в рамках риск-аппетита, принятого организацией для достижения своих целей, выполнения миссии или реализации стратегии.

Все восемь компонентов процесса управления рисками не могут функционировать одинаково в каждой организации. Их применение в небольших организациях, например, может быть менее формализовано и менее структурировано. В то же время, даже небольшие организации могут иметь эффективную систему управления рисками только в том случае, если каждый из компонентов в ней присутствует и должным образом функционирует.

Для более детальной оценки эффективности управления рисками для каждого компонента определяются соответствующие ему принципы.

При этом оценка уровня реализации каждого принципа управления рисками осуществляется по формуле:

$$\text{Уровень реализации принципа} = \text{Уровень значимости} * \text{Коэффициент реализации}$$

Уровень значимости принципа (в целях проведения оценки эффективности системы управления рисками) задается экспертным путем/определяется высшим руководством.

Уровни значимости принципов управления рисками определяются таким образом, чтобы суммарная значимость всех принципов была равна 1. Суммирование значимостей принципов, реализуемых в рамках конкретного компонента, определяет значимость компонента с точки зрения организации.

Заключение об отсутствии значимости принципа (уровень значимости равен 0), в случае, если оно делается организацией, должно подкрепляться логическим обоснованием, показывающим, каким образом в отсутствие принципа связанный с ним компонент управления рисками может иметься в наличии и работать.

Величина *коэффициент реализации принципа* зависит от наличия/отсутствия выявленных в ходе проведения оценки существенных недостатков системы управления рисками при реализации соответствующего принципа. Шкала значений коэффициентов устанавливается организацией.

На основании суммарного уровня реализации принципов в рамках отдельного компонента делается вывод о степени влияния конкретного компонента на эффективность системы управления рисками.

Если суммарный уровень реализации принципов, относящихся к конкретному компоненту, меньше половины уровня значимости компонента, то уровень его реализации признается

недостаточно обеспечивающим эффективность системы управления рисками, а если равен и больше половины, но меньше максимального значения – не полностью обеспечивающим эффективность системы управления рисками.

Покомпонентная сумма показателей реализации принципов позволяет оценить эффективность системы управления рисками организации по шкале, установленной организацией.

При этом рекомендуется принимать во внимание сам факт *наличия существенных недостатков системы управления рисками, которые* проявляются в рамках покомпонентной оценки реализации принципов.

Существенные недостатки управления рисками в соответствии с настоящей методикой оценки эффективности имеют место, когда принципы управления рисками не определены (не описаны во внутренних документах компании), и (или) определены, но не внедрены, и (или) определены и внедрены, но не выполняются, и (или) эти принципы не работают все вместе. Существенные недостатки в реализации соответствующего принципа не могут быть компенсированы наличием, приемлемым уровнем или функционированием других принципов.

В Приложении 8 приведен пример оценки соответствия системы управления рисками принципам и компонентам COSO ERM.

Оценка эффективности системы управления рисками на основе показателей системы управления рисками

В рамках данного способа оценки эффективности системы управления рисками определяются:

- показатели системы управления рисками, на основании которых определяется ее эффективность;
- механизм сбора данных, позволяющих оценить уровень достижения результатов/показателей по системе управления рисками;
- порядок анализа показателей системы управления рисками и применение результатов указанного анализа.

Значение каждого показателя в целях оценки эффективности системы управления рисками рассчитывается по формуле:

Значение показателя = Уровень значимости показателя*Коэффициент реализации

Уровень значимости показателя задается экспертным путем таким образом, чтобы суммарная значимость всех показателей была равна 1.

Величина коэффициента реализации показателя зависит от наличия/отсутствия выявленных в ходе оценки недостатков системы управления рисками. Шкала значений коэффициентов реализации устанавливается организацией.

Сумма значений всех показателей позволяет оценить эффективность системы управления рисками по шкале, определенной в организации.

Рассмотрение результатов оценки эффективности управления рисками и действия, предпринимаемые для устранения выявленных недостатков

По итогам оценки эффективности даются рекомендации по развитию системы управления рисками, устранению нарушений и т.д.

Результаты оценки эффективности системы управления рисками (отчет) предоставляются высшему руководству организации в установленные внутренними документами сроки и порядке для принятия соответствующих решений.

Поручения высшего руководства по итогам рассмотрения результатов проведенной оценки доводятся до сведения должностных лиц, ответственных за функционирование бизнес – процессов, руководителей подразделений внутреннего контроля и управления рисками в порядке и сроки, определенные внутренними документами организации.

Исполнительному органу организации необходимо организовать разработку и утвердить план мероприятий по устранению замечаний, сформулированных по результатам оценки с учетом содержащихся в ней рекомендаций, с указанием ответственных должностных лиц организации и сроков устранения замечаний.

Реализация исполнения плана мероприятий по учету результатов оценки эффективности системы управления рисками может состоять из следующих процедур:

- направление информации о нарушениях/недостатках, выявленных по результатам оценки руководителям подразделений/должностным лицам организации, ответственным за принятие мер по устранению выявленных недостатков;
- осуществление обратной связи с руководителями подразделений/должностными лицами организации по ходу исполнения плана мероприятий, внесение при необходимости уточнений в указанный план;

Комитет ПАРТАД по внутреннему контролю, внутреннему аудиту и управлению рисками

- получение от руководителей структурных подразделений/должностных лиц сведений об устранении выявленных в ходе оценки недостатков;
- контроль устранения выявленных нарушений/недостатков (в случае необходимости).

С учетом анализа всех показателей системы управления рисками органами управления принимается решение о формировании бюджета (увеличение/уменьшение) на следующий период.

РАЗДЕЛ 8. Обмен информацией о рисках. Ответность по системе управления рисками

Организация в рамках обмена информацией о рисках обеспечивает выполнение следующих мероприятий:

- обмен информацией о рисках между сотрудниками структурных подразделений, их руководителями, Должностным лицом, ответственным за организацию системы управления рисками, и руководством организации, в том числе доведение Плана мероприятий по снижению рисков и информации о его реализации, а также информации об ограничениях рисков и нарушениях ограничений рисков до сведения руководства организации;
- составление и представление на рассмотрение руководству организации отчетов о результатах осуществления в рамках организации системы управления рисками процессов и мероприятий в целях обеспечения эффективности функционирования системы управления рисками, принятия решений по вопросам развития (совершенствования) системы управления рисками.

Ответность, формируемая в рамках управления рисками, предназначена для полноценного и прозрачного обмена информацией и отчетными материалами между всеми участниками системы управления рисками, а также для информирования о рисках в установленном формате должностных лиц, принимающих управленческие решения, и направлена на достижение конечных целей и задач управления рисками организации.

В формировании внутренних отчетных документов и обмене информацией в рамках документооборота, действующего у организации по системе управления рисками, могут принимать участие все сотрудники организации в целях обеспечения реализации систематического, квалифицированного и качественного контроля за достижением целей и задач системы управления рисками, обеспечения непрерывности контроля динамики изменения показателей, характеризующих риски организации, контроля выполнения Плана мероприятий, оценки эффективности системы управления рисками.

В Приложении 9 приведен пример состава отчетности и иных внутренних документов организации в рамках системы управления рисками.

В Приложении 10 приведен пример Реестра рисков организации.

Пример Классификации рисков организации

Операционные риски

1. Риски персонала (служебные риски) – риски возникновения убытков, причинами реализации которых являются ненадлежащие действия работников, в том числе:

- неисполнение (ненадлежащее исполнение) сотрудниками своих должностных обязанностей вследствие недостаточной квалификации или служебной халатности, включая риск неисполнения (ненадлежащего исполнения) поручений (распоряжений) клиентов, в том числе при осуществлении ЭДО;
- совершение сотрудниками действий, не входящих в область их компетенции (превышение служебных полномочий);
- совершение сотрудниками непреднамеренных ошибок (ошибочных действий);
- мошеннические действия персонала – совершение сотрудниками умышленных действий (в том числе в сговоре с внешними лицами), включая совершение действий с использованием поддельных ценных бумаг и/или документов, в том числе несанкционированный доступ к компьютерным сетям с целью уничтожения, изменения (искажения) электронных данных, направленных на получение личной выгоды и/или причинение ущерба организации, клиентам;
- утрата (уничтожение, порча, хищение) сертификатов ценных бумаг (в том числе в результате пожара, залива жидкостью) в результате ошибочных, противоправных действий или бездействия сотрудников.
- потеря ключевых сотрудников

2. Риски внешних лиц - риски возникновения убытков, причинами реализации которых являются ненадлежащие действия внешних по отношению к организации лиц, в том числе:

- неисполнение (ненадлежащее исполнение) внешними лицами своих обязательств;
- совершение внешними лицами непреднамеренных ошибок (ошибочных действий) при исполнении своих обязательств;
- совершение внешними лицами умышленных (криминальных) действий с целью причинения ущерба организации, клиентам, включая совершения действий с использованием поддельных ценных бумаг и/или документов, а также несанкционированный доступ к компьютерным сетям с целью уничтожения, изменения (искажения) электронных данных.

3. Риски воздействия внешних событий - риски возникновения убытков, причинами реализации которых являются:

- недостаточные и/или неадекватные средства обеспечения сохранности имущества организации и ее клиентов;
- утрата (уничтожение, порча) имущества и информации организации и ее клиентов, в том числе в результате пожара или залива жидкостью.

4. Коммуникационные риски - риски возникновения убытков, причинами реализации которых являются различного рода нарушения, возникающие при взаимодействии организации с внешними лицами:

- изменение, искажение получаемой/передаваемой информации и документов;
- утрата, порча получаемой/передаваемой информации и документов.

5. Технологические риски - риски возникновения убытков, причиной реализации которых является неэффективность или неадекватность применяемых технологий, в том числе:

- установленного порядка функционирования структурных подразделений, а также порядка действий сотрудников (сбой бизнес-процессов);
- установленного порядка взаимодействия между структурными подразделениями, сотрудниками;
- установленного порядка применения оборудования и технических средств;
- установленного порядка обеспечения информационной безопасности;
- необеспечения (ненадлежащего обеспечения) порядка осуществления ЭДО вследствие неэффективности и/или неадекватности технологий, порядка и способов осуществления ЭДО;
- ненадлежащего функционирования используемых средств криптографической защиты информации (СКЗИ) и иного аппаратно-программного обеспечения;
- необеспечение (ненадлежащее обеспечение) ЭДО вследствие неэффективности системы электронного документооборота (СЭД).

6. Технические риски - риски возникновения убытков, причиной реализации которых является ненадлежащее функционирование используемого оборудования (вычислительной техники, программного обеспечения, иного оборудования и технических средств), в том числе:

- неисполнение оборудованием возложенных на него функций из-за отказов и нарушений в работе;
- самопроизвольные сбои в работе оборудования, включая сбои вычислительной техники и программного обеспечения, приводящие к несанкционированным изменениям данных.

7. Комплаенс-риск (регуляторный) – риски возникновения убытков в связи с применением юридических санкций или санкций органов регулирования, причиной реализации которых является несоблюдения ею законов, инструкций, правил, стандартов саморегулируемой организации или кодексов поведения, касающихся профессиональной деятельности.

8. Риски ОД/ФТ – риски возникновения убытков, причиной реализации которых является вовлечение организации в отмыwanie преступных доходов, в том числе обусловленное совершением клиентом организации операций, направленных на легализацию (отмыwanie) доходов, полученных преступным путем и финансирование терроризма.

9. Организационные риски - риски возникновения убытков, причиной реализации которых является неэффективность сформированной системы организации и управления:

- организационной структуры, устанавливающей состав, подчиненность, взаимосвязи структурных подразделений и должностных лиц;
- распределения функциональных (должностных) обязанностей и полномочий между структурными подразделениями (должностными лицами).

Иные риски

10. Стратегические риски – риски возникновения убытков в результате ошибок (недостатков), допущенных при принятии решений, определяющих стратегию деятельности и развития организации (стратегическое управление), неправильном или недостаточно обоснованном определении перспективных направлений деятельности, отсутствии или обеспечении в неполном объеме необходимых ресурсов (финансовых, материально-технических, людских) и организационных мер (управленческих решений), которые должны обеспечить достижение стратегических целей деятельности организации.

11. Политические риски – риски возникновения убытков, причиной реализации которых является совокупность политических, административных, национальных событий, способных повлечь за собой финансовые и иные потери организации.

12. Отраслевые риски – риски возникновения убытков, причиной реализации которых является изменение бизнес-ситуации (влияние возможного ухудшения ситуации) в отрасли.

13. Репутационные риски (риск потери деловой репутации) – это риски возникновения убытков (снижения доходов) в результате уменьшения числа клиентов организации, вследствие формирования негативного мнения и снижения доверия к финансовому институту у клиентов, контрагентов, акционеров, участников финансового рынка, органов государственной власти, саморегулируемых организаций, негативного представления о качестве оказываемых услуг, финансовой устойчивости или характере деятельности организации в целом.

14. Риски правового регулирования (правовой риск) - риск возникновения убытков организации вследствие неоднозначности толкования норм права.

15. Инновационные риски - это риски возникновения убытков, возникающих при вложении средств в проектирование, разработку и ввод в эксплуатацию новой услуги (продукта).

16. Финансовые риски – риски возникновения убытков (снижения доходов), возникновения дополнительных расходов, причиной реализации которых является инфляция, изменение курсов валют, условий кредитования, ликвидности активов организации, инвестиций организации, а также с формой организации финансово-хозяйственной деятельности организации.

В составе финансового риска выделяется:

16.1. Кредитный риск – риск того, что любое обязанное перед организацией лицо (контрагент, эмитент, заемщик) не исполнит свои обязательства в полной мере либо на требуемую дату, либо в любое время после этой даты.

16.2. Риск ликвидности – риск убытков вследствие неспособности организации обеспечить исполнение обязательств в полном объеме.

Риск ликвидности возникает в результате несбалансированности финансовых активов и финансовых обязательств, в том числе вследствие несвоевременного исполнения финансовых обязательств одним или несколькими контрагентами и/или возникновения непредвиденной необходимости немедленного и единовременного исполнения у организации своих финансовых обязательств.

Риск ликвидности можно условно разделить на три категории:

- Риск текущей (балансовой) ликвидности;
- Риск рыночной ликвидности;
- Риск долгосрочной ликвидности.

Риск текущей (балансовой) ликвидности – это риск нехватки ликвидных средств для выполнения текущих финансовых обязательств. Чем большее количество обязательств имеет организация, чем больше величина гарантированных обязательств, тем большая величина рисков текущей (а также долгосрочной) ликвидности ложится на организацию.

Риск рыночной ликвидности – это риск невозможности реализовать финансовый актив на рынке в требуемые сроки по текущим рыночным котировкам. Риск рыночной ликвидности может усугублять риск текущей ликвидности (кассовых разрывов).

Риск долгосрочной ликвидности – это риск нехватки ликвидных средств для выполнения долгосрочных финансовых обязательств.

16.3. Рыночный риск – это риск возникновения у организации убытков от инвестирования активов в финансовые инструменты вследствие изменения рыночной стоимости данных инструментов.

В составе рыночного риска выделяются:

Фондовый риск – риск несения убытков по финансовым активам вследствие неблагоприятного изменения цен данных активов, прежде всего, для инструментов, обращающихся на фондовом рынке.

Валютный риск – риск возникновения убытков по финансовым активам, выраженным в иностранной валюте или чувствительных к изменению курсов иностранной валюты, вследствие изменения курсов валют.

Процентный риск – риск возникновения убытков по финансовым активам, чувствительным к изменению процентной ставки, вследствие изменения рыночных процентных ставок.

17. Форс-мажорные риски - риски возникновения убытков, причиной реализации которых является возникновение непредотвратимых (форс-мажорных) чрезвычайных ситуаций

техногенного, природного и социального характера, в том числе:

- стихийные бедствия, природные катаклизмы;
- техногенные катастрофы, аварии, поражения компьютерными вирусами;
- массовые беспорядки, забастовки, эпидемии, военные действия, террористические акты.

18. Кастодиальный риск – риск утраты имущества организации или имущества его клиентов вследствие действий или бездействия лица, ответственного за хранение этого имущества и учет прав на это имущество.

19. Коммерческий риск – риск возникновения расходов (убытков), в том числе при уменьшении доходов или превышении расходов над доходами, в результате неэффективного управления организацией, возникновения непредвиденных расходов.

Пример выбора методов оценки риска в зависимости от вида риска

№п/п	Вид риска	Возможное применение методов оценки		
		Качественный	Количественный	Смешанный
1	Операционный риск	Часто применяется качественный экспертный подход. Возможно использование всех методов оценки, приведенных в Разделе 2	Использование вероятностных методов оценки возможно при наличии статистической базы. Численная оценка риска может производиться на основе величины возможных штрафов в случае нарушения законодательства. Оценка стоимости активов (например, в случаях их физического уничтожения или хищения). Оценка остаточной величины незакрытого страхованием риска.	Может применяться Матрица последствий и вероятности, сочетающая экспертную оценку вероятности реализации риска и количественную оценку размеров последствий реализации риска.
2	Кредитный риск	Может применяться. Например, проведение экспертной оценки финансового состояния заемщика/контрагента	Используется наиболее часто. Например, расчет вероятности дефолта эмитентов.	Может применяться
3	Рыночный риск	Экспертная оценка	Используется	Может

№п/п	Вид риска	Возможное применение методов оценки		
		Качественный	Количественный	Смешанный
	(фондовый и валютный)	применяется редко	наиболее часто. Например, анализ стоимости, подверженный риску (Var). Стресс-тестирование или сценарный анализ поведения инструмента.	применяться. Например, сочетание экспертной оценки сценариев изменения рыночной ситуации (процентных ставок, биржевых индексов) с расчетом финансовых результатов для каждого сценария.
4	Правовой риск	Часто применяется качественный экспертный подход. Возможно использование всех методов оценки, приведенных в Разделе 2	Использование вероятностных методов оценки возможно при наличии статистической базы.	Может применяться Матрица последствий и вероятности, сочетающая экспертную оценку вероятности реализации риска и количественную оценку размеров последствий реализации риска.
5	Риск ликвидности	Экспертная оценка применяется в случае невозможности или нецелесообразности	Используется наиболее часто. Для рыночной	Может использоваться. Например, сочетание

№п/п	Вид риска	Возможное применение методов оценки		
		Качественный	Количественный	Смешанный
		применения математического алгоритма расчета	ликвидности проводится анализ уровня ликвидных активов, необходимого для урегулирования обязательств при наступлении срока их погашения; расчет потерь при продаже актива в заданные ограниченные сроки. Для текущей ликвидности проводится расчет показателей сбалансированности потоков по активам и пассивам в будущем для предотвращения кассовых разрывов.	экспертной балльной оценки отдельных факторов ликвидности с расчетом конечного агрегированного численного показателя ликвидности.
6	Кастодиальный риск	Часто применяется качественный экспертный подход. Возможно использование всех методов оценки, приведенных в Разделе 2	Использование вероятностных методов оценки возможно при наличии статистической базы. Численная оценка риска может производиться на основе оценки стоимости утраченного	Может применяться Матрица последствий и вероятности, сочетающая экспертную оценку вероятности реализации риска и количественную оценку размеров

№п/п	Вид риска	Возможное применение методов оценки		
		Качественный	Количественный	Смешанный
			имущества вследствие действий лица, ответственного за хранение этого имущества.	последствий реализации риска.
7	Коммерческий риск	Может применяется качественный экспертный подход. Возможно использование всех методов оценки, приведенных в Разделе 2	Может применяться. Например, сценарный анализ, процедуры стресс-тестирования. Может производиться оценка снижения доходов.	Может применяться Матрица последствий и вероятности, сочетающая экспертную оценку вероятности реализации риска и количественную оценку размеров последствий реализации риска.

Примеры шкал оценки размера потенциального ущерба и вероятности реализации риска

Шкала оценки размера потенциального ущерба:

Размер ущерба	Финансовый ущерб	Иной ущерб
критический	Убыток, свыше ____ млн. руб.	Указывается размер ущерба: Например, широкое освещение проблемы в крайне негативной форме в национальных и международных СМИ
высокий	Убыток от ____ до ____ млн. руб.	Указывается размер ущерба: Например, широкое освещение проблемы в негативной форме в национальных СМИ.
средний	Убыток от ____ до ____ млн. руб.	Указывается размер ущерба: Например, широкое освещение проблемы в негативной форме в местных СМИ.
низкий	Убыток от ____ до ____ млн. руб.	Указывается размер ущерба: Например, серия негативных публикаций в местных СМИ.
незначительный	Убыток менее ____ млн. руб.	Указывается размер ущерба: Например, единичные негативные публикации в местных СМИ.

Шкала оценки вероятности реализации риска:

Оценка вероятности реализации	Значение, %	Интерпретация	
		для повторяющихся событий	для разовых событий
очень высокая вероятность	Больше 80%	Событие скорее всего произойдет в течение ближайшего времени	Шансы для наступления события велики
	60-80%	Событие скорее всего	Событие скорее

высокая вероятность		произойдет в течение месяца	произойдет, чем не произойдет
средняя вероятность	40-60%	Событие скорее всего произойдет в течение года	Шансы для наступления события оцениваются как «50 на 50»
низкая вероятность	20-40%	Событие скорее всего произойдет в течение следующих 3 лет	Событие скорее не произойдет, чем произойдет
очень низкая вероятность	Меньше 20%	Событие скорее всего произойдет в течение в долгосрочной перспективе	Шансы для наступления события малы

Пример оценки и признания кредитного риска значимым с использованием Матрицы рисков

Регламентом по управлению рисками организации предусмотрено, что риски признаются значимыми, если в результате их оценки вес риска в баллах составляет 15 и более баллов.

Установлены следующие веса в баллах по размеру ущерба и вероятности наступления для кредитного риска:

Размер ущерба	Вес в баллах	Финансовый ущерб
критический	5	Убыток, свыше 10 млн. руб.
высокий	4	Убыток от 7 до 10 млн. руб.
средний	3	Убыток от 5 до 7 млн. руб.
низкий	2	Убыток от 1 до 5 млн. руб.
незначительный	1	Убыток менее 1 млн. руб.

Оценка вероятности реализации риска	Вес в баллах	Значение, %
очень высокая вероятность	5	Больше 80%
высокая вероятность	4	60-80%
средняя вероятность	3	40-60%
низкая вероятность	2	20-40%
очень низкая вероятность	1	Меньше 20%

Итоговый балл определяется путем умножения соответствующих значений размера ущерба и вероятности реализации риска.

При установлении весов по размеру ущерба организация учитывает ожидаемые доходы и расходы на предстоящий календарный период, а также законодательные требования к размеру собственных средств.

В Таблице 2 приведена Матрица рисков организации.

Таблица 2

Матрица рисков

Размер потенциального ущерба	Критический 5	5	10	15	20	25
	Высокий 4	4	8	12	16	20
	Средний 3	3	6	9	12	15
	Низкий 2	2	4	6	8	10
	Незначительный 1	1	2	3	4	5
		очень низкая вероятность 1	низкая вероятность 2	средняя вероятность 3	высокая вероятность 4	очень высокая вероятность 5
	Вероятность					

В рамках экспертной оценки кредитного риска размер ущерба оценен как высокий (4 балла), а вероятность реализации риска как низкая (4 балла).

Итоговый вес для кредитного риска составляет 16 баллов.

Таким образом, данный вид риска организация относит к категории значимого риска.

Пример ключевых индикаторов рисков

Вид риска	Подвид риска	КИР	Пороговое значение
Риск персонала (служебный риск)	Дефицит ресурсов персонала	- открытые вакансии; - переработка сотрудниками	количество в % от рабочего дня
Риск персонала (служебный риск)	Умышленные действия работников организации	- конфликтные ситуации с администрацией организации	количество
Риск персонала (служебный риск)	Непреднамеренные ошибки работников организации	- факты совершения ошибочных действий персонала различного свойства	количество
Риск внешних лиц	Неисполнение (ненадлежащее исполнение) внешними лицами своих обязательств	- банкротство контрагента и связанные с этим финансовые потери	в % от общей выручки организации
Риск внешних лиц	Совершение внешними лицами умышленных (криминальных) действий с целью причинения ущерба организации, клиентам организации	- судебные разбирательства с контрагентом	количество
Риск внешних лиц	Техногенные чрезвычайные ситуации	- случаи приостановки деятельности ключевых подразделений организации более чем на 30 минут	количество
Коммуникационный риск	Изменение, искажение (порча, утрата) получаемой/передаваемой информации и документов	- конфликтная ситуация с администрацией организации у работника организации	количество

Коммуникационный риск	Недоступность проведения операций в Банк - клиенте	- ситуация, связанная с невозможностью осуществления операций в клиент-банке непрерывно на протяжении 3 часов	количество
Коммуникационный риск	Невозможность связаться с клиентом организации в процессе его обслуживания	- случаи невозможности установить связь с клиентом по каналам связи, известным организации, в течение 1 месяца	количество
Коммуникационный риск	Невозможность получить распоряжения /поручения клиентов	- случаи невозможности получения поручений клиента в течение 3 часов	количество
Технологический риск	Сбой технологического процесса	- случаи сбоев в бизнес-процессах	количество
Технологический риск	Не обеспечена непрерывность деятельности в чрезвычайных ситуациях	- случаи невозможности осуществления привычной деятельности Организации на протяжении более 1 часа	количество
Технологический риск	Сбои в работе оборудования (ПК, серверное оборудование, средства связи)	- случаи невозможности осуществления привычной деятельности Организации на протяжении более 1 часа	количество
Технологический риск	Несанкционированное распространение конфиденциальной информации, информации, составляющей коммерческую тайну, или персональных данных	- случаи несанкционированного распространения информации	количество
Технологический риск	Сбои в работе средств криптографической защиты информации	- случаи невозможности подписать документы, исходящие от организации, уполномоченным лицом в течение 1 часа и более	количество

Технологический риск	Сбои в работе систем ЭДО	- случаи невозможности осуществления обмена электронными документами в течение 1 часа и более	количество
Технологический риск	Нарушение целостности информации в базах данных	- случаи выявления факта наличия некорректной информации на уровне учетной системы или других информационных баз данных организации или на уровне внешних информационных ресурсов; - случаи выявления факта некорректного формирования отчетных форм, формируемых на основании данных, содержащихся в информационных базах организации	количество количество
Технологический риск	Кризис организации работы в подразделении	- случаи нарушений технологических процессов подразделения	количество
Технологический риск	Сбои в процедуре заключения договора	- случаи нарушений технологических процессов подразделения, осуществляющего подготовку и последующее подписание договора с клиентом или контрагентом	количество
Технологический риск	Сбои в процедуре приема поручений от клиента	- случаи невозможности получения поручений клиента в течение 1 часа и более	количество
Технологический риск	Сбой в процедуре выставления счетов за услуги организации	- случаи несвоевременного выставления счетов за услуги организации; - случаи нарушения графика поступлений вознаграждений организации за оказанные услуги	количество количество

Технологический риск	Сбой в процедуре проведения операций с бездокументарными ценными бумагами	- случаи неисполнения поручений клиентов в установленные сроки; - случаи перевода ценных бумаг в пользу лица, которое не было указано в поручении клиента	количество количество
Технический риск	Невозможность оперативного устранения последствий неисправности оборудования	- случаи невозможности осуществления привычных бизнес-процессов организации в течение 1 часа и более	количество
Технический риск	Неисполнение оборудованием возложенных на него функций из-за сбоев и нарушений в работе	- случаи невозможности осуществления привычных бизнес-процессов организации в течение 3 часов	количество
Технический риск	Отключение электроэнергии/ перепады напряжения	- случаи отсутствия подачи электроэнергии в течение 1 часа и более	количество
Регуляторный риск (комплаенс-риск)	Применение регулируемыми органами, а также уполномоченными государственными органами различного рода санкций к Организации	- случаи получения различного рода предписаний, содержащих требование об устранении нарушений законодательства	количество
Риск ОД/ФТ	Вовлечение Организации в отмывание доходов, полученных преступным путем	- случаи выявления в деятельности клиентов признаков отмывания доходов, полученных преступным путем или финансирования терроризма	количество
Организационный риск	Неэффективное распределение функциональных (должностных) обязанностей и полномочий между	- случаи выполнения функциональных задач, не закрепленных за работником в должностной инструкции или ином внутреннем	количество

	структурными подразделениями Организации	документе организации	
Кастодиальный риск	Возникновение различного рода убытков, связанных с учетом (хранением) ценных бумаг клиентов организации, самой организации	- случаи выявления факта нарушений, связанных с учетом ценных бумаг	количество
Кредитный риск	Неисполнение третьими лицами финансовых обязательств перед Организацией	- случаи выявления факта нарушения условий договоров	количество
Риск ликвидности	Невозможность реализовать финансовый актив	- случаи невозможности реализовать финансовый актив организации в течение 15 дней для ценных бумаг и в течение 1 месяца для иного вида активов	количество
Рыночный риск	Валютный риск	- обязательства организации в иностранной валюте, которые предстоит выполнить в случае резкого падения курса национальной валюты	% от общей суммы обязательств
Рыночный риск	Обесценение финансовых вложений	- резкое снижение стоимости активов	% от стоимости актива
Рыночный риск	Рост инфляции	- рост инфляции на фоне отсутствия изменений в тарифной политике организации	% инфляции
Стратегический риск	Отсутствие в полном объеме необходимых ресурсов и организационных мер, которые должны обеспечить достижение стратегических целей	- случаи отсутствия возможности обеспечения в срок необходимыми ресурсами, заявленными для конкретного проекта, бизнес-процесса и т.п.	количество

	деятельности Организации		
Стратегический риск	Изменение спроса на услуги	- сокращение договоров на обслуживание в рамках видов деятельности, осуществляемых организацией	% от общего количества договоров
Отраслевой риск	Изменение бизнес – ситуации в отрасли	- факт проведения конкурентами агрессивной политики по привлечению новых клиентов; - сокращение потенциальных клиентов, которые могут быть привлечены на обслуживание в организацию	количество % от общего количества потенциальных клиентов
Репутационный риск	Снижение доверия к Организации	- случаи участия организации в процессах, которые негативно отразились в отзывах о ней в прессе, Интернете или иных массовых источниках получения информации или распространения информации; - факты получения организацией официальных уведомлений о прекращении с ней договорных отношений	количество количество
Риск правового регулирования (правовой риск)	Несоблюдение организацией требований заключенных договоров	- случаи выявления факта несоблюдения условий договоров	количество
Риск правового регулирования (правовой риск)	Несовершенство правовой системы	- случаи выявления фактов противоречивости законодательства; - случаи выявления фактов отсутствия правовых норм регулирования отдельных	количество количество

		вопросов деятельности организации	
Коммерческий риск	Потеря доходности по основному виду деятельности Организации	- расторжение действующих договоров с клиентами	в % от доходной части бюджета организации
Коммерческий риск	Увеличение просроченной кредиторской задолженности	- случаи выявления фактов нарушения графика платежей по ожидаемым к поступлению сумм вознаграждения организации	количество
Коммерческий риск	Увеличение просроченной дебиторской задолженности	- случаи нарушения клиентами условий оплаты вознаграждения организации, установленные в договоре	количество
Коммерческий риск	Ошибки при проведении расчетно - кассовых операций	- случаи несанкционированного перечисления (выдачи наличными) денежных средств;	количество
		- случаи допущения ошибок в платежных (кассовых) документах	количество
Коммерческий риск	Использование некорректных или неполных исходных данных для осуществления расчетов по налогам	- случаи нарушения целостности данных в информационных базах данных организации;	количество
		- случаи возникновения технических сбоев в работе программного обеспечения, в том числе задействованного для формирования расчетных и отчетных данных	количество

Пример определения риск – аппетита организации в балльном эквиваленте

Для каждого вида риска организацией установлено ограничение (допустимый уровень) в балльном эквиваленте:

Вид риска	Допустимый уровень (в балльном эквиваленте)
Кредитный риск	4
Операционный риск	3
Рыночный риск	2
Правовой риск	3
Регуляторный риск	2
Риск ликвидности	3
Кастодиальный риск	4
Коммерческий риск	3

При этом риск – аппетит устанавливается в организации в виде набора баллов по видам рисков и составляет следующее значение **4 3 2 3 2 3 4 3**.

При оценке соответствия рисков установленным ограничениям рассматривается каждый конкретный вид риска. При превышении допустимого уровня риска хотя бы по одному виду риска можно говорить о нарушении установленного уровня риск - аппетита организации.

Пример проведения самооценки в организации

1. Порядок проведения Самооценки

Руководители структурных подразделений организации «Х» определяют ответственных сотрудников для заполнения Анкеты.

Должностное лицо, ответственное за организацию системы управления рисками, не позднее трех рабочих дней с даты окончания квартала направляет форму Анкеты в структурные подразделения.

Ответственный сотрудник на основе информации о деятельности структурного подразделения идентифицирует и оценивает операционные риски и контрольные процедуры структурного подразделения и заполняет Анкету. В случае необходимости Должностное лицо, ответственное за организацию системы управления рисками, оказывает консультационную поддержку ответственному сотруднику по вопросам заполнения Анкеты.

Руководитель структурного подразделения контролирует полноту и своевременность заполнения Анкеты ответственным сотрудником. Заполненная Анкета подписывается ответственным сотрудником и руководителем структурного подразделения.

Ответственный сотрудник направляет заполненную Анкету Должностному лицу, ответственному за организацию системы управления рисками, не позднее 20 рабочих дней с даты окончания квартала. Должностное лицо, ответственное за организацию системы управления рисками, осуществляет обработку и анализ Анкет, поступивших от структурных подразделений. Результаты проведенной самооценки доводятся до сведения высшего руководства.

2. Этапы проведения Самооценки

2.1. Идентификация операционных рисков

Процедура идентификации операционных рисков осуществляется в разрезе бизнес-процессов структурного подразделения. Для этого могут использоваться

- классификатор бизнес – процессов (при наличии);
- технологические карты бизнес - процессов (при наличии);
- регламент проведения операций (при наличии);
- дополнительные источники информации;
- положение о структурном подразделении;

- должностные инструкции.

В процессе идентификации операционных рисков также могут использоваться иные источники информации, включая акты проверок структурного подразделения контролером и паспорта рисков.

Для каждого из выделенного в структурном подразделении бизнес – процесса выявляются возможные операционные риски. В перечень включаются операционные риски, которые уже реализовывались, либо могут реализоваться с большой долей вероятности в результате особенностей бизнес - процесса и контрольных процедур.

По каждому бизнес - процессу выделяется как минимум один операционный риск.

Информация о выявленных в ходе проведения идентификации операционных рисках заносится в Анкету. В таблице 3 представлена часть Анкеты в отношении идентификации операционных рисков.

Таблица 3

Идентификация операционных рисков

№ риска	Описание бизнес - процесса	Описание операционного риска	Источник операционного риска
1	2	3	4
1	Контроль доступа к информационным ресурсам	Предоставление полного или несанкционированного доступа к БД «Операционные риски» лицам с ограниченным доступом	Персонал
2	Составление отчетности для клиентов	Ошибочный отчет для клиента	Бизнес -процесс Персонал
3	Прочие бизнес процессы ...	Прочие риски ...	

2.2. Анализ контрольных процедур³

После формирования перечня операционных рисков ответственный сотрудник структурного подразделения анализирует перечень действующих контрольных процедур в разрезе каждого

³ **Контрольная процедура** – это действия, установленные политиками и процедурами, которые помогают обеспечить исполнение указаний менеджмента по снижению рисков, препятствующих достижению целей

операционного риска. В перечень также включаются отсутствующие, но планируемые к внедрению контрольные процедуры.

По каждой контрольной процедуре указывается внутренний документ (при наличии), определяющий порядок выполнения этой процедуры. На основе экспертного мнения определяется достаточность контрольных процедур (контроль достаточный/недостаточный).

Если контрольные процедуры в отношении определенного вида риска отсутствуют или требуют улучшения (недостаточный контроль), ответственный сотрудник указывает возможные меры по его улучшению.

Далее указываются мероприятия, позволяющие осуществлять мониторинг выполнения заданных контрольных процедур.

Информация по контрольным процедурам заносится ответственным сотрудником структурного подразделения в Анкету. В Таблице 4 представлена часть Анкеты в отношении контрольных процедур.

Таблица 4

Анализ контрольных процедур

№ риска	Контрольные процедуры	Достаточность контроля/возможные меры по улучшению	Ссылка на внутренние документы, определяющие контрольные процедуры (при наличии)	Мониторинг контрольных процедур
1	5	6	7	8
1	Предоставление доступа производится на основании заявки по решению главного специалиста по информационной безопасности	Достаточный контроль	Инструкция по управлению доступом к информационным системам	Ежеквартальная проверка руководителем подразделения соблюдения инструкции по управлению доступом к системам информационной безопасности

2	Автоматизация отчетов для клиентов	Достаточный контроль	-	Ежеквартальная выборочная проверка выданных отчетов руководителем структурного подразделения
3	...			

2.3. Оценка операционного риска

По итогам формирования форм по операционным рискам и контрольным процедурам ответственный сотрудник структурного подразделения проводит ранжирование операционных рисков по уровню значимости.

Оценка значимости (ранжирование) операционных рисков структурного подразделения производится по следующей пятибалльной шкале:

1. Действие операционного риска, в случае его реализации, не прервет штатное исполнение бизнес - процесса; все необходимые контрольные процедуры и формы мониторинга частично, либо полностью реализованы; прямые потери – отсутствуют в любом случае;
2. действие операционного риска, в случае его реализации, приведет к незначительным изменениям в качестве исполнения бизнес - процесса; последствия легко исправимы силами структурного подразделения, необходимые контрольные процедуры требуют незначительных доработок; прямые потери полностью возмещаются;
3. действие операционного риска, в случае его реализации, приведет к незначительным изменениям в качестве исполнения бизнес - процесса; последствия исправимы, как правило, с привлечением стороннего структурного подразделения, частично отсутствуют необходимые контрольные процедуры и формы мониторинга, прямые потери полностью возмещаются или их величина незначительна;
4. действие операционного риска, в случае его реализации, приведет к значительным изменениям в качестве исполнения бизнес - процесса, возможна полная остановка исполнения бизнес - процесса; ликвидация последствий требует затрат времени, необходимые контрольные процедуры и формы мониторинга частично или практически отсутствуют; прямые потери невосполнимы или частично восполнимы;
5. действие операционного риска, в случае его реализации, приведет к значительным изменениям в качестве исполнения бизнес - процесса, возможна полная остановка исполнения процесса; ликвидация последствий, как правило, невозможна, необходимые контрольные процедуры и формы мониторинга отсутствуют, прямые потери невосполнимы или составляют значительные суммы.

Дополнительно к оценке значимости ответственный сотрудник оценивает операционные риски в разрезе вероятности наступления и последствий при реализации риска.

Результаты проведенной оценки вносятся в Анкету. В Таблице 5 приведена часть Анкеты в отношении оценки операционного риска.

Таблица 5

Оценка операционного риска

№ Риска	Описание операционного риска (ОР)	Уровень значимости	Вероятность наступления	Последствия
1	3	9	10	11
1	Предоставление полного или несанкционированного доступа к БД «Операционные риски» людям с ограниченным доступом	3	Можно отразить в баллах, в %	Можно отразить в баллах, в руб., в рабочих часах, в иной форме
2	Составление отчетности для клиентов	3	Можно отразить в баллах, в %	Можно отразить в баллах, в руб., в рабочих часах, в иной форме
3	...			

2.4. Разработка ключевых индикаторов риска

В отношении выявленных рисков ответственным сотрудником определяются ключевые индикаторы риска (КИР).

КИР устанавливается для тех рисков, где:

- установлен балльный коэффициент значимости операционных рисков от 3 до 5-ти;
- контрольные процедуры практически отсутствуют или не работают;
- наблюдается высокая частота проявления этого риска;

Также КИР могут устанавливаться по иным рискам.

Определенные КИР заносятся в Анкету. В таблице 6 форму приведена часть Анкеты в отношении КИР.

Таблица 6

Перечень ключевых индикаторов риска

№ риска	Описание ключевого индикатора риска	Предельное значение	Частота сбора отчетности (расчетов)
1	12	13	14
1	Количество несанкционированных или некорректных доступов к общему числу пользователей за квартал (%)	5%	Раз в квартал
2	Количество недостоверных событий к общему числу операционных событий за квартал (%)	1%	Раз в квартал
3	...		

2.5. Разработка планов мероприятий

Ответственный сотрудник совместно с руководителем структурного подразделения анализируют заполненные поля Анкеты по операционным рискам, контрольным процедурам и мониторингу и определяют мероприятия по устранению выявленных пробелов. Часть Анкеты в отношении планируемых мероприятий приведена в таблице 7.

Таблица 7

План мероприятий

№ риска	Мероприятия	Ответственный исполнитель	Срок исполнения
1	15	16	17
1	Обучение сотрудников	Должность/ФИО	1 квартал
2	Разработка инструкций по актуализации и проверки отчетов для клиентов	Должность/ФИО	1 квартал
3	...		

На основе предоставленных от структурных подразделений организации Анкет Риск – менеджер формирует сводный документ по результатам проведенной самооценки «Отчет по самооценке» (Таблица 8).

Отчет по самооценке

№ риска	Идентификация операционных рисков			Перечень контрольных процедур				Оценка операционного риска			Перечень ключевых индикаторов риска			План мероприятий			Примечание
	Описание бизнес - процесса	Описание операционного риска	Источник операционного риска	Контрольные процедуры	Достаточность контроля/ возможные меры по улучшению	Ссылка на внутренние документы	Мониторинг контрольных процедур	Уровень значимости	Вероятность наступления	Последствия	Описание КИР	Предельное значение	Частота сбора отчетности (расчетов)	Описание мероприятия	Ответственный исполнитель	Срок исполнения	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Пример оценки соответствия системы управления рисками принципам и компонентам COSO ERM

Определяются принципы внутри каждого компонента управления рисками.

Таблица 9

№ п/п	№ внутри компонента	Принцип
Компонент «Внутренняя среда»		
1	1	Организация демонстрирует приверженность принципу порядочности и этическим ценностям
2	2	Совет директоров демонстрирует независимость от исполнительного руководства и осуществляет надзор за развитием и функционированием внутреннего контроля
3	3	Исполнительное руководство, под надзором совета директоров, определяет структуру организации, линии подчиненности, а также соответствующие полномочия, обязанности и ответственность в процессе достижения целей
4	4	Организация демонстрирует стремление к привлечению, развитию и удержанию компетентных сотрудников в соответствии с поставленными целями
5	5	Организация устанавливает ответственность сотрудников за выполнение ими своих обязанностей в сфере внутреннего контроля, управления рисками в процессе достижения целей
6	6	Система внутреннего контроля и управления рисками должна соответствовать масштабам деятельности организации и ее стратегии
7	7	Высшее руководство определяет философию в отношении риска и риск-аппетита организации
Компонент «Постановка целей»		
8	1	Организация определяет четкие цели для того, чтобы иметь возможность идентифицировать и оценить риски, препятствующие их достижению
9	2	Цели организации определяются до того, как высшее руководство выявит события, потенциально влияющие на достижение целей
10	3	При постановке целей должна соблюдаться иерархия целей: общие цели ставятся на стратегическом уровне, на их основе разрабатываются

		тактические цели, а также подцели.
11	4	Процесс управления рисками обеспечивает «разумную» гарантию того, что высшее руководство имеет правильно организовало процесс выбора и формулировки целей, и что цели устанавливаются таким образом, чтобы соответствовать миссии организации и учитывать уровень ее риск-аппетита
Компонент «Определение событий»		
12	1	Организация определяет внутренние и внешние события, оказывающие влияние на достижение ее целей
13	2	Исходя из перечня событий, сформулированного на основе анализа внешних и внутренних факторов, воздействующих на цели организации, организация <u>оценивает влияние</u> данных событий: положительное (возможности), отрицательное (риски) либо смешанное
14	3	Для отрицательных событий (рисков) определяются показатели, влияющие на возникновение данных рисков, - ключевые индикаторы рисков
15	4	Высшее руководство учитывает существующие возможности в процессе формирования стратегии и постановки целей
Компонент «Оценка рисков»		
16	1	Организация идентифицирует риски, препятствующие достижению полного спектра своих целей, и осуществляет анализ рисков для определения подходов к управлению ими
17	2	Организация учитывает возможность мошенничества при оценке рисков, препятствующих достижению поставленных целей
18	3	Организация определяет и оценивает изменения, которые могут оказать значительное воздействие на систему внутреннего контроля
19	4	Организация оценивает риски с учетом вероятности их возникновения и влияния
20	5	Организация проводит сравнительную оценку риска – соотнесение уровня риска с его допустимым (целевым) уровнем
Компонент «Реагирование на риски»		
21	1	Организация определяет и оценивает возможные виды реагирования на риски, включая возможность уклонения от риска, принятия его, сокращения или перераспределения риска.
22	2	Выбранные методы реагирования должны привести выявленный риск в соответствие с допустимым уровнем данного риска и с уровнем риск-

		аппетита организации.
23	3	При выборе способа реагирования организация должна оценить затраты и выгоды от использования данного метода
Компонент «Средства контроля»		
24	1	Организация выбирает и разрабатывает контрольные процедуры, которые позволяют снизить до приемлемого уровня риски, препятствующие достижению целей
25	2	Организация выбирает и разрабатывает общие процедуры контроля над технологиями для достижения поставленных целей
26	3	Организация реализует контрольные процедуры посредством политик, которые определяют ожидаемые результаты, и процедур, посредством которых политики претворяются в жизнь
Компонент «Информация и коммуникации»		
27	1	Организация получает или формирует и использует значимую и качественную информацию для поддержания функционирования внутреннего контроля и управления рисками
28	2	В организации осуществляется внутренний обмен информацией, включая информацию о целях и обязанностях в области внутреннего контроля и управления рисками, которая необходима для их функционирования
29	3	Организация осуществляет обмен информацией с внешними сторонами по вопросам, оказывающим влияние на функционирование внутреннего контроля и управления рисками
Компонент «Мониторинг»		
30	1	Организация выбирает, готовит и проводит непрерывные и/или периодические оценки компонентов внутреннего контроля и управления рисками с целью удостовериться, что они есть в наличии и работают
31	2	Организация оценивает недостатки внутреннего контроля и управления рисками и своевременно информирует о них стороны, ответственные за осуществление корректирующих действий, включая исполнительное руководство и совет директоров
32	3	Мониторинг системы управления рисками осуществляется путем контроля за величинами ключевых индикаторов риска и их соответствием допустимым (целевым) уровням КИР

Установлены следующие **значения коэффициента реализации принципа**:

0 – отсутствие реализации принципа (принцип не определен – не описан во внутренних документах)

0,5 – недостаточная реализация принципа (принцип определен, но не функционирует должным образом)

1,0 – принцип реализуется должным образом (принцип определен и функционирует)

Уровень реализации принципа (столбец 4 Таблицы 10) рассчитывается как **произведение уровня значимости принципа** (столбец 3 Таблицы 10) и **коэффициента реализации принципа** (экспертная оценка по определенной выше шкале).

Покомпонентная сумма показателей реализации принципов позволяет оценить эффективность системы управления рисками организации по шкале, установленной организацией.

0,8-1,0/80-100% - система управления рисками организации высоко эффективна;

0,6-0,8/60-80% - система управления рисками организации достаточно эффективна;

0,4-0,6/40-60% - система управления рисками организации недостаточно эффективна;

менее **0,4/40%** - система управление рисками организации неэффективна.

Таблица 10

№	Принцип	Уровень значимости принципа	Уровень реализации принципа	Обоснование (наличие/отсутствие существенных недостатков внутреннего контроля*)	Рекомендации аудитора
1	2	3	4	5	6
Компонент «Внутренняя среда»					
1	Организация демонстрирует приверженность принципу порядочности и этическим ценностям	0,02	$0,02 \cdot 1,0 = 0,02$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют

2	Совет директоров демонстрирует независимость от исполнительного руководства и осуществляет надзор за развитием и функционированием внутреннего контроля	0,02	$0,02 \cdot 0,5 = 0,01$	Недостаточная реализация принципа. Принцип описан во внутреннем документе организации, но не внедрен на практике	Для повышения эффективности внутреннего контроля организации совету директоров необходимо осуществлять надзор за его развитием и функционированием в соответствии с «Положением о Совете директоров».
3	Исполнительное руководство, под надзором совета директоров, определяет структуру организации, линии подчиненности, а также соответствующие полномочия, обязанности и ответственность в процессе достижения целей	0,02	$0,02 \cdot 1,0 = 0,02$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
4	Организация демонстрирует стремление к привлечению, развитию и удержанию компетентных сотрудников в соответствии с поставленными целями	0,02	$0,02 \cdot 1,0 = 0,02$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
5	Организация устанавливает ответственность сотрудников за выполнение ими своих обязанностей в сфере внутреннего контроля, управления рисками в процессе достижения целей	0,02	$0,02 \cdot 0 = 0,00$	Отсутствие реализации принципа. Принцип не определен во внутренних документах организации и не реализуется	Внутренними документами организации необходимо установить ответственность сотрудников за выполнение ими своих должностных обязанностей в сфере внутреннего контроля и

					управления рисками в процессе достижения целей.
6	Система внутреннего контроля и управления рисками соответствует масштабам деятельности организации и ее стратегии	0,02	$0,02 \cdot 1,0 = 0,02$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
7	Высшее руководство определяет философию в отношении риска и риск – аппетита организации	0,02	$0,02 \cdot 1,0 = 0,02$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
	ИТОГО	$K_{uz1} = 0,14$ /14%	0,11 /11%		
Компонент «Постановка целей»					
8	Организация определяет четкие цели для того, чтобы иметь возможность идентифицировать и оценить риски, препятствующие их достижению	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
9	Цели организации определяются до того, как высшее руководство выявит события, потенциально влияющие на достижение целей	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
10	При постановке целей должна соблюдаться	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом.	Отсутствуют

	иерархия целей: общие цели ставятся на стратегическом уровне, на их основе разрабатываются тактические цели, а также подцели.			Принцип определен во внутренних документах организации и функционирует	
11	Процесс управления рисками обеспечивает «разумную» гарантию того, что высшее руководство имеет правильно организовало процесс выбора и формулировки целей, и что цели устанавливаются таким образом, чтобы соответствовать миссии организации и учитывать уровень ее риск-аппетита	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
	ИТОГО	$K_{y31} = 0,12$ /12%	0,12 /12%		
Компонент «Определение событий»					
12	Организация определяет внутренние и внешние события, оказывающие влияние на достижение ее целей	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют

13	Исходя из перечня событий, сформулированного на основе анализа внешних и внутренних факторов, воздействующих на цели организации, организация <u>оценивает влияние</u> данных событий: положительное (возможности), отрицательное (риски) либо смешанное	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
14	Для отрицательных событий (рисков) определяются показатели, влияющие на возникновение данных рисков, - ключевые индикаторы рисков	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
15	Высшее руководство учитывает существующие возможности в процессе формирования стратегии и постановки целей	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
	ИТОГО	$K_{\text{уз1}} = 0,12$ /12%	0,12 /12%		
Компонент «Оценка рисков»					
16	Организация идентифицирует риски, препятствующие достижению полного спектра своих целей, и осуществляет анализ рисков для определения	0,03	$0,03 \cdot 1,0 = 0,03$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют

	подходов к управлению ими				
17	Организация учитывает возможность мошенничества при оценке рисков, препятствующих достижению поставленных целей	0,02	$0,02 \cdot 1,0 = 0,02$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
18	Организация определяет и оценивает изменения, которые могут оказать значительное воздействие на систему внутреннего контроля	0,03	$0,03 \cdot 0 = 0,00$	Отсутствие реализации принципа. Принцип не определен во внутренних документах организации и не реализуется	Внутренними документами организации необходимо установить, что организация определяет и оценивает изменения, которые могут оказать значительное воздействие на систему внутреннего контроля, а именно: - оцениваются изменения во внешней среде (регулятивной, экономической); - оцениваются изменения в бизнес – модели (новые направления деятельности, быстрый рост организации, новые технологии и т.д.); - оцениваются изменения в руководстве (состав, философия и т.д.).

19	Организация оценивает риски с учетом вероятности их возникновения и влияния	0,02	$0,02 \cdot 1,0 = 0,02$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
20	Организация проводит сравнительную оценку риска – соотношение уровня риска с его допустимым (целевым) уровнем	0,02	$0,02 \cdot 0,5 = 0,01$	Недостаточная реализация принципа. Принцип описан во внутреннем документе организации, но не внедрен на практике	Для повышения эффективности управления рисками необходимо внедрить на практике соотношение уровня риска с его допустимым (целевым значением).
	ИТОГО	$K_{y32} = 0,12$ /12%	0,08 /8%		
Компонент «Реагирование на риски»					
21	Организация определяет и оценивает возможные виды реагирования на риски, включая возможность уклонения от риска, принятия его, сокращения или перераспределения риска.	0,04	$0,04 \cdot 1,0 = 0,04$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
22	Выбранные методы реагирования приводят выявленный риск в соответствие с допустимым уровнем данного риска и с уровнем риск-аппетита организации.	0,05	$0,05 \cdot 1,0 = 0,05$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют

23	При выборе способа реагирования организация оценивает затраты и выгоды от использования данного метода	0,05	$0,05 \cdot 1,0 = 0,05$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
	ИТОГО	$K_{y1} = 0,14$ /14%	0,14 /14%		
Компонент «Средства контроля»					
24	Организация выбирает и разрабатывает контрольные процедуры, которые позволяют снизить до приемлемого уровня риски, препятствующие достижению целей	0,04	$0,04 \cdot 1,0 = 0,04$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
25	Организация выбирает и разрабатывает общие процедуры контроля над технологиями для достижения поставленных целей	0,04	$0,04 \cdot 1,0 = 0,04$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
26	Организация реализует контрольные процедуры посредством политик, которые определяют ожидаемые результаты, и процедур, посредством которых политики претворяются в жизнь	0,04	$0,04 \cdot 0,5 = 0,02$	Недостаточная реализация принципа. Принцип описан во внутреннем документе организации, но не полностью внедрен на практике	Необходимо на практике периодически анализировать контрольные процедуры на предмет сохранения актуальности и обновлять их по мере необходимости.
	ИТОГО	$K_{y3} = 0,12$ /12%	0,10 /10%		
Компонент «Информация и коммуникации»					

27	Организация получает или формирует и использует значимую и качественную информацию для поддержания функционирования внутреннего контроля и управления рисками	0,04	$0,04 * 1,0 = 0,04$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
28	В организации осуществляется внутренний обмен информацией, включая информацию о целях и обязанностях в области внутреннего контроля и управления рисками, которая необходима для его функционирования	0,04	$0,04 * 0,5 = 0,02$	Недостаточная реализация принципа. Принцип описан во внутреннем документе организации, но не полностью внедрен на практике	Способ осуществления коммуникаций не всегда учитывает такие факторы, как своевременность и характер информации. Отсутствуют отдельные каналы передачи информации, такие как «горячие линии» для сообщения о нарушениях, которые служат надежными механизмами для передачи анонимных или конфиденциальных сообщений в тех случаях, когда обычные каналы не функционируют или неэффективны.
29	Организация осуществляет обмен информацией с внешними сторонами по вопросам, оказывающим влияние на функционирование внутреннего контроля и управления рисками	0,04	$0,04 * 1,0 = 0,04$	Принцип реализуется должным образом. Принцип определен во внутренних документах организации и функционирует	Отсутствуют
ИТОГО		$K_{y34} = 0,12$	0,10 / 10%		

		/12%			
Компонент «Мониторинг»					
30	Организация выбирает, готовит и проводит непрерывные и/или периодические оценки компонентов внутреннего контроля и управления рисками с целью удостовериться, что они есть в наличии и работают	0,4	0,4*0=0,00	Отсутствие реализации принципа. Принцип определен в документах организации и не реализуется	Во внутренних документах организации необходимо определить проведение непрерывных и/или периодических оценок компонентов внутреннего контроля и управления рисками с целью удостовериться, что они есть в наличии и работают. При этом необходимо учитывать быстроту изменения бизнеса и бизнес – процессов, обеспечить интеграцию оценок с бизнес – процессами, корректировать объем и частоту оценок в зависимости от рисков и др.
31	Организация оценивает недостатки внутреннего контроля и управления рисками и своевременно информирует о них стороны, ответственные за осуществление корректирующих действий, включая высшее исполнительное руководство и совет директоров	0,4	0,4*0=0,00	Отсутствие реализации принципа. Принцип определен в документах организации и не реализуется	Во внутренних документах организации необходимо определить, что организация оценивает недостатки внутреннего контроля и управления рисками и своевременно информирует о них стороны, ответственные за осуществление корректирующих действий, включая

					исполнительное руководство и совет директоров, а именно: - исполнительное руководство и совет директоров анализируют результаты непрерывных и периодических оценок; - информация о недостатках предоставляется в установленном порядке сторонам, ответственным за осуществление корректирующих действий, исполнительном у руководству и совету директоров; - исполнительное руководство контролирует своевременность устранения недостатков.
32	Мониторинг системы управления рисками осуществляется путем контроля за величинами ключевых индикаторов риска и их соответствием допустимым (целевым) уровням КИР	0,4	$0,4 \cdot 0,5 = 0,02$	Недостаточная реализация принципа. Принцип описан во внутреннем документе организации, но не внедрен на практике	Необходимо внедрить в практике деятельности организации контроль за величинами ключевых индикаторов риска и их соответствием допустимым (целевым) уровням КИР.
	ИТОГО	$K_{v35} = 0,12 / 12\%$	0,02 / 2%		
	ВСЕГО	1,0 / 100%	0,79 / 79%		

Покомпонентная сумма показателей реализации принципов составляет 0,79 (или 79%).

Система управления рисками организации **достаточно эффективна**.

Пример состава отчетности и иных внутренних документов организации в рамках системы управления рисками

В организации может быть определен следующий состав отчетности в рамках системы управления рисками:

- Отчет о результатах самооценки;
- План мероприятий по снижению рисков (Таблица 11);
- Отчет о выполнении плана мероприятий по снижению рисков (Таблица 12);
- Отчет Должностного лица, ответственного за организацию системы управления рисками, о проделанной работе по организации системы управления рисками (далее – Отчет Должностного лица) (Таблица 13).

Также могут быть определены иные внутренние документы организации в рамках системы управления рисками:

- Паспорт риска (Таблица 14);
- Матрица рисков (Таблица 15);
- иные.

Представление отчетов по системе управления рисками, за исключением Отчета о результатах анкетирования, осуществляется ежеквартально.

В течение 15 рабочих дней после завершения квартала Должностным лицом, ответственным за организацию системы управления рисками, может формироваться Матрица рисков, План мероприятий по снижению рисков, Отчет о проделанной работе, и/или иные документы, формируемые в организации в рамках системы управления рисками по итогам отчетного периода. Указанные документы с определенной в организации периодичностью представляются на ознакомление руководителю организации в целях принятия соответствующих управленческих решений.

Отчет Должностного лица формируется ежеквартально в течение 15 рабочих дней после завершения квартала. В Отчете Должностного лица указывается информация о выявленных рисковых событиях, а также может быть указана информация о количестве составленных за квартал Паспортов риска, результаты анализа составленной по итогам квартала Матрицы рисков, результаты анализа установленных предельных размеров рисков и совокупного предельного размера рисков. В Отчете Должностного лица по итогам года также указываются результаты оценки эффективности системы управления рисками. Руководитель организации по итогам

рассмотрения Отчета Должностного лица принимает решение по вопросам развития (совершенствования) системы управления рисками.

Таблица 11

**План мероприятий по снижению рисков
за ____ квартал ____ года**

№ п/п	Вид риска	Наименование мероприятия	Срок исполнения и/или периодичность проведения	Ответственное лицо и/или подразделение, ответственное за выполнение мероприятия
1	2	3	4	5

Таблица 12

**Отчет о выполнении плана мероприятий по снижению рисков
за ____ квартал ____ года**

№ п/п	Вид риска	Наименование мероприятия	Ответственное лицо и/или подразделение, ответственное за выполнение мероприятия	Планируемый срок выполнения мероприятия (периодичность проведения)	Фактический срок выполнения мероприятия (периодичность проведения)	Документы, подтверждающие факт выполнения мероприятия (при наличии)	Причины невыполнения (нарушения сроков выполнения) мероприятия (в случае невыполнения, нарушения сроков выполнения мероприятия)
1	2	3	4	5	6	7	8

Таблица 13

**Отчет Должностного лица, ответственного за организацию системы управления
рисками, о проделанной работе по организации системы управления рисками
за ____ квартал ____ года**

В ходе мониторинга рисков _____ в _____ квартале
наименование организации

_____ года _____

_____ (количество выявленных рисков, количество заполненных Паспортов рисков, последствия реализации рисков, выводы)

По итогам _____ квартала _____ года составлена Матрица рисков деятельности. По результатам анализа Матрицы рисков выявлена зона максимального риска в деятельности –

(вид риска)

План мероприятий по снижению рисков деятельности _____

(утвержден / не утвержден / сроки утверждения)

По итогам _____ квартала _____ года предельные размеры рисков (допустимый уровень рисков), совокупный предельный размер рисков _____

_____ (превышены / не превышены, результаты анализа установленных на квартал предельных размеров рисков, совокупного предельного размера рисков)

В течение _____ года система управления рисками

(результаты оценки эффективности СУР)

Должностное лицо, ответственное за организацию системы управления рисками _____ (ФИО)

«___» _____ 2018 г.

Паспорт риска

«__» «_____» 20__ г.

Вид риска Описание события, имеющего признаки реализации риска	Источник риска	Причина реализации риска	Владелец риска и/или лицо, поставляющее информацию о риске	Дата наступления события	Дата выявления события	Последствия риска (в т.ч. размер фактического или возможного убытка)	Коэффициент значимости (критерий существенности последствий), Кз	Процедуры реагирования
1	2	3	4	5	6	7	8	9

Руководитель структурного подразделения _____/

Ф.И.О./

Таблица 15

Матрица рисков за __ квартал 20__ года

«__» «_____» 20__ г.

№ вида риска	Вид риска / количество выявленных событий по видам рисков	Кз	Отсутствует	Однократное выявление	Выявлено более одного события
	Кв		0,1	1	2
1	Кредитный риск	2	Ур	Ур	Ур
2	Операционный риск	3	Ур	Ур	Ур
3	Рыночный	2	Ур	Ур	Ур
4	Правовой риск	2	Ур	Ур	Ур
5	Регуляторный риск	2	Ур	Ур	Ур
6	Риск ликвидности	2	Ур	Ур	Ур
7	Кастодиальный риск	2	Ур	Ур	Ур
8	Коммерческий риск	2	Ур	Ур	Ур

При этом для определения коэффициента значимости Кз используется следующая шкала:

Значимость риска	Существенность последствий риска	Коэффициент значимости (Кз)
Низкая	Реализация риска не приводит к негативным последствиям, расходам (убыткам) и не влияет на бизнес-процессы, имеются легко и быстро устранимые замечания, достаточно планового контроля	1
Умеренная	Реализация риска приводит к частичной неработоспособности бизнес-процесса, но не влияет на основные функции, требуется разработка мероприятий по управлению риском	2
Высокая	Реализация риска приводит к неработоспособности бизнес-процесса и потере основных функций, необходимо принимать срочные меры	3

Для определения коэффициента вероятности (Кв) используется следующая шкала:

Вероятность возникновения риска	Коэффициент вероятности (Кв)
Низкая вероятность (событие в квартале не происходит)	0,1
Средняя вероятность (событие происходит до 1 раза в квартал)	1
Высокая вероятность (событие происходит чаще 1 раза в квартал)	2

Определение уровня (критичности) риска (Ур):

Уровень (критичность) риска $Ур = Кз \times Кв$	Необходимость в мероприятиях по управлению риском
$3 < Ур$	Срочно необходимо разработать корректирующие мероприятия, направленные на снижение уровня риска в кратчайшие сроки
$1 \leq Ур \leq 3$	Необходимо разработать корректирующие мероприятия, направленные на снижение уровня риска
$Ур < 1$	Удовлетворяют существующие защитные мероприятия

Пример Реестра рисков

Риски персонала, служебные риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Текущая укомплектованность персонала не соответствует потребностям Организации	риск нехватки квалифицированных сотрудников	нехватка финансирования, отсутствие необходимых кадров на рынке труда, некорректное планирование потребности организации в квалифицированных специалистах	Дирекция	
	Нехватка персонала нужной квалификации на рынке труда	на рынке труда не хватает специалистов необходимой для организации квалификации либо нужные специалисты не готовы работать на условиях, предоставляемых организацией	высокий уровень требований при приеме на работу, низкий уровень заработной платы	Дирекция	
	Уровень компетентности персонала Организации не соответствует потребностям Организации	квалификация работников, принятых на работу, не соответствует потребностям организации	отсутствие необходимого выбора компетентных претендентов на позицию, изменение требований к специалистам	Дирекция	
	Низкий уровень мотивированности персонала	мотивация персонала не поддерживается на уровне, достаточном для эффективной деятельности организации	отсутствие понимания стратегии организации и роли каждого сотрудника в ее реализации, отсутствие четко сформулированных целей и задач на уровне подразделений организации, отсутствие системы вознаграждения сотрудников	Дирекция	

	Внутренние программы обучения не соответствуют текущим нуждам организации	существующие программы обучения сотрудников (ПОД/ФТ, СУР, внутренний контроль и др.) не учитывают потребности организации, существующие требования законодательства	Отсутствие планирования обучения, несвоевременное изменение программ обучения и подготовка методических материалов	Дирекция, Отдел по ПОД/ФТ, Управление информационных технологий, Управление спецдепозитарных операций, Депозитарий	
	Чрезмерная зависимость от ключевых сотрудников	чрезмерная зависимость от ключевых сотрудников	некоторые бизнес - процессы замкнуты на ключевых сотрудниках, процесс делегирования полномочий не развит,	Дирекция, Отдел по ПОД/ФТ, Управление информационных технологий, Управление спецдепозитарных операций, Депозитарий	
	Увольнение сотрудников	риск увольнения высококвалифицированного персонала	низкий уровень компенсации труда и размера социального пакета по сравнению с другими аналогичными организациями на рынке, высокий уровень ответственности и требований к сотрудникам	Дирекция	
	Умышленные действия сотрудников Организации	Риск совершения умышленных действий, включая совершение действий с использованием поддельных ценных бумаг и/или документов, в том числе несанкционированный доступ к компьютерным сетям с целью уничтожения, изменения (искажения) электронных данных, направленных на получение личной выгоды и/или причинение ущерба организации, клиентам	недостаточная квалификация, служебная халатность, мошеннические действия	Дирекция, Отдел по ПОД/ФТ, Управление информационных технологий, Управление спецдепозитарных операций, Депозитарий	
	Неисполнение/ ненадлежащее исполнение сотрудниками своих должностных обязанностей	Риск неисполнения/ ненадлежащего исполнения сотрудниками своих должностных обязанностей	недостаточная квалификация, халатность, мошеннические действия	Дирекция, Отдел по ПОД/ФТ, Управление информационных технологий, Управление спецдепозитарных операций,	

				Депозитарий	
	Совершение сотрудниками действий, не входящих в область их компетенции	Риск совершения сотрудниками действий, которые не входят в область их компетенции в соответствии с внутренними документами организации	недостаточная квалификация, халатность, мошеннические действия, незнание внутренних документов организации	Дирекция, Отдел по ПОД/ФТ, Управление информационных технологий, Управление спецдепозитарных операций, Депозитарий	

Риски внешних лиц					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Неисполнение (ненадлежащее исполнение) внешними лицами своих обязательств	Неисполнение (ненадлежащее исполнение) внешними лицами своих обязательств	нарушение обязательств контрагентами, мошеннические действия	Бухгалтерия	
	Совершение внешними лицами непреднамеренных ошибок (ошибочных действий) при исполнении своих обязательств	Совершение внешними лицами непреднамеренных ошибок (ошибочных действий) при исполнении своих обязательств	низкая компетентность сотрудников иных организаций при взаимодействии с организацией	Бухгалтерия, Депозитарий, Управление спецдепозитарных операций	
	Совершение внешними лицами умышленных (криминальных) действий с целью причинения ущерба организации, клиентам	Совершение внешними лицами умышленных (криминальных) действий с целью причинения ущерба организации, клиентам, включая совершения действий с использованием поддельных ценных бумаг и/или документов, а также несанкционированный доступ к компьютерным сетям с целью уничтожения, изменения (искажения) электронных данных	умышленные, мошеннические действия	Бухгалтерия, Депозитарий, Управление спецдепозитарных операций	

Риски воздействия внешних событий					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Хищения	Риск хищения имущества, принадлежащего организации третьими лицами или сотрудниками организации	Отсутствие необходимого уровня охраны в организации, мошенничество со стороны сотрудников	Дирекция	
	Затопление	Риск залива жидкостью имущества и документов организации	Аварии водопроводов	Дирекция	
	Пожары	Риск пожаров в организации	Несоблюдение мер противопожарной безопасности, халатность персонала	Дирекция, Подразделения организации	

Коммуникационные риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Изменение, искажение получаемой/передаваемой информации и документов	Изменение, искажение получаемой/передаваемой информации и документов	Неисправность телефонной сети, ЭДО, электронной почты и прочих средств связи, мошеннические действия, нарушение целостности технических коммуникаций и оборудования, обеспечивающих связь. Сбой в	Управление информационных технологий	

			деятельности оператора связи		
	Утрата, порча получаемой/ передаваемой информации и документов	Утрата, порча получаемой/ передаваемой информации и документов	Неисправность телефонной сети, ЭДО, электронной почты и прочих средств связи, мошеннические действия, нарушение целостности технических коммуникаций и оборудования, обеспечивающих связь. Сбой в деятельности оператора связи	Управление информационных технологий	
	Невозможность уведомить клиента об отсутствии распоряжения/ поручения	Невозможность уведомить клиента об отсутствии распоряжения/ поручения	Неисправность телефонной сети, ЭДО, электронной почты и прочих средств связи, нарушение целостности технических коммуникаций и оборудования, обеспечивающих связь. Сбой в деятельности оператора связи	Управление информационных технологий	
	Невозможность войти в Банк - клиент для акцепта платежа	Невозможность войти в Банк - клиент для акцепта платежа	Неисправность телефонной сети, ЭДО, электронной почты и прочих средств связи, нарушение целостности технических коммуникаций и оборудования, обеспечивающих связь. Сбой в деятельности оператора связи	Управление информационных технологий	

	Невозможность в срок уведомить клиента о возникших сложностях при исполнении поручения/ распоряжения	Невозможность в срок уведомить клиента о возникших сложностях при исполнении поручения/ распоряжения	Неисправность телефонной сети, ЭДО, электронной почты и прочих средств связи, нарушение целостности технических коммуникаций и оборудования, обеспечивающих связь. Сбой в деятельности оператора связи	Управление информационных технологий	
	Невозможность в срок предоставить отчеты клиентам по исполненным поручениям/ распоряжениям	Невозможность в срок предоставить отчеты клиентам по исполненным поручениям/ распоряжениям	Неисправность телефонной сети, ЭДО, электронной почты и прочих средств связи, нарушение целостности технических коммуникаций и оборудования, обеспечивающих связь. Сбой в деятельности оператора связи	Управление информационных технологий	
	Невозможность получить распоряжения /поручения клиентов	Невозможность получить распоряжения /поручения клиентов	Неисправность телефонной сети, ЭДО, электронной почты и прочих средств связи, нарушение целостности технических коммуникаций и оборудования, обеспечивающих связь. Сбой в деятельности оператора связи	Управление информационных технологий	

Технологические риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Сбой технологического процесса	риск нарушения установленного порядка функционирования структурных подразделений, порядка действий сотрудников, порядка взаимодействия между структурными подразделениями; нарушение установленного порядка применения оборудования и технических средств, установленного порядка обеспечения информационной безопасности	Некомпетентность сотрудников, халатность в части соблюдения внутренних документов организации, устанавливающих порядок функционирования бизнес - процессов	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	
	Текущая структура информационных потоков не позволяет своевременно принимать управленческие решения	Текущая структура информационных потоков не достаточна для принятия взвешенных и своевременных управленческих решений	Доступ пользователей к информации не обеспечивает потребности организации в части регулярности, актуальности и полноты информации	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	
	Внедренные технологические решения не в состоянии обеспечить потребности организации/изменения законодательства	Внедренные технологические решения не в состоянии обеспечить текущие либо перспективные потребности организации	невозможность/ несвоевременность адаптации существующих технологий к изменения законодательства, требованиям к организации работы в организации, внутренним регламентам и процедурам	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	

	Несовместимость внедряемых технологий с существующими системами	При взаимодействии внедряемых технологий с существующими системами могут возникать конфликты или новая система не может функционировать на базе существующего оборудования	принятие решений о внедрении новой технологии без анализа специфики существующих технологий, отсутствие информации о конфликтах между существующими и внедряемыми технологиями	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	
	Внедрение технологических решений не в срок	При внедрении технологических решений могут быть задержки, не позволяющие осуществлять текущую деятельность эффективным образом или в соответствии с действующими требованиями	задержки в работе организаций, внедряющих технологические решения	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	
	Недостаточная адаптация ИТ решений к изменениям требований действующего законодательства	Риск того, что при изменении требований законодательства настройки автоматизированной системы учета не будут своевременно адаптированы, что может привести к несоответствиям в деятельности и штрафам	отсутствие информации об изменениях требований действующего законодательства, несвоевременная/не полная адаптация к изменениям	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	
	Не обеспечена непрерывность деятельности	В организации отсутствуют эффективные механизмы взаимодействия в режиме чрезвычайной ситуации и обеспечения восстановления нормального функционирования	отсутствие плана действий организации в чрезвычайной ситуации, отсутствие плана восстановления ИТ функций после чрезвычайной ситуации	Дирекция	
	Сбои в работе программного обеспечения	Сбои в работе программного обеспечения. Например, сбои ИТ систем, поддерживающих формирование отчетности организации	сбои в энергообеспечении, преднамеренные действия персонала и третьих лиц, вирусов, вредоносных программ, сбои в системном программном обеспечении	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	

	Сбои в работе оборудования (ПК, серверное оборудование, средства связи)	Сбои в работе оборудования (ПК, серверное оборудование, средства связи)	сбои в энергообеспечении, чрезмерные нагрузки, преднамеренные действия персонала и третьих лиц, износ оборудования	Управление информационных технологий	
	Утечка/потеря конфиденциальной информации, информации, составляющей коммерческую тайну, или персональных данных	Утечка/потеря конфиденциальной информации, информации, составляющей коммерческую тайну, или персональных данных	халатность персонала, незащищенность информационных источников, несанкционированный доступ третьего лица к информации, нарушение режима хранения информации	Управление информационных технологий	
	Несоответствие прав доступа к информационным системам	Отсутствие разграничения прав доступа к информационным системам, предоставленные права не соответствуют потребностям, отсутствует контроль за нарушением прав доступа	отсутствие регламента предоставления прав доступа, сотрудники имеют избыточные права доступа к информационным системам	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	
	Ненадлежащее функционирование используемых средств криптографической защиты информации	Риск ненадлежащего функционирования используемых средств криптографической защиты информации	неэффективность и/или неадекватность технологий	Управление информационных технологий	
	Необеспечение порядка осуществления ЭДО	Риск необеспечения (ненадлежащего обеспечения) порядка осуществления ЭДО	неэффективность и/или неадекватность технологий, порядка и способов осуществления ЭДО	Управление информационных технологий	
	Нарушение целостности информации баз данных	Риск нарушения целостности информации баз данных организации	некомпетентность, халатность сотрудников, сбои в работе	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	

	Сбой организации работы в подразделениях	Риски возникновения сбоев работы в подразделениях	изменение порядка взаимодействия и порядка проведения операций непосредственными исполнителями без уведомления руководителя, отсутствие взаимопонимания между сотрудниками, непередача или передача с опозданием информации между сотрудниками, способной повлиять на адекватность действий, нечеткое представление сотрудниками организации прав и обязанностей организации и клиентов, незнание или нечеткое знание действующего законодательства и положений внутренних документов, недобросовестное исполнение должностных обязанностей сотрудниками	Управление информационных технологий, Депозитарий, Управление спецдепозитарных операций	
--	--	--	---	--	--

	Сбой в процедуре заключения договора	Риски возникновения сбоев в процедуре заключения договоров	оформление договора клиентом самостоятельно без последующей проверки сотрудниками организации, подписание договора неуполномоченным лицом либо получение договора с неподлинными подписями, некорректное составление договора при внесении изменений и дополнений в шаблонный договор, заключение договора по поддельным документам, предоставление клиентом недостоверных сведений при заключении договора, недостаточно тщательная экспертиза документов клиента сотрудниками организации	Депозитарий, Управление спецдепозитарных операций	
	Сбой в процедуре приема поручений от клиента	Риск нарушения процедуры приема поручений от клиента	прием поручений/распоряжений с неподлинными подписями, прием поручений/распоряжений с ошибками в заполнении, прием поручений/распоряжений, подписанных неуполномоченным лицом, выбор для исполнения ошибочного поручения/распоряжения при неоднократном переделывании документа клиентом, ошибка	Депозитарий	

			сотрудника при внесении информации в систему учета		
	Сбой в процедуре выявления нарушений	Риск сбой в процедуре выявления нарушений	несвоевременное выявление/устранение нарушений; ложное обнаружение факта нарушения (фактов устранения нарушения или не устранения нарушения в установленный срок); выдача ошибочного согласия или отказа в согласии на распоряжение имуществом; несвоевременная отправка уведомлений о выявлении/устранении нарушений; несвоевременное включение (исключение) актива в расчете; нарушение сроков выполнения контрольных функций (формирования и направления отчетов, выдачи согласий, уведомлений о нарушениях и т.д.)	Управление спецдепозитарных операций	
	Сбой при обслуживании корпоративных действий эмитента	Риск возникновения нарушений при проведении обслуживании корпоративных действий эмитента	ошибки сотрудников организации при проведении операций в системе учета, несвоевременное уведомление клиентов о проведенных корпоративных действиях, ошибки при перечислении клиентам доходов по ценным бумагам	Депозитарий	

	Сбой в процедуре выставления счетов за услуги	Риск нарушения процедуры выставления счетов за услуги	неверный расчет комиссии по тарифам организации, выставление счета с указанием неверных реквизитов клиента, неверный расчет при перевыставлении расходов, понесенных организацией при оплате услуг третьих лиц	Депозитарий, Управление спецдепозитарных операций	
	Сбой в процедуре проведения операций с бездокументарными ценными бумагами	Риск сбоев в процедуре проведения операций с бездокументарными ценными бумагами	ошибки сотрудников организации при заполнении поручений/ распоряжений депозитариям - корреспондентам и регистраторам, в результате чего операции не исполняются либо бумаги пререходят не на тот счет; недобросовестное отношение (умышленные ошибки) депозитариев - корреспондентов и/или регистраторов к исполнению поручений/ распоряжений, в результате чего операции не исполняются либо бумаги переходят не на тот счет; несвоевременное уведомление депозитариями - корреспондентами об исполнении/ неисполнении поручений; умышленный вывод ценных бумаг сотрудниками организации на подставные компании в реестр с целью личного обогащения; исполнение	Депозитарий	

			операций без поручения клиента и/или отчета с места хранения; при наличии ошибки в выписке из реестра сделок, принятых в клиринг, зачисление/списание ценных бумаг не по тому счету; при подаче клиентом поручения на количество ценных бумаг, превышающее остаток по счету депо, трансляция поручения в депозитарий-корреспондент (регистратор) и последующее исполнение поручения по месту хранения; ввод недостоверной информации при приеме выпуска ценных бумаг на обслуживание; ошибки сотрудников при исполнении поручений клиентов		
	Сбой в процедуре перевода по счетам депо	Риск нарушения процедуры перевода ценных бумаг по счетам депо	ошибки сотрудников организации при исполнении поручений (переведены неверные ценные бумаги, неверно выбран счет получателя), исполнение операций в отсутствии встречного поручения	Депозитарий	
	Несоблюдение условий заключенных договоров	Риск несоблюдения организацией условий заключенных договоров (с регистраторами, депозитариями - депонентами, вышестоящими депозитариями, клиентами)	халатность (мошеннические действия) сотрудников Депозитария, технические проблемы, проблемы связи	Депозитарий, Управление спецдепозитарных операций	

Технические риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Невозможность оперативного устранения последствий неисправностей оборудования	Организация не в состоянии организовать своевременную и эффективную работу по устранению последствий неисправностей оборудования	низкая надежность систем, недостаточный уровень квалификации персонала, недостаточность финансирования	Управление информационных технологий	
	Неисполнение оборудованием возложенных на него функций из-за отказов и нарушений в работе	Риск невозможности исполнения оборудованием возложенных на него функций из-за отказа и нарушений в работе	износ оборудования, отсутствие планирования замены устаревшего оборудования	Управление информационных технологий	
	Самопроизвольные сбои в работе оборудования	Риск самопроизвольного сбоя в работе оборудования	износ оборудования	Управление информационных технологий	
	Отключение электроэнергии/перепады напряжения	Риск отключения электроэнергии/перепады напряжения	сбой в деятельности энергопоставляющей компании. Нарушение электропроводки в здании, в котором находится офис	Управление информационных технологий	

Комплаенс-риск (регуляторный)					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Применение юридических санкций или санкций государственных органов	Риск возникновения убытков, прекращения деятельности в связи с применением юридических санкций или санкций государственных органов	Несоблюдение законов и нормативно - правовых актов, касающихся деятельности Организации, несоответствие внутренних документов требованиям законодательства, несвоевременное внесение изменений и дополнений во внутренние документы в связи с изменением законодательства, предоставление отчетности не в полном объеме и в нарушении установленных сроков, нарушение сроков выполнения операций, несоответствие деятельности в целом лицензионным требованиям (достаточность собственного капитала, количество аттестованных сотрудников, соответствие сотрудников квалификационным требованиям)	Дирекция, Депозитарий, Управление спецдепозитарных операций	

Риски ОД/ФТ					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Вовлечение организации в отмывание преступных доходов	Риск вовлечения организации в отмывание преступных доходов, в том числе обусловленное совершением клиентом организации операций, направленных на легализацию (отмывание) доходов, полученных преступным путем и финансирование терроризма	Несоблюдение законодательства в части ПОД/ФТ	Дирекция, Депозитарий, Управление спецдепозитарных операций	

Организационные риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Несоответствие организационной структуры	Риск несоответствия/ неэффективности организационной структуры деятельности организации, а также риск несоблюдения требований регулирующего органа к организационной структуре организации	отсутствие анализа деятельности организации, распределения функций между подразделениями; незнание законодательства по направлениям деятельности организации	Дирекция	
	Несоответствие распределения функциональных (должностных) обязанностей и полномочий между структурными подразделениями	Риск несоответствия/ неэффективности распределения функциональных (должностных) обязанностей и полномочий между структурными подразделениями	отсутствие анализа распределения функций между подразделениями организации	Дирекция, Депозитарий, Управление спецдепозитарных операций	

Стратегические риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Неправильное или недостаточно обоснованное определение перспективных направлений деятельности организации	Риск недостаточного изучения и определения перспективных направлений деятельности	Изменение экономической ситуации. Ошибки, допущенные при стратегическом планировании деятельности организации	Дирекция	
	Отсутствие в полном объеме необходимых ресурсов и организационных мер, которые должны обеспечить достижение стратегических целей деятельности организации	Риск недостаточности ресурсов для достижения стратегических целей	Изменение экономической ситуации. Ошибки, допущенные при стратегическом планировании деятельности организации	Дирекция	
	Изменение спроса на услуги	Риск изменения рыночной конъюнктуры	Изменение экономической ситуации. Ошибки, допущенные при стратегическом планировании деятельности организации	Дирекция	

Политические риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Изменение политической ситуации	Риск изменения политической ситуации	Введение санкций, решения Правительства (замораживание накопительной части пенсии и др.)	Дирекция	

Отраслевые риски

№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Изменение бизнес - ситуации в отрасли	Риск изменения бизнес - ситуации (возможное ухудшение) в отрасли	Введение дополнительных требований к деятельности, выход новых аналогичных организаций на рынок	Дирекция	

Репутационные риски (риск потери деловой репутации)

№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Снижение доверия к организации	Риск формирования негативного мнения и снижения доверия к организации у клиентов, контрагентов	Негативные публикации в СМИ о качестве оказываемых услуг, финансовой устойчивости, характере деятельности организации в целом	Дирекция	

Риски правового регулирования

№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Несоблюдение организацией требований заключенных договоров	Риск несоблюдения условий договоров, что может существенно повлиять на деятельность организации	Неукомплектованность квалифицированным персоналом	Дирекция, юридическая служба	

	Несовершенство правовой системы	Противоречивость законодательства, отсутствие правовых норм по регулированию отдельных вопросов, возникающих в процессе деятельности организации	Неукомплектованность квалифицированным персоналом	Дирекция, юридическая служба	
--	--	--	---	------------------------------	--

Финансовые риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Рост просроченной кредиторской задолженности	Недостаток запланированных финансовых ресурсов для обеспечения своевременного выполнения обязательств организации перед контрагентами	отсутствие денежных средств на оплату услуг контрагентов, отсутствие контроля за финансовыми потоками организации	Дирекция, бухгалтерия	
	Рост просроченной дебиторской задолженности	Рост просроченной дебиторской задолженности в связи с ростом задолженности по оплате оказанных организацией услуг	банкротство контрагента, несвоевременная оплата услуг клиентами,	Дирекция, бухгалтерия	
	Ошибки при проведении расчетно - кассовых операций	Ошибки при формировании документации для проведения расчетно - кассовых операций и последующее некорректное осуществление таких операций с ущербом для организации	ошибки персонала, недостаточность контроля финансовой деятельности организации, низкий уровень мотивации персонала	Дирекция, бухгалтерия	

	Валютный риск при исполнении контрактов	Контракты, заключенные в иностранной валюте являются источником валютного риска организации. При изменении курса валюты к рублю изменяются и платежи по данным контрактам.	заключение контрактов в иностранной валюте, рост курса иностранной валюты к рублю на финансовых рынках	Дирекция, бухгалтерия	
	Валютный риск финансовых вложений	Риск возникновения убытков по финансовым активам, выраженным в иностранной валюте	Рост курса рубля по отношению к иностранной валюте	Дирекция, бухгалтерия	
	Использование некорректных или неполных исходных данных для осуществления расчетов налогов	Риск предоставления неполной или некорректной исходной информации для проведения налоговых расчетов, что может привести к завышению или занижению налоговых обязательств организации, отраженных в финансовой отчетности	отсутствие четких методологических материалов и инструкций для учета затрат организации для целей налогообложения, сбой программного обеспечения, серверного оборудования или каналов связи	Дирекция, бухгалтерия	
	Ошибки в расчетах платежей по налогам	При формировании налоговой отчетности организации возможны ошибки расчетов	ошибки персонала при расчетах налогооблагаемой базы и начислении налога, в учетных системах данные о начисленных суммах налогов частично или полностью утрачены по причине сбоев программного обеспечения	Дирекция, бухгалтерия	

	Несвоевременная/ не в полном объеме уплата налогов	Риск задержки и неполной уплаты налоговых обязательств организации	отсутствие необходимых денежных средств, сбой программного обеспечения, ошибки персонала при осуществлении перечисления денежных средств, либо несвоевременность перечисления денежных средств	Дирекция, бухгалтерия	
	Обесценение финансовых вложений	Организация обладает финансовыми вложениями, стоимость которых может со временем существенно снизиться	Стоимость финансовых вложений на балансе организации имеет завышенную стоимость по сравнению с рыночной стоимостью	Дирекция, бухгалтерия	
	Невозможность реализовать финансовый актив	Риск невозможности реализации финансового актива на рынке в требуемые сроки по текущим рыночным котировкам	Отсутствие спроса на реализуемый финансовый актив, изменение рыночной ситуации	Дирекция, бухгалтерия	
	Рост инфляции	Риск увеличения уровня инфляции сверх ожидаемых значений	изменение экономической ситуации	Дирекция, бухгалтерия	

Форс-мажорные риски					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Непредотвратимые чрезвычайные ситуации	Риск возникновения непредотвратимых чрезвычайных ситуаций	стихийные бедствия, военные действия, террористические акты, техногенные катастрофы	Дирекция, Управление информационных технологий	

Кастодиальный риск					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Возникновение различного рода убытков, связанных с учетом (хранением) ценных бумаг клиентов организации, самой организации	Риск неисполнения обязательств перед клиентом в отношении принадлежащих ему ценных бумаг; Риск утраты (повреждения) ценных бумаг клиентов, существующих в наличной форме; Риск утраты ценных бумаг организации	Выбор недостаточно надежных мест хранения ценных бумаг; Недостаточно защищенный способ хранения ценных бумаг, существующих в наличной форме	Дирекция, Управление спецдепозитарных операций, Депозитарий	

Коммерческий риск					
№ п/п	Подвид риска	Описание риска		Владелец риска	
		описание риска	источники риска	Подразделение	ФИО
1	2	3	4	5	6
	Потеря доходности по основному виду деятельности	Риск снижения поступлений от основной деятельности организации	Отсутствие новых договоров на обслуживании; Расторжение действующих договоров с клиентами	Дирекция	