Утверждено
Советом директоров
ОАО «УК «ЕВРОФИНАНСЫ»
Протокол №11/11/2011
от 11 ноября 2011 г.
Председатель Совета директоров

_____А.А. Снежко

РЕГЛАМЕНТ

ПО УПРАВЛЕНИЮ

операционными рисками

Открытого Акционерного Общества

«УПРАВЛЯЮЩАЯ КОМПАНИЯ «ЕВРОФИНАНСЫ»

(2-я редакция)

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ 3
2. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ 3
3. ВЫЯВЛЕНИЕ И ФИКСАЦИЯ ОПЕРАЦИОННОГО РИСКА..... 4
4. МЕТОДЫ ОЦЕНКИ ОПЕРАЦИОННОГО РИСКА..... 5
5. ПРОЦЕСС УПРАВЛЕНИЯ И КОНТРОЛЯ РИСКОВ..... 6

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент разработан в соответствии со стандартами и требованиями современной практики управления рисками компаний, основной деятельностью которых выступает управление денежными средствами на финансовых рынках. Регламент соответствует требованиям Устава ОАО «УК «ЕВРОФИНАНСЫ» (далее – Общества) и его внутренних документов.

1.1. Настоящий регламент определяет следующие направления деятельности по управлению операционными рисками:

- цель, задачи и принципы управления рисками;
- выявление и фиксация рисков;
- методы оценки рисков;
- процесс управления и контроля рисков.

1.2. Настоящий регламент разработан с целью достижения оптимального баланса между рисками и доходностью для Общества в целом и его Клиентов, при соблюдении норм законодательства и положений Устава Общества, а также с целью выработки стимулов, адекватных уставной деятельности органов управления Общества, его структурных подразделений и отдельных сотрудников.

1.3. Под операционным риском понимается риск прямых или косвенных потерь (убытков) от неадекватных или ошибочных внутренних процессов Общества, действий сотрудников, операционных систем, внешних событий.

1.3.1. Источниками операционных рисков выступают ошибки, несоответствия, нарушения деятельности персонала, внутренних систем Общества, а также внешних систем, взаимодействующих с Обществом.

1.3.3. Основными факторами или событиями, способными усилить влияние и масштабы проявления опреационного риска являются:

- изменение законодательства, требований регулирующих органов;
- расширение масштабов деятельности, увеличение объемов операций;
- усложнение финансовых инструментов и стратегий;
- освоение новых продуктов и технологий;
- усложнение систем технологической поддержки операций, внедрение новой техники.

1.3.4. Управление операционным риском нацелено на максимально возможное его предотвращение и вследствие этого основано как на применении качественных и количественных методов анализа, так и на создании адекватной системы внутреннего контроля.

2. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ

2.1. Целью управления операционными рисками как составной частью общего процесса управления рисками выступает предотвращение данного риска или максимально возможное снижение угрозы потенциальных убытков для обеспечения устойчивой и эффективной деятельности Общества, а также для соблюдения интересов его Клиентов при максимальной сохранности капитала и активов.

2.2. Задачами Общества в области управления операционными рисками являются:

- создание, поддержание и совершенствование эффективного механизма своевременной идентификации и предотвращения возможных негативных событий;
- определение приемлемого уровня конкретных видов операционных рисков с точки зрения экономической целесообразности затрат на их оценку, анализ и мониторинг;
- создание, поддержание и совершенствование системы внутреннего контроля за операционными рисками;
- принятие адекватных мер для снижения/избежания потерь.

2.3. Принципы управления операционными рисками:

- осведомленность о риске;
- разделение полномочий;

- контроль операционных рисков от нижнего уровня, операционного контроля, до верхнего уровня, управленческий контроль;
- использование новейших информационных технологий;
- постоянное совершенствование системы управления операционными рисками.

2.4. Основные подходы к оценке и управлению операционными рисками:

- восходящий подход – выявляются и оцениваются источники, причины и последствия возникновения риска. Осуществляется на постоянной основе сотрудниками и руководителями департаментов Общества в соответствии с функциональными обязанностями, положениями и операционными регламентами, других внутренних нормативных документов;
- нисходящий подход – оцениваются последствия реализации риска. В целях принятия адекватных мер, направленных на совершенствование системы управления операционными рисками, руководство Общества рассматривает подготовленные отчеты о реализованных операционных рисках, фактах нарушений операционных регламентов и процедур, установленных полномочий и ограничений.

3. ВЫЯВЛЕНИЕ И ФИКСАЦИЯ ОПЕРАЦИОННОГО РИСКА

3.1. В целях выявления операционного риска используются следующие методы:

- анализ доступных сведений и информации, включая описание случаев реализации операционных рисков;
- проведение консультаций/тренингов с сотрудниками Общества и внешними экспертами;
- изучение структуры корпоративного управления и бизнес-процессов;
- сценарный анализ деятельности Общества;
- проверка условий работы сотрудников Общества;
- оценка рисков;
- исследование финансового рынка и других сред, в которых задействована деятельность Общества.

3.2. Основные типы операционного риска, необходимые для принятия во внимание риск-менеджерами:

- внутреннее мошенничество и злоупотребление служебным положением;
- внешнее мошенничество;
- трудовые отношения и безопасность рабочих мест;
- ошибки профессиональной деятельности;
- физическое уничтожение имущества;
- приостановление процессов и ошибки систем;
- эндогенные и экзогенные нарушения в бизнес-процессах.

3.3. Перечень обстоятельств, наступление которых необходимо учитывать риск-менеджерам:

- локальные и муниципальные чрезвычайные ситуации техногенного или природного характера (в том числе аварии, аварийные выбросы, пожары, взрывы, высвобождения различных видов энергии, разрушения, затопления зданий, землетрясения, ураганы, наводнения);
- отключение электро-, водо-, теплоснабжения, систем вентиляции и кондиционирования, иных видов обеспечения повседневной деятельности;
- перебои в предоставлении услуг телефонной связи, телематических услуг связи, услуг передачи данных, услуг электронной почты, услуг доступа к информационным ресурсам в сети Интернет, других видов информационных услуг;
- акты иностранных государств, содержащие запрет или ограничивающие осуществление деятельности российских компаний;
- законы и иные нормативные акты РФ, устанавливающие запреты и ограничения;
- действия органов государственной власти РФ в отношении Общества, в том числе наложение ареста на счета, запрет на проведение отдельных операций, приостановление действия лицензий, проведение следственных действий и

другие действия, приводящие к приостановлению нормального режима деятельности;
- противоправные действия в отношении Общества и ее исполнительных органов, приводящие к приостановлению нормального режима ее деятельности.

3.4. По каждому выявленному операционному риску риск-менеджеры в целях описания и документирования рисков составляют формализованные описания операционных рисков, которые в совокупности формируют и пополняют карту операционных рисков Общества.

4. МЕТОДЫ ОЦЕНКИ ОПЕРАЦИОННОГО РИСКА

4.1. Общество проводит оценку операционного риска в отношении отдельных бизнес-процессов и в отношении деятельности в целом. Риск-менеджеры проводят оценку рисков не реже одного раза в полугодии. Помимо планового проведения оценки рисков, оценка также производится в случаях внедрения новых бизнес-процессов, технологий, продуктов и услуг.

4.2. Для оценки операционного риска могут применяться следующие методы оценки:
- метод, основанный на статистическом анализе распределения убытков;
- балльно-весовой метод (метод экспертной оценки);
- математические методы и модели оценки.

4.3. Общество осуществляет последовательный, поэтапный переход от применения простых методов и подходов к оценке операционного риска к более сложным, перемещаясь вдоль цепочки возможных подходов по мере разработки более продвинутых систем и практики измерения операционного риска.

4.4. Одновременно с процессом накопления и систематизации внутренних данных о реализованных рисках, в целях развития и совершенствования процедур мониторинга уровня операционного риска Общество осуществляет последовательное формирование системы индикаторов операционных рисков с определением пороговых значений и проведением тестирования индикаторов. Применяемые индикаторы и их пороговые значения подлежат уточнению и корректировке в процессе моделирования и обратного тестирования, с учетом оценки чувствительности конкретного индикатора и анализа его эффективности.

4.5. Базовый подход - оценка операционного риска в целях определения достаточности средств Общества:

4.5.1. Требование к необходимым средствам для покрытия операционного риска определяется по следующей формуле ОР=(ЧД/n)*К, где

ЧД – чистые доходы (только положительные) по видам деятельности, которым присущ операционный риск, за каждый из предыдущих n лет;

n – количество лет, в которых ЧД был положительным (определяется риск-менеджерами по согласованию с руководством);

К – коэффициент (согласно современной практике берется равным за 15%, однако может корректироваться риск-менеджерами по согласованию с руководством);

4.5.2. Базовый подход проводится по итогам работы Общества за год или квартал;

4.5.3. Базовый подход применяется также в целях бизнес-планирования и в рамках процедур стресс-тестирования.

4.6. Оценка текущего уровня операционного риска:

4.6.1. В целях мониторинга текущего уровня операционного риска проводится индикативная оценка на основании данных о расходах общества, связанных с реализацией операционного риска, и прибыли Общества;

4.6.2. Текущий уровень операционного риска определяется по формуле ТОР=Р/П*100%, где

Р – расходы, связанные с реализацией операционного риска, произведенные/понесенные в отчетном периоде;

П – чистая прибыль, полученная в отчетном периоде;

4.6.3. После определения значения показателя текущего уровня операционного риска, анализируется его динамика в сравнении с предшествующим (сопоставимым) периодом, соответствующим периодом прошлого года, а также со средним значением данного показателя за последние три года (включая текущий);

4.6.4. Оценка текущего уровня операционного риска осуществляется на регулярной (ежеквартальной) основе, по итогам работы за квартал, полугодие, девять месяцев, год;

4.6.5. Показатель текущего уровня операционного риска может применяться в целях прогнозирования величины потенциальных операционных убытков. При его определении применяются трендовые методы и экспертные оценки.

4.7. Экспертная оценка операционного риска:

4.7.1. Метод экспертных оценок применяется в отношении операционных рисков, не имеющих явного стоимостного выражения, а также при отсутствии полноценных исторических или статистических данных о реализованных рисках;

4.7.2. Экспертная оценка проводится в целях выявления подверженности процессов и операций подразделения или Общества в целом отдельным источникам и факторам операционного риска, в том числе влиянию внешней среды, а также выявления слабых мест и зон концентрации риска на отдельных направлениях бизнеса, операциях и процедурах;

4.7.3. Процедура экспертной оценки проводится на основе комплексного анализа принимаемых операционных рисков (отдельных видов операционного риска) и оценки адекватности деятельности требованиям нормативных документов;

4.7.4. Экспертная оценка операционных рисков (в том числе в целях стресс-тестирования отдельных направлений деятельности) осуществляется не реже одного раза в год.

4.8. В целях обеспечения учета, хранения и анализа данных о случаях реализации операционного риска Обществом ведется внутренняя база данных о случаях реализации операционного риска. Во внутреннюю базу данных о случаях реализации операционного риска включаются сведения о рисках, повлекших убытки в любом размере.

5. ПРОЦЕСС УПРАВЛЕНИЯ И КОНТРОЛЯ РИСКОВ

5.1. Основные этапы процесса управления операционными рисками:

- идентификация (определение причин и предпосылок, вследствие которых Обществу причинен или может быть причинен ущерб);
- оценка операционного риска;
- анализ проблемных зон процессов, выработка и принятие решения по оптимизации или изменению процессов в целях снижения уровня операционного риска;
- мониторинг операционного риска (выявление событий, способствующих изменению степени подверженности деятельности Общества операционному риску, а также изменению уровня операционного риска; отслеживание динамики показателей, характеризующих уровень операционного риска, с целью выявления отклонений и определения тенденций в изменении уровня операционного риска);
- контроль и снижение операционного риска (принятие управленческого решения в отношении выявленного операционного риска, контроль выполнения заявленных мероприятий по снижению уровня операционного риска и устранению проблемных зон в процессах).

5.2. В процессе управления операционными рисками Общество использует следующие методы:

- разработка, согласование и утверждение стратегических планов развития и отдельных направлений деятельности Общества;
- система разделения полномочий и иерархии подчиненности;
- коллегиальность принятия решений по проведению операций, подверженных риску;
- процедура разработки, согласования, юридической экспертизы и утверждения внутренних нормативных документов;
- система лимитов и ограничений;
- реализация принципа двойного контроля при совершении операций, их отражении в бухгалтерском учете, вводе данных в учетные и операционные системы;
- система санкционирования операций, предварительного, текущего и последующего контроля;

- наличие эффективной системы внутреннего контроля;
- регулярная ревизия адекватности действующих внутренних нормативных документов;
- обеспечение сокращения числа нештатных ситуаций и минимизация влияния сбоев в ИТ-инфраструктуре;
- обеспечение оптимальных характеристик автоматизированных систем в соответствии с требованиями бизнеса, исключение ситуаций недостатка ресурсов для решения операционных задач;
- наличие плана действий в случае возникновения аварийных и нештатных ситуаций;
- адекватная кадровая политика, определяющая систему подбора, расстановки, аттестации, повышения квалификации и мотивации персонала;
- наличие внутренних документов, определяющих функции и полномочия структурных подразделений;
- наличие должностных инструкций, определяющих полномочия, функциональные обязанности и заменяемость сотрудников.
- система администрирования (разграничения прав доступа) и контроля предоставленных прав доступа;
- система аудита действий пользователей информационных сетей;
- система записи переговоров в дилинговом зале.
- защита помещений, оборудования и электронных систем от взлома, несанкционированного проникновения, несанкционированных операций, хищения активов и перехвата информации;
- система мониторинга и противодействия попыткам взлома и несанкционированного проникновения в информационные сети;
- разработка типовых форм договорной документации и внутренней документации;
- разработка порядка рассмотрения, экспертизы и заключения нестандартных договоров и соглашений;
- поддержание в актуальном состоянии справочных правовых систем.