**Реферат**

По дисциплине: «УПРАВЛЕНИЕ ФИНАНСОВЫМИ РИСКАМИ»

На тему:

**«СИСТЕМА УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ В КРЕДИТНОЙ ОРГАНИЗАЦИИ»**

г. Москва – 2009 г.

**Введение**

Руководство и собственники кредитных организаций уделяют все более пристальное внимание управлению операционными рисками (ОР). Несмотря на безусловную очевидность существования подобных рисков и необходимость управления ими специалисты не всегда имеют четкое и исчерпывающее представление о методах комплексной и эффективной реализации данного процесса. В рамках настоящей статьи мы рассмотрим основные подходы и принципы внедрения системы управления операционными рисками. Изначально определим, что под системой управления операционными рисками (далее — СУОР) мы понимаем комплекс организационных, методических, автоматизированных средств по предупреждению возможных операционных рисков, минимизацию отрицательных последствий и недопущение повторов их реализации. В качестве определения операционного риска приведем наиболее часто встречающуюся формулировку: риск возникновения убытков (недополучения прибыли) в результате несоответствия характеру и масштабам деятельности банка и/или требованиям действующего законодательства внутренних порядков и процедур проведения банковских операций и других сделок, их нарушения служащими банка и/или иными лицами (вследствие некомпетентности, непреднамеренных или умышленных действий или бездействия), несоразмерности (недостаточности) функциональных возможностей (характеристик) информационных, технологических и других систем и/или их отказа (нарушения функционирования), а также в результате воздействия внешних событий. Можно указать следующие источники возникновения ОР:

персонал (намеренные / ненамеренные действия сотрудников организации, которые могут нанести ущерб ее деятельности);

процессы (ошибки и некорректное выполнение операций в ходе осуществления бизнеспроцессов либо должностных обязанностей);

системы (нарушение текущей деятельности организации в результате сбоя в информационных системах и/или недоступности IT-сервиса);

внешняя среда (воздействия извне, которыми организация не может управлять и которые выходят за рамки ее непосредственного контроля). Операционные риски корпоративного уровня безусловно влияют на деятельность банка, однако не всегда учитываются в стратегии его развития. Бесспорным является и тот факт, что реализация указанных рисков влияет на финансовый результат: статистика показывает, что прямые потери могут составлять 5–20% от величины капитала под операционные риски, остальные потери являются скрытыми и носят качественный характер. Таким образом, отсутствие СУОР приводит к возникновению массы проблем и повышает подверженность кредитной организации операционным рискам.

**Модель формирования и внедрения СУОР**

В соответствии с письмом Банка России от 24 мая 2005 г. №76-Т «Об организации управления операционным риском в кредитных организациях» под управлением операционными рисками понимаются их выявление, оценка, мониторинг, контроль и минимизация. Детализировав данную формулировку, мы получим следующие компоненты модели организации СУОР:

планирование внедрения СУОР;

обучение персонала банка и развитие культуры управления операционными рисками;

выявление операционных рисков;

учет и классификация инцидентов операционных рисков;

оценка операционных рисков;

предметный анализ операционных рисков;

решение задач по минимизации (устранению) операционных рисков;

мониторинг и контроль минимизации операционных рисков;

анализ СУОР.

**Планирование внедрения СУОР**

Планирование может выражаться в разработке документа «Концепция управления операционными рисками в рамках общей стратегии кредитной организации». Данный документ должен давать представление об «идеальном» состоянии уровня операционных рисков, к которому следует стремиться, чтобы получить максимальный результат. По мере возможности необходимо конкретизировать способы достижения целей, перечислив плановые задачи (оперативные, тактические, стратегические), которые будут решены в рамках СУОР.

**Обучение персонала и развитие культуры управления операционными рисками**

Формирование культуры управления ОР является одной из наиболее сложных задач: на начальном этапе риск-менеджеры, как правило, сталкиваются с сопротивлением и скепсисом персонала. Обучение персонала отличается от обучения риск-менеджеров. В рамках учебного курса необходимо найти разумный баланс между теорией и практикой, кроме того, следует обеспечить условия, позволяющие сотрудникам проходить обучение без отрыва от выполнения своих непосредственных обязанностей. По окончании учебного курса персонал должен иметь четкое представление о своем праве сообщать о выявленных операционных рисках, об адресате подобных сообщений, их форме, а также способах мотивации и получения обратной связи по результатам минимизации операционного риска. Очная форма обучения требует б*о*льших трудозатрат на организацию и проведение обучающих мероприятий, при этом объем аудитории сравнительно мал, а темп учебного процесса невысок. Система дистанционного обучения является более эффективной за счет широкого охвата аудитории (в нее могут входить все сотрудники филиальной сети), незначительных трудозатрат, возможности контролировать состав обучаемых и результаты динамичного учебного процесса. Развитие культуры управления ОР предполагает не только обучение персонала, но и проведение других мероприятий.

Разработка нормативных документов, а именно:

— раздела в составе политики по управлению рисками, касающегося управления ОР; идеальным вариантом является гармоничное функционирование СУОР в рамках общей системы управления рисками и ее взаимосвязь с другими корпоративными системами управления;

— регламента выявления и оценки операционных рисков (положение по операционным рискам);

— документов (в соответствии с перечнем нормативной документации), касающихся плана действий, направленных на обеспечение непрерывности деятельности и/или восстановление деятельности банка в случае возникновения непредвиденных обстоятельств.

Ознакомление сотрудника с регламентом выявления и оценки ОР при приеме на работу (в банке должен быть формализован перечень документов, обязательных для ознакомления при приеме на работу).

Внесение в раздел «Общие должностные обязанности» должностной инструкции пункта об обязанности каждого сотрудника банка минимизировать операционные риски в рамках своей должности.

Регулярная рассылка информационных писем, напоминающих о необходимости сообщать о возникших операционных рисках.

Внесение в реестр управленческой отчетности банка (при наличии такового) формата отчета по операционным рискам.

Донесение информации о выявленных ОР до ответственных подразделений (владельцев риска).

Неперсонифицированный обмен опытом между подразделениями (филиалами) в области управления ОР.

Внесение в форму сообщения об ОР графы «Предложения по минимизации операционных рисков». Сотрудников, внесших эффективные предложения, после проведения соответствующих мероприятий следует премировать. В данном случае можно провести аналогию с системой инноваций и рацпредложений.

**Выявление операционных рисков**

Важнейшим источником информации об операционных рисках являются сообщения от работников банка (горячая линия). Подобную информацию также получают в результате анализа проводок по операциям бухгалтерского учета (денежные выплаты, добровольно произведенные банком; денежные выплаты, произведенные банком на основании решений уполномоченных государственных органов; досрочное списание (выбытие) материальных активов; повторные затраты; регрессные потери; снижение стоимости активов; счета, отражающие создание резервов на возможные потери, и др.). Безусловно, необходимо выстраивать взаимодействие со смежными подразделениями, в ходе которого будет происходить обмен конфиденциальной информацией и ее анализ. В числе таких подразделений можно указать следующие:

бизнес-подразделения;

подразделение по информационной безопасности (информационные риски);

маркетинговое подразделение (жалобы клиентов, данные о мониторинге качества обслуживания);

подразделение по информационным технологиям (сведения о сбоях в IT-системах и количестве обращений пользователей в службу технической поддержки);

подразделение по безопасности (инциденты, по которым завершено / ведется расследование, информация о чрезвычайных и аварийных ситуациях);

подразделение по описанию и оптимизации бизнес-процессов банка;

подразделение по банковским технологиям и методологии (существенные операционные риски, источником которых могут быть бизнеспроцессы и документы банка);

подразделение финансового мониторинга;

подразделение по работе с персоналом;

юридическое подразделение (информация из области страхования);

служба внутреннего контроля. В связи с большим количеством бизнес-подраз делений и подразделений бэк-офиса одной из важных задач отдела по управлению операционными рисками является грамотное выстраивание информационных потоков в целях эффективного выявления ОР.

**Учет и классификация инцидентов ОР**

Выявленные инциденты операционного риска необходимо учитывать в специализированной базе данных. Содержание базы может меняться в зависимости от условий работы внутреннего заказчика. Перечислим основные реквизиты базы данных:

дата уведомления об операционном риске;

дата свершения инцидента;

структурное подразделение, в котором произошел инцидент;

описание инцидента;

причина инцидента;

последствия инцидента;

уровень последствий (существенность риска);

объем операции, сумма фактического и возможного убытка, сумма возмещения;

предложения по минимизации операционного риска;

направление деятельности (банковские продукты и услуги);

источник (фактор) риска (1–3 уровень);

принадлежность события к репутационному и информационному риску;

ФИО эксперта (в случае привлечения);

подразделение, отвечающее за минимизацию операционного риска. При ведении учета операционных рисков можно дополнительно определять степень их влияния на бизнес-процессы (при наличии в кредитной организации системы управления бизнес-процессами), на проекты (при наличии системы управления проектами), на расходы по статьям бюджета (при наличии системы бюджетирования). Операционные риски можно разделять по уровням: корпоративный уровень, уровень бизнес-единиц, операционный уровень. Взаимосвязь операционных рисков с теми или иными элементами смежных систем управления позволяет вести многогранный учет в соответствии с требованиями законодательства и пожеланиями внутреннего заказчика, а также проводить системный анализ уровня ОР и определять корреляцию между отдельными фактами их реализации. С целью разделения существенных и несущественных операционных рисков банк может самостоятельно разработать процедуру их классификации. В данной работе авторы не рассматривают такой критерий существенности / несущественности, как денежное выражение риска, поскольку при повышенной интенсивности реализации даже несущественные в денежном выражении риски могут значительно повлиять на работу банка. Незаменимым помощником при учете и анализе является справочник операционных рисков. Такие справочники составляют на основе результатов опросов страховых компаний, опросов внутри банка, по материалам изданий, специализирующихся на банковских технологиях, по данным базы инцидентов операционного риска. Стоит отметить, что база инцидентов операционного риска по аналогии с прецедентным правом может являться источником типовых решений, т.е. решение, вынесенное по какому-либо инциденту ОР, обязательно для всех подразделений организации при рассмотрении ими аналогичных операционных рисков. Данная система дает банку возможность выполнять нормотворческие функции не только в случае отсутствия описания бизнес-процессов, но и при наличии недостаточно четкой нормативной документации. Для проведения сравнительного анализа необходимо фиксировать ОР сторонних банков, обращаясь при этом к внешним источникам (например, к неструктурированной базе внешних операционных рисков, сформированной силами участников форума на сайте www.riskofficer.ru). Внешние источники позволяют отследить различные отечественные и зарубежные тенденции в сфере операционных рисков. Так, во время кризиса участились кражи денежных средств из банкоматов, кражи со счетов клиентов через систему дистанционного банковского обслуживания (ДБО), при изменении погодных условий (с наступлением морозов) увеличилось количество сбоев в работе банкоматов, возросло число мошеннических действий при кредитовании и т.д. Следует непрерывно изучать тенденции, анализировать текущую ситуацию в кредитной организации и в случае необходимости принимать меры по предупреждению операционных рисков (анализировать защищенность банкоматной сети и систем ДБО, оперативно менять месторасположение банкоматов (при наличии резервных мест), укреплять банкоматы, управлять лимитами загрузки банкоматов, вводить дополнительные способы защиты систем ДБО, обеспечивать страховое покрытие и т.д.). Отметим, что в других отраслях хозяйственной деятельности при наступлении аварии на одном участке автоматически проверяют все другие действующие участки в целях предупреждения повторных аварий. Авторы считают данный подход абсолютно правильным. Анализ внешних операционных рисков позволяет понять, какие системы защиты той или иной банковской услуги наиболее эффективны, и обеспечить новый банковский продукт надежной системой защиты.

**Оценка операционного риска**

В соответствии с Положением ЦБ РФ от 3 ноября 2009 г. №346-П «О порядке расчета размера операционного риска» размер ОР включают в расчет норматива достаточности собственных средств (капитала) банка (Н1) следующим образом:

начиная с отчетности на 1 августа 2010 г. — в размере 40% от рассчитанного в соответствии с настоящим Положением;

начиная с отчетности на 1 августа 2011 г. — в размере 70%;

начиная с отчетности на 1 августа 2012 г. — в размере 100%. Положение №346-П подлежит официальному опубликованию в «Вестнике Банка России» и вступает в силу с 1 июля 2010 г. В международной банковской практике применяют следующие методы оценки резерва капитала под операционные риски.

**Подход на основе базового индикатора**

**(Basic Indicator Approach, BIA)**

Упрощенный подход к расчету размера резерва капитала под операционные риски на основе базового индикатора предполагает прямую зависимость уровня операционного риска от масштабов деятельности организации. Естественно, что при этом не учитываются ни внутренние процедуры контроля, ни подверженность риску в различных направлениях деятельности.

**Стандартный подход**

**(The Standardized Approach, TSA)**

Данный подход основан на выделении нескольких типовых направлений деятельности кредитной организации и определении размера капитала, резервируемого по каждому из них. Такой подход является более точным, чем BIA.

**Альтернативный стандартный подход**

**(Alternative Standardized Approach, ASA)**

Отличие данного подхода от стандартного заключается в том, что для таких направлений деятельности, как банковское обслуживание физических и юридических лиц, расчет величины резервов производят не на основании показателя среднего валового дохода, а на основании величины средних остатков на соответствующих балансовых счетах.

**Балльно-весовой метод**

**(метод оценочных карт)**

Для определения величины потенциальных убытков на основании экспертных оценок выбирают наиболее информативные для целей управления операционным риском аналитические показатели и устанавливают их относительную значимость, затем выбранные показатели сводят в специальные таблицы (оценочные карты). Полученные результаты обрабатывают с учетом заданных весовых коэффициентов и сопоставляют по направлениям деятельности кредитной организации, отдельным видам банковских операций и сделок. На основании рассчитанных значений строят карты операционных рисков, наглядно демонстрирующие вероятность появления операционных рисков и размеры возможных потерь по каждому направлению деятельности организации.

**Статистический анализ распределения фактических убытков**

Методы, основанные на применении статистического анализа, позволяют составить прогноз потенциальных операционных убытков исходя из величины операционных убытков, полученных в прошлом. В ходе применения этих методов в качестве исходных параметров рекомендуется использовать информацию о реально понесенных операционных убытках, накопленную в аналитической базе данных.

**Моделирование (сценарный анализ)**

В рамках метода моделирования (сценарного анализа) величины операционных рисков экспертным путем определяют возможные сценарии возникновения событий или обстоятельств, приводящих к операционным убыткам. Для сравнительного анализа капитала под операционные риски различных банков можно воспользоваться сайтом www.tridea.ru и ознакомиться с оценкой указанного капитала, полученной с применением подходов BIA, TSA, ASA. В рамках оценки ОР можно сформировать *справочник потерь* для рисков, реализация которых не приносит прямых денежных потерь. Экспертным путем можно определить косвенные потери в денежном выражении: час простоя той или иной информационной и платежной системы стоит X руб., исправление ошибки персонала стоит Y руб., отказ клиента от дальнейшего обслуживания — Z руб. и т.д. Такой справочник может быть привязан к показателям конкретного филиала (доля выручки, количество процессов, количество персонала и др.), т.к. потери из-за аналогичных инцидентов в небольшом и крупном филиалах могут значительно отличаться. При отсутствии взаимосвязи потерь с показателями филиалов банка предлагается рассматривать несколько вариантов потерь (минимальные, средние, максимальные). В случае утверждения и размещения данного справочника в открытом доступе с риск-менеджеров будет снята масса вопросов по оцифровыванию потерь в результате инцидентов. Оценка косвенных потерь в денежном выражении позволяет определять приоритеты при минимизации операционных рисков. Прежде чем приступать к созданию такого справочника, необходимо оценить его необходимость и полезность (например, использование при расчете окупаемости мероприятий (проектов), направленных на минимизацию операционного риска). Справочник необходимо пересматривать с установленной периодичностью.

**Предметный анализ операционных рисков**

Зачастую мы имеем лишь общее и поверхностное описание выявленного операционного риска, и может сложиться обманчивое впечатление, что его можно без труда устранить силами нескольких работников за достаточно короткий срок. Практика показывает, что это не так. Необходимо проводить предметный анализ операционных рисков, представляющий собой не что иное, как функцию бизнес-анализа, т.е. риск-менеджер должен обладать навыками бизнес-аналитика. Последовательность проведения анализа может быть следующей: 1) анализ наличия / отсутствия нормативной документации (НД); отсутствие или неактуальность НД уже является операционным риском для банка; 2) анализ содержательной части НД (анализ технологий и бизнес-процессов); 3) описание бизнес-процесса (при отсутствии описания) в какой-либо нотации (например, IDEF) и проведение встреч с его владельцами и участниками; 4) сравнение выполнения процесса на практике с описанием в нормативной документации, выявление несоответствий; 5) запрос мнений экспертов, которые в обязательном порядке следует фиксировать и использовать в дальнейшей работе; 6) формирование отчета с предложениями по минимизации операционных рисков. В некоторых случаях вместо анализа инцидентов операционного риска необходимо проводить служебное расследование — в зависимости от того, какими правами, обязанностями и полномочиями наделены риск-менеджеры банка и как организовано взаимодействие с подразделением безопасности. При невозможности решения проблемы, выявленной в результате анализа, силами сотрудников данный вопрос передается на более высокий уровень:

путем формирования служебных записок в адрес руководства;

путем вынесения на обсуждение правлением банка;

путем вынесения на обсуждение специализированным коллегиальным органом управления (далее — КОУ) (технологическим комитетом, комитетом по операционным и информационным рискам);

при отсутствии специализированного КОУ — путем сбора информации о действующих коллегиальных органах управления банка и вынесения вопросов минимизации операционных рисков на обсуждение данными КОУ (в рамках полномочий каждого КОУ).

**Решение задач по минимизации (устранению) ОР**

В целях минимизации операционных рисков принимают как стандартные, так и нестандартные решения. К первым можно отнести принятие несущественного риска (в случае когда затраты на его устранение превышают ожидаемый эффект), а также выставление лимитов, страхование и аутсорсинг процессов (передача рисков сторонним организациям). По мере развития СУОР все большее применение получают нестандартные решения, т.к. операционные риски разноформатны и охватывают практически всю деятельность банка. В зависимости от трудоемкости, сложности задачи и компетенции риск-менеджеров ОР снижают различными способами:

силами ответственного подразделения (владельца риска);

силами подразделения риск-менеджмента;

путем формирования рабочих (кросс-функциональных) групп;

путем запуска проекта (проектный подход). Допустим, процесс кредитования в конкретном банке является длительным, дорогим и неэффективным (с высокой долей просроченных кредитов), т.е. банк несет прямые потери (кредитный риск) из-за неправильно выстроенного процесса (операционный риск). В ходе анализа процесса на соответствие бизнес-логике выявляют его недостатки и конкретизируют операционные риски. Далее разрабатывают варианты мероприятий по оптимизации процесса кредитования и минимизации операционных рисков. Затем реализуют утвержденные мероприятия по повышению прозрачности процесса (в том числе за счет автоматизации), вводят контрольные управленческие процедуры, изменяют входы и выходы подпроцессов и последовательность выполнения подпроцессов, актуализируют нормативные документы. Проведенная работа позволяет увеличить скорость кредитования, снизить стоимость процесса, рост и долю просроченных кредитов. Работу проводят несколько подразделений, и вклад каждого подразделения (в процентном соотношении) в финансовый результат определить сложно. Однако практика показывает, что в целом применение СУОР может в значительной степени влиять на финансовый результат. Кроме опосредованного влияния (в виде снижения операционных рисков, оптимизации бизнес-процессов, усиления внутреннего контроля за процессами, участия в коллегиальных органах управления и т.д.) подразделение по операционным рискам может оказывать и прямое влияние на финансовый результат, выражающееся в предупреждении мошенничества (в том числе возврат денежных средств), организации возмещения страховых сумм при наступлении страховых случаев, инициировании внедрения новых продуктов и технологий. По мнению авторов, СУОР должна функционировать таким образом, чтобы минимизация операционных рисков производилась комплексно. Рассмотрим несколько комплексов мероприятий (проектов), направленных на решение указанной задачи.

**Комплекс мероприятий по снижению риска персонала**

Повышение стандартов обслуживания и регулярный мониторинг качества обслуживания клиентов.

Разработка системы поддержки фронтофиса через call-центр.

Внедрение системы противодействия мошенничеству.

Распределение прав доступа в информационных системах и соблюдение правил информационной безопасности.

Внедрение эффективной системы мотивации персонала.

Анализ хронометража оказания услуг клиенту (сравнение нормативного значения с фактическим).

Создание «единого окна обслуживания» для сотрудников фронт-офиса (в случае если банк использует несколько разнородных информационных систем).

Анализ показателей по управлению персоналом (текучесть кадров, количество обученных сотрудников и т.д.).

**Комплекс мероприятий по снижению риска процесса**

Внедрение процессного подхода (структурирование бизнеса на процессы, описание процессов, определение владельцев процессов, нейтрализация «зон безответственности», своевременная актуализация внутренней нормативной документации и т.д.).

Формирование электронной *базы бизнеспроцессов*, поддерживаемых в актуальном состоянии (например, с применением программного обеспечения Business Studio (www.businessstudio.ru)).

Внедрение системы мониторинга показателей деятельности на ежедневной основе (применение ключевых индикаторов риска в рамках общей системы мониторинга показателей банка).

Анализ организационной структуры банка.

Внедрение системы разработки (от идеи до ввода в действие) дополнительных процессов и новых продуктов. В качестве примеров подобных процессов можно указать следующие:

— «Управление инновациями и рацпредложениями»;

— «Анализ внутренних инвестиционных проектов» (чистый денежный поток (NCF), индекс прибыльности (PI), срок окупаемости проекта (PBP), внутренняя норма рентабельности (IRR), модифицированная внутренняя норма рентабельности (MIRR), дисконтирование, средневзвешенная стоимость капитала (WACC));

— «Расчет маржинальной доходности в разрезе продуктов для эффективного управления продуктовым рядом».

Внедрение системы определения приоритетности автоматизации процессов (с учетом рисков).

Создание единого хранилища данных и формирование на его основе ERP-системы, системы бизнес-анализа (Business Intelligence, BI).

Усиление внутреннего контроля бизнеспроцессов.

**Комплекс мероприятий по снижению риска систем**

Оперативный учет информационных активов (информационные системы, оборудование, каналы связи).

Формирование планов восстановления IT-сервиса.

Внедрение системы оперативной замены оборудования, системы резервирования каналов связи.

Внедрение системы Help-Desk.

Виртуализация серверов.

Внедрение *проектного подхода* к деятельности подразделения, отвечающего за доработку используемого ПО и разработку нового.

Внедрение *сервисного подхода* к деятельности подразделения, отвечающего за обслуживание IT-сервисов (информационных систем) (IT Service Management, ITSM).

Четкое разделение функций между отделами, занимающимися разработкой программного обеспечения и обслуживанием информационных систем.

**Комплекс мероприятий по снижению риска внешней среды**

Комплексное страхование бизнеса.

Внедрение системы ОНиВД (обеспечения непрерывности деятельности и/или восстановления деятельности банка в случае возникновения непредвиденных обстоятельств): — повышение физической безопасности объектов банка; — повышение информационной безопасности банка; — повышение организационной безопасности банка. Представленные выше проекты могут быть как взаимодополняющими, так и взаимоисключающими. Мы понимаем, что решение данных задач требует активного участия всех подразделений банка. Успех описанных проектов зависит от уровня слаженности управленческой команды и понимания общих целей и задач.

**Мониторинг и контроль минимизации ОР**

Мониторинг проводят с установленной периодичностью путем наблюдения, т.е. операционному риску (группе операционных рисков) присваивается статус: «устранен», «минимизирован», «принят», «передан сторонним организациям», «в работе». Необходимо фиксировать, каким образом был минимизирован тот или иной операционный риск. Существует несколько вариантов проведения мониторинга.

На основании анализа индикаторов операционного риска. Отметим, что в некоторых случаях внедрение учетной системы ключевых индикаторов риска требует значительных затрат, при этом получаемый эффект остается «непрозрачным» в денежном выражении.

На основании отчетов руководителя рабочей группы о ходе выполнения того или иного проекта.

На основании повторного выявления операционных рисков.

На основании данных системы административного контроля (результаты выполнения задач, зафиксированных в письменной или электронной форме в контрольных карточках). Административный контроль позволяет снижать вероятность затягивания работ по минимизации ОР и зачастую помогает улучшить качество и эффективность выполнения решений. По мнению авторов, наиболее сложным моментом в мониторинге процесса минимизации ОР является определение качества выполняемых работ. Этот вопрос можно решить путем повышения компетентности риск-менеджеров в той или иной профессиональной области, а также с помощью сторонних экспертов (дорогой вариант решения) либо путем проведения опроса внутренних потребителей услуг. Система управления операционными рисками может быть представлена следующими отчетами:

отчеты, рекомендуемые ЦБ РФ;

отчет об операционных рисках, выявленных за определенный период (и вероятности их реализации); отметим, что большинство внутренних заказчиков интересует не математический расчет вероятности реализации риска (особенно в условиях кризиса), а конкретные меры по его предотвращению;

отчет по ключевым индикаторам риска (планфакт-анализ КИР);

отчет о технологическом отличии (превосходстве / отставании) от лидирующих кредитных организаций в части операционного риска;

отчет об операционных рисках корпоративного уровня и уровня бизнес-единиц;

карта рисков.

**Анализ СУОР**

Дополнительной полезной работой является регулярный анализ СУОР. Данный анализ можно проводить на основании методики, изложенной в письме Банка России от 23 марта 2007 г. №26-Т «О Методических рекомендациях по проведению проверки системы управления банковскими рисками в кредитной организации (ее филиале)». Результаты анализа дают представление о недостатках системы и позволяют определить приоритеты ее развития.

**Организационная структура подразделения, отвечающего за ОР**

В зависимости от величины кредитной организации, количества бизнес-процессов, широты продуктового ряда, наличия тех или иных систем управления численность подразделения по операционным рискам может варьироваться:

в небольших кредитных организациях — один сотрудник в каждом филиале (дополнительный функционал для сотрудника); качество управления рисками не будет высоким и может «иметь уклон» в профессиональную деятельность ответственного лица;

в средних кредитных организациях — рискменеджер в головном офисе (основной функционал) и ответственный сотрудник в каждом филиале (дополнительный функционал);

в больших кредитных организациях — рискменеджеры операционного риска в головном офисе (две-четыре штатные единицы) и рискменеджер в каждом филиале (две штатные единицы) либо ответственные сотрудники в филиале (два человека). Организационная структура подразделения по операционным рискам головного офиса может быть представлена следующими отделами:

отдел операционных рисков;

отдел по борьбе с мошенничеством;

отдел информационных рисков;

отдел оптимизации бизнес-процессов;

отдел методологии.

**Информационные средства управления ОР**

В качестве автоматизированного инструмента при управлении операционными рисками можно использовать следующее ПО: Excel, ULTOR, Zirvan, «Техносерв», «Бизнес-студио», а также собственные разработки. Мы не будем подробно рассматривать плюсы и минусы перечисленных программных продуктов. Отметим лишь, что автоматизация СУОР снижает трудоемкость работы риск-менеджеров, повышает оперативность выявления и качество анализа инцидентов операционного риска, способствует формированию базы знаний по операционным рискам, является эффективным инструментом контроля за мероприятиями, позволяет сократить денежные и временн*ы*е затраты на сопровождение системы.

**Заключение**

В данной статье мы не только рассмотрели структуру СУОР, но и попытались ответить на вопрос, как выстроить СУОР. Наличие в кредитной организации действующей системы управления операционными рисками обеспечивает эффективную работу риск-менеджеров, позволяет соответствовать ожиданиям внутреннего заказчика и требованиям законодательства. Безусловно, внедрение СУОР — это сложный, продолжительный, отчасти творческий процесс. Изложенные в статье тезисы не являются догмой или прямым указанием к действию. В качестве одной из важнейших характеристик системы управления операционными рисками следует указать ее гибкость, способность принимать ту или иную конфигурацию в зависимости от поставленных задач и потребностей внутреннего заказчика и эффективно дополнять корпоративную систему управления кредитной организации. Надеемся, что данная статья будет полезной как для начинающих риск-менеджеров, так и для опытных специалистов.