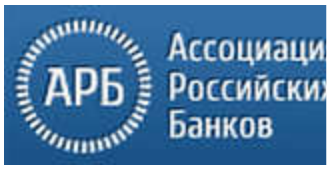
Комитет по стандартам Базель II и управлению рисками



Управление операционным риском

Авторы:

Арустамов Марат,	Росбанк
Белялова Светлана,	Райффайзенбанк
Бедрединов Рустам,	Бинбанк
Васильев Николай,	ЮниКредит Банк
Гатиятуллина Анжела,	Уралсиб
Глашев Мурат,	Oliver Wyman
Зырянова Полина,	ЮниКредит Банк
Ivell Thomas,	Oliver Wyman
Козырева Надежда,	ДжиИ Мани Банк
Пеникас Генрих,	Альфа-Банк
Сивакова Наталья,	Райффайзенбанк
Соловьева Дарья,	ДжиИ Мани Банк
Ясакова Елизавета,	Газпромбанк

Москва, 2013

Оглавление

Введение

Настоящий документ создан с целью отражения консолидированного мнения Экспертной группы №1, сформированной в рамках Постоянно действующей группы по вопросам Компонента 1 Комитета по стандартам Базель II и управлению рисками при Ассоциации российских банков, по направлению работы «Управление операционным риском» для представления Банку России и имеет следующую структуру.

Раздел «Аннотация» содержит краткое описание организации структуры документа и освещаемых в нём вопросов.

В разделе 1 «Перечень раскрываемых в документе тем» перечислена тематика вопросов, раскрываемых в документе. Структура раскрываемых тем повторяется в следующих разделах.

Раздел 2 «Позиция надзорных органов» содержит подразделы «Позиция Банка России» и «Позиция Европейских регуляторов». В каждом из подразделов приводятся цитаты либо резюме позиции регуляторов по темам, заявленным в разделе **Ошибка! Источник ссылки не найден.**.

Раздел 3 «Опыт коммерческих банков, лучшие практики» содержит описание используемых в российских коммерческих банках лучших практик. При этом формулировки данного раздела, имеющие характер требований (например, «банк должен осуществлять качественную оценку своих операционных рисков», «для эффективного применения КИР должны определяться следующие его характеристики» и др.), говорят о том, что в лучших практиках соответствующие принципы являются обязательными к исполнению. Структура раскрываемых тем соответствует заявленной в разделе **Ошибка! Источник ссылки не найден.**.

Раздел 4 «Консолидированная позиция ЭГ» содержит согласованные предложения Экспертной группы Банку России по нормативному регулированию вопросов, перечисленных в разделе **Ошибка! Источник ссылки не найден.**.

Раздел 5 «Особые мнения экспертов» содержит особые мнения экспертов по различным вопросам.

Раздел 6 «Дополнительная информация» содержит список сокращений, приложения и другую дополнительную информацию.

«Организация эффективной системы управления операционными рисками»

Мнение Экспертной группы 5 по операционному риску постоянно действующей группы №1 (ПГ 1) при Комитете по стандартам Базель II и управлению рисками при АРБ.

1. Перечень раскрываемых в документе тем

Организация эффективной системы управления операционными рисками. В частности, предлагается рассмотреть вопросы:

1.1. Определение операционного риска (включая взаимосвязь со смежными видами рисков)
1.2. Структура управления операционным риском
1.3. Основные инструменты системы управления операционным риском, включая
1.3.1. Идентификация и оценка рисков. Документирование этапа идентификации рисков / пересмотра перечня значимых рисков. Качественная оценка рисков. Ведение реестра рисков
1.3.2. Сбор данных о потерях
1.3.3. Контрольная среда. Самооценка рисков и контролей (RCSA)
1.3.4. Ключевые индикаторы риска (KRIs) и ключевые индикаторы контроля (KCI)
1.3.5. Ключевые показатели эффективности управления операционным риском (КПЭ/KPIs)
1.3.6. Сценарный анализ и стресс-тестирование
1.3.7. Планирование непрерывности и восстановления бизнеса
1.3.8. Тестирование контрольных процедур и влияние на остаточный риск
1.3.9. Система отчетности по операционным рискам

1.4. Классификация операционных рисков

1.4.1. Классификация событий операционного риска по видам

1.4.2. Классификация направлений деятельности

1.5. Требования по зрелости процессов и инструментов управления операционным риском для Базового индикативного, Стандартизированного и Усовершенствованного подходов.

2. Позиция надзорных органов

2.1. Позиция Банка России

2.1.1. Определение операционного риска (включая взаимосвязь со смежными видами рисков)

В нормативно-правовых актах Банка России содержится ряд рекомендательных писем по организации управления операционным риском: Письмо от 24 мая 2005 г. N 76-Т «Об организации управления операционным риском в кредитных организациях», далее Письмо 76-Т; Письмо 16 мая 2012 г. N 69-Т «О рекомендациях Базельского Комитета по банковскому надзору «Принципы надлежащего управления операционным риском», далее Письмо 69-Т; Письмо от 29 июня 2011 г. N 96-Т «О методических рекомендациях по организации кредитными организациями внутренних процедур оценки достаточности капитала», далее Письмо 96-Т; Письмо от 23 июня 2004 г. N 70-Т «О типичных банковских рисках», далее Письмо 70-Т и др. В части управления правовым риском и риском потери деловой репутации рекомендации содержаться в Письме от 30 июня 2005 г. N 92-Т "Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах", далее Письмо 92-Т.

Письмо 76-Т дает следующее определение операционного риска:

«**Операционный риск** - риск возникновения убытков в результате несоответствия характеру и масштабам деятельности кредитной организации и (или) требованиям действующего законодательства внутренних порядков и процедур проведения банковских операций и других сделок, их нарушения служащими кредитной организации и (или) иными лицами (вследствие непреднамеренных или умышленных действий или бездействия), несоразмерности (недостаточности) функциональных возможностей (характеристик) применяемых кредитной организацией информационных, технологических и других систем и (или) их отказов (нарушений функционирования), а также в результате воздействия внешних событий».

Письмо 96-Т дает следующее определение операционного риска:

«**Операционный риск** - риск возникновения убытков в результате ненадежности внутренних процедур управления кредитной организации, недобросовестности сотрудников, отказа информационных систем либо вследствие влияния на деятельность кредитной организации внешних событий».

Более того, Письмо 70-Т дает отдельные определения правового риска и репутационного риска без указания взаимосвязи с операционным риском.

Вышеуказанное определение, в свою очередь отличается от определения Базельского Комитета: «Под операционным риском понимается риск убытков, вызванных неадекватными или неработоспособными внутренними процессами и системами, их нарушением персоналом или в результате воздействия внешних факторов. Данное определение включает юридический риск, но исключает стратегический и репутационный риски».

Базельский комитет включает юридический риск в состав операционного риска, тогда как Банк России рассматривает правовой риск отдельно, что видно из названий Письма 76-Т и Письма 92-Т.

С точки зрения Банка России согласно Письму 92-Т

правовой риск - это риск возникновения у кредитной организации убытков вследствие влияния нижеследующих внутренних и внешних факторов.

К внутренним факторам относятся:

- несоблюдение кредитной организацией законодательства Российской Федерации, в том числе по идентификации и изучению клиентов, установлению и идентификации выгодоприобретателей (лиц, к выгоде которых действуют клиенты), учредительных и внутренних документов кредитной организации;
- несоответствие внутренних документов кредитной организации законодательству Российской Федерации, а также неспособность кредитной организации своевременно приводить свою деятельность и внутренние документы в соответствие с изменениями законодательства;
- неэффективная организация правовой работы, приводящая к правовым ошибкам в деятельности кредитной организации вследствие действий служащих или органов управления кредитной организации;
- нарушение кредитной организацией условий договоров;
- недостаточная проработка кредитной организацией правовых вопросов при разработке и внедрении новых технологий и условий проведения банковских операций и других сделок, финансовых инноваций и технологий.

К внешним факторам возникновения правового риска относятся:

- несовершенство правовой системы (отсутствие достаточного правового регулирования, противоречивость законодательства Российской Федерации, его подверженность изменениям, в том числе в части несовершенства методов государственного регулирования и (или) надзора, некорректное применение законодательства иностранного государства и (или) норм международного права), невозможность решения отдельных вопросов путем переговоров и как результат - обращение кредитной организации в судебные органы для их урегулирования;
- нарушения клиентами и контрагентами кредитной организации условий договоров;
- нахождение кредитной организации, ее филиалов, дочерних и зависимых организаций, клиентов и контрагентов под юрисдикцией различных государств.

Важно также, что, Банк России придаёт большое значение полноте и связности системы терминов, касающихся операционного риска. Так, согласно Письму 69-Т, непоследовательная система использования терминологии, относящейся к операционному риску, повышает вероятность того, что риски не будут выявлены и классифицированы или не будут распределены обязанности по оценке, мониторингу, контролю и снижению рисков.

2.1.2. Структура управления операционным риском

В нормативно-правовых актах Банка России содержится ряд рекомендательных писем по структуре управления операционным риском. Письмо 69-Т дает следующее определение: «Эффективное корпоративное управление является основой для создания Системы эффективного управления операционным риском (далее - Система управления).

Общепринятая банковская практика надлежащего управления операционным риском нередко основана на трех направлениях "линиях обороны" - (i) управлении направлениями деятельности, (ii) независимой корпоративной функции управления операционным риском и (iii) независимом анализе. Уровень формализации применения этих трех направлений в каждом случае зависит от особенностей, размеров и сложности организационной структуры банка, а также уровня и видов рисков, присущих его деятельности. Однако во всех случаях подразделение по управлению операционным риском банка должно быть полностью интегрировано в общую систему управления рисками банка.

Верификация Системы управления проводится периодически, как правило, внутренними и/или внешними аудиторами банка, но в ней могут участвовать и другие независимые внешние стороны, обладающие необходимой квалификацией. Верификация позволяет проверять эффективность всей Системы управления, ее соответствие принципам, одобренным советом

директоров, а также процессы подтверждения правильности на предмет обеспечения их независимости и реализации в соответствии с утвержденной политикой банка.

В соответствии с Письмом 76-Т «В целях создания условий для эффективного управления операционным риском кредитной организации рекомендуется учредительными и (или) внутренними документами отнести к компетенции совета директоров (наблюдательного совета) следующие вопросы:

- -утверждение основных принципов управления операционным риском;
- -создание организационной структуры кредитной организации, соответствующей основным принципам управления операционным риском;
- -осуществление контроля за полнотой и периодичностью проверок службой внутреннего контроля соблюдения основных принципов управления операционным риском отдельными подразделениями и кредитной организацией в целом;
- -утверждение мер по обеспечению непрерывности финансово-хозяйственной деятельности при совершении банковских операций и других сделок, включая планы действий на случай непредвиденных обстоятельств (планы по обеспечению непрерывности и (или) восстановления финансово-хозяйственной деятельности);
- -оценка эффективности управления операционным риском;
- -контроль за деятельностью исполнительных органов кредитной организации по управлению операционным риском.

Учредительными и (или) внутренними документами к компетенции исполнительных органов рекомендуется отнести следующие вопросы:

- -обеспечение принятия внутренних документов, определяющих правила и процедуры управления операционным риском, в целях соблюдения основных принципов управления операционным риском, утвержденным советом директоров (наблюдательным советом);
- -распределение полномочий и ответственности по управлению операционным риском между руководителями подразделений различных уровней, обеспечение их необходимыми ресурсами, установление порядка взаимодействия и представления отчетности».

В целом рекомендации Банка России по организации структуры управления операционными рисками совпадает с рекомендациями Базельского комитета, изложенных в документах «Лучшие практики по управлению и надзору за операционными рисками» (2002-2003гг.) и «Принципы рационального (надлежащего) управления операционным риском» (2011г.).

2.1.3. Основные инструменты системы управления операционным риском

2.1.3.1. Идентификация и оценка рисков. Документирование этапа идентификации рисков/ пересмотра перечня значимых рисков. Качественная оценка рисков. Ведение реестра рисков

Согласно Письму 76-Т идентификация (выявление) и оценка операционных рисков является составной частью управления операционным риском наряду с мониторингом, контролем и (или) минимизацией операционного риска.

Письмо 69-Т фиксирует, что выявление и оценка риска являются основополагающими атрибутами эффективной системы управления операционным риском. Согласно данному документу, для эффективного выявления рисков необходимо учитывать как внутренние (организационную структуру банка, качество его кадровых ресурсов и т.п.), так и внешние (изменения условий для осуществления деятельности, внедрение технологических нововведений в отрасли) факторы.

Согласно Письму 76-Т, выявление операционного риска предполагает анализ всех условий функционирования кредитной организации на предмет наличия или возможности возникновения факторов операционного риска, который рекомендуется проводить на нескольких уровнях:

- анализ изменений в финансовой сфере, которые могут оказать влияние на эффективность деятельности кредитной организации;

- анализ подверженности операционному риску направлений деятельности
- (составление так называемого "риск-профиля" банка);
- анализ отдельных банковских операций и других сделок;
- анализ внутренних процедур, включая систему отчетности и обмена информацией.

Выявление операционных рисков связывается с выявлением и учетом источников операционного риска. Так, согласно Письму 96-Т кредитным организациям, использующим АМА-подход, рекомендуется регулярно пересматривать существующие внутренние процессы и процедуры, используемые информационно-технологические системы с целью выявления не учтенных ранее источников операционного риска. Периодичность их пересмотра рекомендуется определить во внутренних документах кредитной организации.

Значимая роль в процессах выявления операционных рисков отводится Исполнительному органу Банка. Так, в Письме 96-Т закрепляется принцип, согласно которому Исполнительный орган Банка обеспечивает выявление и оценку операционного риска, присущего всем существенным продуктам, направлениям деятельности, процессам и системам, с целью четкого понимания природы этих рисков и стимулов, создающих предпосылки для их (рисков) возникновения.

Важная роль в выявлении операционных рисков также принадлежит бизнес-линиям. Согласно Письму 69-Т, «в банковской практике первой "линией обороны" является управление направлениями деятельности (бизнес-линиями). Это означает, что надлежащая практика управления операционным риском исходит из того, что управление по направлениям деятельности помогает выявлять и управлять рисками, присущими определенным банковским продуктам, процессам и системам, относящимся к этим направлениям».

Особую важность идентификация и оценка рисков имеет для новых продуктов и направлений деятельности Банка. Так, согласно Письму 69-Т исполнительный орган должен обеспечить наличие процесса одобрения всех новых продуктов, направлений деятельности, процедур и систем, который бы учитывал подверженность операционному риску. Кроме того, банк должен обеспечивать, чтобы инфраструктура управления риском соответствовала новшествам и не отставала от темпов роста или изменений продуктов, видов деятельности, процессов и систем.

Следует отметить, что согласно Письму 69-Т документация Системы управления должна описывать выявление и оценку операционных рисков в т.ч. в следующей части:

- предусматривать проведение надлежащего независимого анализа и оценки опер. риска
- содержать описание способов и методов оценки риска;
- предусматривать единую систему используемой терминологии, относящейся к операционному риску, для обеспечения точности при выявлении риска, классификации подверженности риску и определении целей в области управления риском

К примерам методов, которые могут использоваться для выявления и оценки операционного риска, Письмо 69-Т относит:

- Аудиторские заключения.
- Сбор и анализ данных об убытках кредитной организации.
- Сбор и анализ внешних данных.
- Самооценку риска, в процессе которой банк оценивает процессы, лежащие в основе его операций, путем сопоставления с перечнем потенциальных угроз и трудностей и рассматривает их потенциальные последствия. В рамках подхода, как правило, оцениваются присущий риск (риск до учета средств контроля), эффективность системы контроля и остаточный риск (риск после учета средств контроля).
- Классификация бизнес-процессов.
- Индикаторы уровня рисков и показатели эффективности.
- Сценарный анализ.
- Измерение риска;

- Сравнительный анализ. Сравнительный анализ включает сравнение результатов применения различных методов оценки для получения более полного представления об уровне и видах операционного риска банка.

Оценка операционного риска, согласно Письму 76-Т, предполагает оценку вероятности наступления событий или обстоятельств, приводящих к операционным убыткам, и оценку размера потенциальных убытков. В соответствии с Письмом 76-Т, кредитные организации могут разрабатывать методы оценки операционного риска самостоятельно либо использовать методы, принятые в международной банковской практике:

- статистический анализ распределения фактических убытков (позволяют сделать прогноз потенциальных операционных убытков);
- балльно-весовой метод (метод оценочных карт, сущность метода заключается в оценке операционного риска в сопоставлении с мерами по его минимизации);
- моделирование (сценарный анализ).

2.1.4. Документирование этапа идентификации рисков / пересмотра перечня значимых рисков

Согласно Письму 76-Т:

«Кредитным организациям рекомендуется на регулярной основе пересматривать существующие внутренние процессы и процедуры, используемые информационно-технологические системы с целью выявления не учтенных ранее источников операционного риска.

Периодичность пересмотра рекомендуется определить во внутренних документах кредитной организации».

2.1.4.1. Сбор данных о потерях

В Письме 76-Т в пункте 3.5 идет речь о необходимости ведения аналитической базы данных о понесенных операционных убытках: «В целях обеспечения условий для эффективного выявления операционного риска, а также его оценки рекомендуется создать и вести аналитическую базу данных о понесенных операционных убытках, в которой отражать сведения об их видах и размерах в разрезе направлений деятельности, отдельных банковских операций и других сделок, обстоятельств их возникновения и выявлении.»

Порядок ведения аналитической базы данных о понесенных операционных убытках, форму представления и требования к содержанию вводимой информации рекомендуется установить во внутренних документах кредитной организации»

В пункте 3.6 данного письма идет речь о необходимости ведения базы внешних потерь: «Кредитным организациям рекомендуется наряду с ведением аналитической базы данных о понесенных операционных убытках на постоянной основе с использованием различных источников собирать и анализировать информацию о случаях операционных убытков в других кредитных и финансовых организациях».

В Письме 96-Т в пункте 3.6 также отмечены рекомендации ведения внутренних и внешних баз понесенных убытков:

«Кредитной организации рекомендуется создать и систематически отслеживать аналитическую базу данных о понесенных операционных убытках. Важно обеспечить, чтобы аналитическая база данных о понесенных операционных убытках была всеобъемлющей, то есть учитывала все существенные события и риски по направлениям деятельности (подразделениям), отдельным операциям (сделкам), и содержала в том числе информацию о видах и размерах, датах понесения (возмещения) операционных убытков в разрезе направлений деятельности, отдельных операций (сделок), обстоятельств их возникновения и выявления. Целесообразно также, чтобы аналитическая база данных о понесенных операционных убытках позволяла распределять убытки по бизнес-линиям и типам событий в соответствии с установленными во внутренних документах

кредитной организации критериями. Порядок ведения аналитической базы данных о понесенных операционных убытках, форму представления и требования к содержанию вводимой информации, порог размера убытков, информация о которых подлежит помещению в указанную базу данных, целесообразно установить во внутренних документах кредитной организации.»

2.1.4.2. Контрольная среда. Самооценка рисков и контролей (RCSA)

В соответствии с Письмом 69-Т:

«Оценка риска. В процессе оценки риска, которую часто называют Самооценкой риска (СОР), банк оценивает процессы, лежащие в основе его операций, путем сопоставления с перечнем потенциальных угроз и трудностей и рассматривает их потенциальные последствия. Подобный подход используется в процессе Самооценки контроля над рисками (СОКР), в рамках которого, как правило, оцениваются внутренний риск, присущий деятельности банка (риск до учета средств контроля), эффективность системы контроля и остаточный риск (риск после учета средств контроля). Система показателей, основанная на СОКР и учитывающая остаточные риски, направлена на использование результатов СОКР для построения параметров оценки контрольной среды»

2.1.4.3. Ключевые индикаторы риска (KRIs) и ключевые индикаторы контроля (KCI)

Письмо 76-Т определяет КИР как важнейший инструмент мониторинга операционных рисков, а также вводит понятие лимитов (пороговых уровней) КИР: «В целях предупреждения возможности превышения уровня операционного риска над его предельным уровнем, установленным во внутренних документах кредитной организации, кредитной организации рекомендуется осуществлять его регулярный мониторинг. Периодичность осуществления мониторинга операционного риска определяется кредитной организацией самостоятельно исходя из степени его существенности для соответствующего направления деятельности, внутренних процедур управления операционным риском или возможностей информационно-технологической системы. В целях мониторинга операционного риска рекомендуется создание системы индикаторов уровня операционного риска - показателей или параметров, которые могут быть связаны с уровнем операционного риска, принимаемого кредитной организацией.

В отношении каждого индикатора уровня операционного риска кредитной организации рекомендуется установить лимиты (пороговые значения), обеспечивающие выявление значимых для кредитной организации операционных рисков и своевременное адекватное воздействие на них, а также установить периодичность пересмотра системы индикаторов уровня операционного риска».

Письмом 76-Т также определены примеры КИР: « В качестве индикаторов уровня операционного риска могут быть использованы сведения о количестве несостоявшихся или незавершенных банковских операций и других сделок, увеличении их частоты и (или) объемов, текучести кадров, частоте допускаемых ошибок и нарушений, времени (продолжительности) простоя информационно-технологических систем и других показателях».

Понятие ключевых индикаторов риска также раскрывается в Письме 69-Т: «Индикаторы уровня рисков и показатели эффективности представляют собой значения (величины) и/или статистические данные, дающие представление о рисках, которым подвержен банк. Индикаторы уровня риска используются для контроля основных факторов, связанных с возникновением наиболее значимых рисков.»

В этой связи показательно, что упоминаемые в Письме 76-Т лимиты КИР могут быть интерпретированы в т.ч. как «лимиты начального риска и остаточного риска», пределы или лимиты для отдельных операционных рисков и т.о. стать важной частью риск-аппетита и допустимого уровня риска, о которых говорит Письмо 69-Т: «При установлении и анализе риск-аппетита и допустимого уровня риска совет директоров должен учитывать все существенные риски, допустимый уровень риска, текущее финансовое состояние банка и стратегическое направление развития деятельности банка. Риск-аппетит и допустимый уровень риска должны

учитывать аппетит к различным операционным рискам банка и обеспечивать их сопоставимость. Совет директоров должен утверждать соответствующие пределы или лимиты для отдельных операционных рисков, а также общий риск-аппетит и допустимый уровень риска. Совет директоров должен регулярно анализировать (пересматривать) установленные лимиты и общий уровень риск-аппетита и допустимый уровень риска. В процессе анализа (пересмотра) должны учитываться изменения внешних факторов, существенное увеличение объема деловых операций, в том числе по отдельным видам деятельности, качество системы контроля, эффективность стратегий управления риском или снижения риска, объем понесенных убытков, а также частота, масштабы и характер нарушений установленных лимитов. Совет директоров должен контролировать соблюдение исполнительным органом установленного уровня риск-аппетита и допустимого уровня риска и обеспечивать своевременное выявление и устранение нарушений».

«Индикаторы уровня рисков и показатели эффективности часто используются с эскалационными показателями (показателями обострения, увеличения масштабов) для того, чтобы предупредить момент, когда уровень риска приблизится или станет выше пределов или лимитов, и помочь в подготовке планов по снижению уровня риска».

2.1.4.4. Ключевые показатели эффективности управления операционным риском (КПЭ/KPIs)

Согласно Письму 69-Т «Показатели эффективности, которые часто называют Ключевыми показателями эффективности (КПЭ), позволяют понять состояние операционных процессов, что, в свою очередь, обеспечивает выявление недостатков, сбоев и потенциальных убытков.

В соответствии Положением ЦБ РФ от 16 декабря 2003 г. N 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах», далее Положение 242-П, «Службой внутреннего контроля осуществляется контроль за эффективностью принятых подразделениями и органами управления по результатам проверок мер, обеспечивающих снижение уровня выявленных рисков, или документирование принятия руководством подразделения и (или) органами управления решения о приемлемости выявленных рисков для кредитной организации».

Письмо 76-Т определяет, что «Кредитным организациям рекомендуется определить порядок осуществления контроля за эффективностью управления операционным риском.

Во внутренних документах рекомендуется установить: систему оценки эффективности управления операционным риском.

В целях контроля за эффективностью управления операционным риском целесообразно по мере необходимости пересматривать основные принципы управления операционным риском на основе анализа:

- достигнутого уровня управления операционным риском в кредитной организации;
- международного опыта и опыта российских кредитных организаций в области управления операционным риском;
- изменений, происходящих на финансовых рынках;
- других внешних и внутренних факторов, которые могут оказать влияние на показатели деятельности кредитной организации».

2.1.4.5. Сценарный анализ и стресс-тестирование

В нормативно-правовых актах Банка России понятие сценарного анализа операционного риска раскрывается в Письме 76-Т, при этом сценарный анализ рассматривается как элемент оценки операционного риска методом моделирования: «В рамках метода моделирования (сценарного анализа) на основе экспертного анализа для направлений деятельности кредитной организации, отдельных видов банковских операций и других сделок определяются возможные сценарии возникновения событий или обстоятельств, приводящих к операционным убыткам, и разрабатывается модель распределения частоты возникновения и размеров убытков, которая затем используется для оценки операционного риска».

Также понятие сценарного анализа раскрывается в Письме 69-Т: «Сценарный анализ представляет собой процесс получения экспертного заключения руководителей по направлениям деятельности и риск менеджеров для выявления потенциальных случаев возникновения операционного риска и оценки их возможных последствий. Сценарный анализ является эффективным средством изучения потенциальных источников существенного операционного риска и потребности в дополнительных средствах контроля или снижения риска. Учитывая субъективность процесса сценарного анализа, для обеспечения его непротиворечивости и последовательности необходима надежная система управления».

Подходы и рекомендации Банка России к стресс-тестированию операционного риска применительно ко всем основным видам банковских рисков, включая операционный риск, отражены в документе «Подходы к организации стресс-тестирования в кредитных организациях (на основе обзора международной финансовой практики)», а также в Письме 96-Т. Рекомендации последнего документа состоят в основном в необходимости определения методологии стресс-тестирования:

- «Кредитным организациям рекомендуется разработать процедуры проведения стресс-тестирования и определить в них:
- - типы стресс-тестирования и основные задачи, решаемые в процессе стресс-тестирования;
- - частоту проведения стресс-тестирования в зависимости от типов стресс-тестов и решаемых с их помощью задач;
- - методологию определения актуальных сценариев. Рекомендуется применять широкий спектр сценариев, покрывающих различные виды рисков, принимаемых кредитной организацией, в том числе и ряд самых тяжелых сценариев, включая события, которые могут причинить максимальный ущерб кредитной организации или повлечь потерю деловой репутации;
- - возможные корректирующие действия в стрессовых ситуациях.

Правила и процедуры проведения стресс-тестирования рекомендуется зафиксировать во внутренних документах кредитной организации и периодически пересматривать в зависимости от изменения внешних и внутренних факторов ее деятельности»

2.1.4.6. Планирование непрерывности и восстановления бизнеса

В банке должна осуществляться деятельность по обеспечению непрерывности и восстановления бизнеса согласно требований Приложения 5 Положения 242-П.

2.1.4.7. Тестирование контрольных процедур и влияние на остаточный риск

В соответствии с Письмом 76-Т: «Кредитным организациям рекомендуется на регулярной основе пересматривать существующие внутренние процессы и процедуры, используемые информационно-технологические системы с целью выявления не учтенных ранее источников операционного риска.

Периодичность пересмотра рекомендуется определить во внутренних документах кредитной организации».

2.1.4.8. Система отчетности по операционным рискам

Рекомендации относительно системы отчетности по операционным рискам содержатся в Письме 76-Т, Письме 69-Т, Письме 96-Т, Положении 242-П, в Положении ЦБ РФ от 3 ноября 2009 г. N 346-П «Положение о порядке расчета размера операционного риска», далее Положение 346-П, и Письме от 23 марта 2007 г. N 26-Т «О Методических рекомендациях по проведению проверки системы управления банковскими рисками в кредитной организации (ее филиале)», далее Письмо 26-Т.

2.1.4.9. Виды отчетности

Письмо 76-Т дает рекомендации по организации управления операционным риском в кредитных организациях, в том числе по организации системы отчетности по опер. рискам:

«Основные принципы управления операционным риском должны включать в себя в т.ч. порядок предоставления отчетности и обмена информацией по вопросам управления операционным риском.…Основные принципы управления операционным риском рекомендуется реализовывать во внутренних документах кредитной организации, определяющих:…порядок разработки и предоставления отчетности и иной информации. Выявление операционного риска предполагает анализ всех условий функционирования кредитной организации на предмет наличия или возможности возникновения факторов операционного риска, который рекомендуется проводить на нескольких уровнях:… в том числе, анализ внутренних процедур, включая систему отчетности и обмена информацией».

Положение 346-П регламентирует расчет размера операционного риска и предоставление отчетности.

Письмо 26-Т дает рекомендации по подготовке Кредитной организацией необходимой информации/отчетности для достижения целей проверки системы управления рисками, в том числе операционными, уполномоченными представителями Банка России.

В Письме 96-Т описаны основные принципы формирования отчетности в рамках ВПОДК (Внутренние процедуры оценки достаточности капитала) в части рекомендуемого формата, содержания и периодичности:

Состав и периодичность предоставления отчетов по операционному риску высшему топ-менеджменту и органам управления Банка регулируется внутренними документами и зависит от масштаба деятельности и профиля операционного риска.

«В регулярные отчеты для исполнительного органа и совета директоров следует включать результаты мониторинга, а также оценки Системы управления, проведенные подразделениями внутреннего аудита и/или управления риском. Отчеты, подготовленные надзорными органами (и/или для надзорных органов), должны доводиться до сведения исполнительного органа и совета директоров, когда это необходимо».

2.1.4.10. Исполнители

«Независимая корпоративная функция управления операционным риском (ФУОР) <*>, как правило, является второй "линией обороны", дополняющей меры по управлению направлениями деятельности. … В обязанности указанной структуры могут входить оценка риска и отчетности, организация деятельности комитетов по риску и представление отчетности совету директоров. Одной из главных функций ФУОР является проверка исходных данных и результатов работы системы управления рисками по видам деятельности, а также систем оценки риска и отчетности...»

«Принцип 8: Исполнительный орган должен организовать процесс регулярного мониторинга уровня и природы операционного риска и вероятности возникновения существенных убытков. На уровне совета директоров, исполнительного органа и на уровне осуществления различных направлений деятельности должны применяться механизмы представления отчетности, позволяющие осуществлять упреждающее управление операционным риском.»

2.1.4.11. Адресаты отчетности

Согласно 96-Т «Рекомендуется, чтобы внутренняя отчетность кредитной организации по операционному риску регулярно представлялась руководителям подразделений, единоличному и коллегиальному исполнительным органам и совету директоров (наблюдательному совету). Кредитной организации целесообразно также установить процедуру принятия мер по снижению операционного риска на основании информации, содержащейся во внутренней отчетности по операционному риску.»

«Кредитной организации рекомендуется доводить до участников (акционеров), кредиторов, вкладчиков и иных клиентов, внешних аудиторов, рейтинговых агентств и других заинтересованных лиц (в том числе в составе годового отчета) информацию по управлению операционным риском, обеспечив при этом соответствие степени детализации раскрываемой информации характеру и масштабам деятельности кредитной организации».

Письмо 69-Т дает следующие рекомендации касательно системы отчетности по операционным рискам: «для получения надзорными органами актуальной информации об операционном риске они могут создавать механизмы представления банками отчетности напрямую и внешними аудиторами (например, обязательное представление надзорным органам внутренних отчетов банков об управлении операционным риском.»

2.1.4.12. Периодичность отчетности

Из 69-Т: «Отчетность должна быть своевременной, и банк должен иметь возможность подготовить отчеты как в нормальной ситуации, так и в условиях стресса на рынке. Периодичность отчетности должна отражать степень подверженности банка рискам, а также темпы и характер изменений в его деятельности».

Согласно 96-Т: «Отчетность по операционному риску формируется на ежегодной основе. Например, развернутый отчет о результатах ВПОДК для представления органам управления кредитной организации, как и отчетность Банку России о внутренней оценке достаточности капитала, может формироваться ежегодно. Для отчетов по рискам и о соблюдении подразделениями кредитной организации установленных лимитов, используемых в целях принятия бизнес-решений, целесообразно устанавливать более частую периодичность (вплоть до ежедневной).»

2.1.4.13. Минимальные требования к содержанию отчетности

Согласно 69-Т «…Управление рисками включает в себя процесс выявления рисков, которым подвергается банк, оценки этих рисков (когда это возможно), обеспечения наличия программы планирования и мониторинга капитала, постоянного мониторинга рисков и соответствующих потребностей в капитале, принятия мер по контролю или уменьшению рисков, а также представления отчетности о рисках и состоянии капитала банка совету директоров и исполнительному органу банка. Процедуры внутреннего контроля, как правило, применяются ежедневно в ходе оперативной деятельности банка и призваны по возможности обеспечивать эффективность деятельности банка, надежность, своевременность и полноту полученной информации и соблюдение банком действующих законодательных и нормативных актов.

Отчеты об операционном риске могут содержать внутренние финансовые и операционные показатели, показатели соблюдения действующих правил, а также внешнюю информацию, в том числе о рынке и о событиях и условиях, существенных для принятия решений. Отчеты об операционном риске должны включать:

(а) информацию о нарушениях установленного риск-аппетита и допустимого уровня риска, а также пределов или лимитов, установленных банком;

(б) сведения о последних существенных случаях внутреннего возникновения операционного риска и убытков;

(в) сведения о существенных внешних событиях и их потенциальных последствиях для банка и капитала, предназначенного для покрытия операционного риска.»

Также согласно 96-Т «Кредитной организации рекомендуется формировать внутреннюю отчетность в рамках ВПОДК (далее - отчетность ВПОДК) на базе информационной системы. Информация о результатах внутренней оценки достаточности капитала кредитной организации представлена форма отчета о результатах внутренней оценки, которая включает порядок составления и представления информации, в том числе и по операционному риску.»

В отчетность по операционному риску рекомендуется включать информацию о:

- существенных операционных рисках и статусе исполнения мероприятий по управлению ими;
- реализовавшихся в течение отчетного периода значимых рисковых событиях и понесенных потерях;
- КИР, сигнализирующих о превышении приемлемого уровня риска;
- Результатах оценки операционного риска по Банку в целом;
- Результатах стресс-тестирования операционного риска».

В отчетность ВПОДК рекомендуется включать, как минимум, следующую информацию:

- - об агрегированном объеме рисков, принятых кредитной организацией, а также о принятых объемах каждого существенного для кредитной организации вида риска;
- - об уровнях рисков, принятых отдельными подразделениями кредитной организации;
- - о размере ВК и использовании подразделениями кредитной организации выделенных им лимитов ВК;
- - о фактах нарушения подразделениями кредитной организации установленных лимитов, а также предпринимаемых мерах по урегулированию выявленных нарушений;
- - о результатах стресс-тестирования;
- - о текущей внутренней оценке достаточности капитала

2.1.5. Классификация операционных рисков

Классификация событий операционного риска по видам деятельности предусмотрена в Базеле II и адаптирована на русском языке в Приложении к Рекомендациям Письма 76-Т.

2.1.5.1. Классификация событий операционного риска по видам

Письмом Департамента банковского регулирования и надзора от 28 апреля 2009 г.

N 15-2-1-9/2644 «О подходе к расчету регулятивного капитала, минимально необходимого для покрытия операционного риска, основанном на внутренних оценках кредитных организаций», далее Письмо 15-2-1-9/2644, вводится требование, чтобы используемая классификация событий операционного риска была совместима с предусмотренной Базелем II классификацией видов событий операционного риска. При этом классифицируемые события операционного риска должны быть отнесены к одной из следующих категорий (Рекомендации Письма 15-1-2-9/2644): внутреннее мошенничество (Internal Fraud); внешнее мошенничество (External Fraud); трудовые конфликты (Employment Practices and Workplace Safety); клиенты, продукты и практика ведения бизнеса (Clients, Products & Business Practices); материальный ущерб имуществу (Damage to Physical Assets); прерывание деятельности (Business Disruption and System Failures); исполнение, поставки и управление процессами (Execution, Delivery & Process Management).

Процедуры классификации и учета событий операционного риска должны закрепляться в документе, регламентирующем порядок классификации и учета рисковых событий в базе данных.

Справочник классификации по типу рискового события может поддерживать многоуровневую классификацию, детализированную от уровня к уровню.

2.1.5.2. Классификация направлений деятельности

В Приложении Письма 76-Т рекомендуется применять следующую классификацию направлений деятельности: «в соответствии с указанными источниками для классификации выделяется восемь направлений банковской деятельности, подверженной операционному риску:

1) банковское обслуживание физических лиц:

2) банковское обслуживание юридических лиц:

3) осуществление платежей и расчетов (кроме платежей и расчетов, осуществляемых в рамках обслуживания своих клиентов):

4) агентские услуги:

5) операции и сделки на рынке ценных бумаг и срочных финансовых инструментов:

6) оказание банковских услуг корпоративным клиентам, органам государственной власти и местного самоуправления на рынке капиталов:

7) управление активами:

8) брокерская деятельность

Классификация рисковых событий по направлениям деятельности осуществляется в соответствии с внутренними направлениями деятельности кредитной организации. Возможно применение многоуровневой классификации, детализированной от уровня к уровню. Первый уровень внутренних направлений деятельности должен быть соотнесен (мэппинг) бизнес-линиям Базеля II – Приложение 2.

Классификация рискового события осуществляется последовательно от первого уровня к последующему.»

2.1.5.3. Требования по зрелости процессов и инструментов управления операционным риском для Базового индикативного, Стандартизированного и Усовершенствованного подходов

Из 69-Т: «Общепринятая банковская практика надлежащего управления операционным риском нередко основана на трех направлениях "линиях обороны" - (i) управлении направлениями деятельности, (ii) независимой корпоративной функции управления операционным риском и (iii) независимом анализе <*>. Уровень формализации применения этих трех направлений в каждом случае зависит от особенностей, размеров и сложности организационной структуры банка, а также уровня и видов рисков, присущих его деятельности. Однако во всех случаях подразделение по управлению операционным риском банка должно быть полностью интегрировано в общую систему управления рисками банка… Поскольку управление операционным риском эволюционирует, а условия коммерческой деятельности постоянно меняются, исполнительный орган должен следить, чтобы принципы, процессы и Системы управления оставались достаточно надежными. Совершенствование управления операционным риском будет зависеть от того, в какой степени учитывается мнение лиц, ответственных за управление операционным риском, а также от готовности исполнительного органа своевременно принимать надлежащие меры на основе этого мнения.»

В целях оценки требований к собственным средствам (капиталу) в отношении операционного риска кредитная организация может использовать наряду с базовым индикативным подходом к оценке операционного риска, применение которого определено в Положении Банка России от 03.11.2009 N 346-П "О порядке расчета размера операционного риска", также и внутренние модели, принятые в международной банковской практике, например, базовый индикативный подход (Basic Indicative Approach), стандартизированный подход (Standardized Approach) и "продвинутый" подход (Advanced Measurement Approach (AMA), рекомендованные Базелем II.

Кредитным организациям, применяющим **базовый индикативный подход**, рекомендуется разработать и зафиксировать во внутренних документах критерии распределения валового дохода по текущим бизнес-линиям. Кредитной организации важно обеспечивать по мере появления новых или изменения прежних видов деятельности кредитной организации своевременную корректировку данных критериев.

Кредитными организациями, применяющими **стандартизированный подход** (Standardized Approach) к оценке операционного риска, приводится информация о критериях распределения валового дохода по текущим бизнес-линиям. Кредитные организации, использующие AMA-

подход, приводят результаты бэк-тестинга модели (сопоставления прогнозных оценок с размерами понесенных операционных убытков, имевших место за соответствующий период), а также результаты анализа причин полученных расхождений и описание изменений, внесенных в методологию оценки по результатам такого анализа.»

2.2. Позиция Европейских регуляторов

2.2.1. Определение операционного риска (включая взаимосвязь со смежными видами рисков)

Основополагающий документ Базельского комитета (International Convergence of Capital Measurement and Capital Standards) дает следующее определение операционного риска, включая правовой, но исключая репутационный и стратегический виды рисков:

644. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk,97 but excludes strategic and reputational risk.

Т.е. определение Банка России полностью соответствует определению операционного риска.

Директива о требованиях к капиталу Европейского парламента и Совета (Capital Requirements Directive (CRD) дает аналогичное определение операционного риска:

‘operational risk’ means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, and includes legal risk. Также допускает operational risks that can be associated with CCR (Counterparty Credit Risk (CCR)’ means the risk that the counterparty to a transaction could default before the final settlement of the transaction's cash flows.

2.2.2. Структура управления операционным риском

Основополагающий документ Базельского комитета (International Convergence of Capital Measurement and Capital Standards) определяет следующую структуру управления операционным риском:

The framework outlined below presents three methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity: (i) the Basic Indicator Approach; (ii) the Standardised Approach; and (iii) Advanced Measurement Approaches (AMA).

646. Banks are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices. Qualifying criteria for the Standardised Approach and AMA are presented below. 647. Internationally active banks and banks with significant operational risk exposures (for example, specialised processing banks) are expected to use an approach that is more sophisticated than the Basic Indicator Approach and that is appropriate for the risk profile of the institution.98 A bank will be permitted to use the Basic Indicator or Standardised Approach for some parts of its operations and an AMA for others provided certain minimum criteria are met, see paragraphs 680 to 683. 648. A bank will not be allowed to choose to revert to a simpler approach once it has been approved for a more advanced approach without supervisory approval.

Директива о требованиях к капиталу Европейского парламента и Совета (Capital Requirements Directive (CRD) прописывает Credit institutions must meet the qualifying criteria listed below, in addition to the general risk management standards set out in Article 22 and Annex V. Satisfaction of these criteria shall be determined having regard to the size and scale of activities of the credit institution and to the principle of proportionality. (a) Credit institutions shall have a well-documented assessment and management system for operational risk with clear responsibilities assigned for this system. They shall identify their exposures to operational risk and track relevant operational risk data, including material loss data. This system shall be subject to regular independent review. (b) The operational risk assessment system must be closely integrated into the risk management processes of the credit institution. Its output must be an integral Part of the process of monitoring and controlling the credit institution's operational risk profile. (c) Credit institutions shall implement a system of

management reporting that provides operational risk reports to relevant functions within the credit institution. Credit institutions shall have procedures for taking appropriate action

2.2.3. Основные инструменты системы управления операционным риском, включая

2.2.3.1. Идентификация и оценка рисков. Документирование этапа идентификации рисков / пересмотра перечня значимых рисков. Качественная оценка рисков. Ведение реестра рисков. Идентификация и оценка рисков. Документирование этапа идентификации рисков / пересмотра перечня значимых рисков. Качественная оценка рисков. Ведение реестра рисков

Основополагающий документ Базельского комитета (International Convergence of Capital Measurement and Capital Standards) дополняет требования Банка России по вопросам выявления и оценки операционного риска в следующей части:

- устанавливает дополнительные требования к процессу управления и оценки операционных рисков для использования стандартизованного подхода (в части требований валидации и независимой проверки процессов управления и оценки операционных рисков): « The bank's operational risk management processes and assessment system must be subject to validation and regular independent review. These reviews must include both the activities of the business units and of the operational risk management function. The bank's operational risk assessment system (including the internal validation processes) must be subject to regular review by external auditors and/or supervisors.»
- устанавливает дополнительные требования к процессу управления и оценки операционных рисков для использования AMA-подхода (в части требований к интеграции системы оценки операционных рисков в непрерывный процесс мониторинга и управления профилем операционного риска Банка, а также требований к валидации и независимой проверке процессов управления и оценки операционных рисков): «The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, internal capital allocation, and risk analysis. The bank must have techniques for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the firm.»

2.2.3.2. Сбор данных о потерях

В отношении сбора данных о внутренних события операционного риска Basel II предписывает следующее:

Internal data

670. Banks must track internal loss data according to the criteria set out in this section. The tracking of internal loss event data is an essential prerequisite to the development and functioning of a credible operational risk measurement system. Internal loss data is crucial for tying a bank's risk estimates to its actual loss experience. This can be achieved in a number of ways, including using internal loss data as the foundation of empirical riskestimates, as a means of validating the inputs and outputs of the bank's risk measurement system, or as the link between loss experience and risk management and control decisions.

671. Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and risk management procedures. Therefore, a bank must have documented procedures for assessing the on-going relevance of historical loss data, including those situations in which judgement overrides, scaling, or other adjustments may be used, to what extent they may be used and who is authorised to make such decisions.

672. Internally generated operational risk measures used for regulatory capital purposes must be based on a minimum five-year observation period of internal loss data, whether the internal loss data is

used directly to build the loss measure or to validate it. When the bank first moves to the AMA, a three-year historical data window is acceptable.

В отношении внешних данных следующее:

674. A bank's operational risk measurement system must use relevant external data (either public data and/or pooled industry data), especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, losses. These external data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events,

109 This applies to all banks, including those that may only now be designing their credit risk and operational risk databases.

154 or other information that would help in assessing the relevance of the loss event for other banks. A bank must have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (e.g. scaling, qualitative adjustments, or informing the development of improved scenario analysis). The conditions and practices for external data use must be regularly reviewed, documented, and subject to periodic independent review.

CRD в отношении внутренних данных указывает:

13. Internally generated operational risk measures shall be based on a minimum historical observation period of five years. When a credit institution first moves to an Advanced Measurement Approach, a three-year historical observation period is acceptable.

В отношении внешних данных:

The credit institution's operational risk measurement system shall use relevant external data, especially when there is reason to believe that the credit institution is exposed to infrequent, yet

- potentially severe, losses. A credit institution must have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate
- the data in its measurement system. The conditions and practices for external data use must be regularly reviewed, documented and subject to periodic independent review.

2.2.3.3. Контрольная среда. Самооценка рисков и контролей

Основополагающий документ Базельского комитета (International Convergence of Capital Measurement and Capital Standards) дополняет требования Банка России по вопросам самооценки рисков и контролей:

Business environment and internal control factors

676. In addition to using loss data, whether actual or scenario-based, a bank's firm-wide risk assessment methodology must capture key business environment and internal control factors that can change its operational risk profile. These factors will make a bank's risk assessments more forward-looking, more directly reflect the quality of the bank's control and operating environments, help align capital assessments with risk management objectives, and recognise both improvements and deterioration in operational risk profiles in a more immediate fashion. To qualify for regulatory capital purposes, the use of these factors in a bank's risk measurement framework must meet the following standards: The choice of each factor needs to be justified as a meaningful driver of risk, based on experience and involving the expert judgment of the affected business areas. Whenever possible, the factors should be translatable into quantitative measures that lend themselves to verification. The sensitivity of a bank's risk estimates to changes in the factors and the relative weighting of the various factors need to be well reasoned. In addition to capturing changes in risk due to improvements in risk controls, the framework must also capture potential increases in risk due to greater complexity of activities or increased business volume. The framework and each instance of its application, including the supporting rationale for any adjustments to empirical estimates, must be documented and subject to independent review within the bank and by supervisors. Over time, the process and the outcomes need to

be validated through comparison to actual internal loss experience, relevant external data, and appropriate adjustments made.

Аналогичные критерии указаны в CRD:

Business environment and internal control factors 21. The credit institution's firm-wide risk assessment methodology

must capture key business environment and internal control factors that can change its operational risk profile. 22. The choice of each factor needs to be justified as a meaningful driver of risk, based on experience and involving the expert judgment of the affected business areas. 23. The sensitivity of risk estimates to changes in the factors and the relative weighting of the various factors need to be well reasoned. In addition to capturing changes in risk due to improvements in risk controls, the framework must also capture potential increases in risk due to greater complexity of activities or increased business volume.

24. This framework must be documented and subject to independent review within the credit institution and by competent authorities. Over time, the process and the outcomes need to be validated and re-assessed through comparison to actual internal loss experience and relevant external data.

2.2.3.4. Сценарный анализ и стресс-тестирование

Основополагающий документ Базельского комитета (International Convergence of Capital Measurement and Capital Standards) раскрывает предназначение, порядок проведения и требования к сценарному анализу.

Основное предназначение сценарного анализа – согласно данному документу - совместно с внешними данными служить для определения влияния на банк событий с высокой тяжестью. Данный подход основывается на знаниях и опыте руководителей бизнесис риск-менеджеров и направлен на получение оценки маловероятных, но возможных, и крайне значительных по тяжести потерь. Оценки могут формироваться в т.ч. в виде параметров распределения тяжести потерь: « A bank must use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. This approach draws on the knowledge of experienced business managers and risk management experts to derive reasoned assessments of plausible severe losses. For instance, these expert assessments could be expressed as parameters of an assumed statistical loss distribution. In addition, scenario analysis should be used to assess the impact of deviations from the correlation assumptions embedded in the bank’s operational risk measurement framework, in particular, to evaluate potential losses arising from multiple simultaneous operational risk loss events. Over time, such assessments need to be validated and re-assessed through comparison to actual loss experience to ensure their reasonableness.

В указанном документе также освещается вопрос о месте сценарного анализа в системе управления операционными рисками в целом, а также подчеркивается важность корректного и связного учета сценарного анализа при моделировании, поскольку результаты сценарного анализа в силу экспертной природы получаемых в его результате оценок характеризуются высокой степенью неопределённости.

«Scenario analysis

252. A robust scenario analysis framework is an important element of the ORMF. This scenario process will necessarily be informed by relevant ILD, ED and suitable measures of BEICFs. While there are a variety of integrated scenario approaches, the level of influence of scenario data within these models differs significantly across banks.

253. The scenario process is qualitative by nature and therefore the outputs from a scenario process necessarily contain significant uncertainties. This uncertainty, together with the uncertainty from the other elements, should be reflected in the output of the model producing a range for the capital requirements estimate. Thus, scenario uncertainties provide a mechanism for estimating an appropriate level of conservatism in the choice of the final regulatory capital charge. Because quantifying the

uncertainty arising from scenario biases continues to pose significant challenges, a bank should closely observe the integrity of the modelling process and engage closely with the relevant supervisor.

254. Scenario data provides a forward-looking view of potential operational risk exposures. A robust governance framework surrounding the scenario process is essential to ensure the integrity and consistency of the estimates produced. Supervisors will generally observe the following elements in an established scenario framework:

(a) A clearly defined and repeatable process;

(b) Good quality background preparation of the participants in the scenario generation process;

(c) Qualified and experienced facilitators with consistency in the facilitation process;

(d) The appropriate representatives of the business, subject matter experts and the corporate operational risk management function as participants involved in the process;

(e) A structured process for the selection of data used in developing scenario estimates;

(f) High quality documentation which provides clear reasoning and evidence supporting the scenario output;

(g) A robust independent challenge process and oversight by the corporate operational risk management function to ensure the appropriateness of scenario estimates;

(h) A process that is responsive to changes in both the internal and external environment; and

(i) Mechanisms for mitigating biases inherent in scenario processes. Such biases include anchoring, availability and motivational biases.

2.2.3.5. Планирование непрерывности и восстановления бизнеса

Business Resiliency and Continuity (стр 17)

Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

59. A bank should periodically review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Training and awareness programmes should be implemented to ensure that staff can effectively execute contingency plans. Plans should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in disaster recovery and business continuity testing with key service providers. Results of formal testing activity should be reported to management and the board.

2.2.3.6. Система отчетности по операционным рискам

European Banking Authority (EBA):
Позиция EBA отражена в разделе Supervisory-Reporting/ COREP на сайте:
http://www.eba.europa.eu/Supervisory-Reporting/COREP.aspx
COREP:

To achieve a high level of harmonization and strong convergence in regular supervisory reporting requirements, the Committee of European Banking Supervisors issued guidelines on prudential reporting with the aim of developing a supervisory reporting framework based on common formats. The Guidelines on Common Reporting cover consolidated, sub-consolidated and solo reporting of the capital requirements and own funds based on amended Directives 2006/48/EC and 2006/49/EC.

The original Guidelines on COREP were first released by CEBS in January 2006 and later amended in January 2010 (COREP rev2) to incorporate CRD II amendments (Directives 2009/27/EC, 2009/83/EC and 2009/111/EC). The latest COREP templates (COREP rev3) have been modified due to CRD III amendments (Directive 2010/76/EU) in view of its application by 31 December 2011."

From 31 December 2012 COREP is expected to become part of EBA's implementing technical standards on reporting."

8. Deficiencies identified during the supervisory review may be addressed through a range of actions. Supervisors use the tools most suited to the particular circumstances of the bank and its

operating environment. In order that supervisors receive current information on operational risk, they may wish to establish reporting mechanisms directly with banks and external auditors (eg internal bank management reports on operational risk could be made routinely available to supervisors).

Principles for the management of operational risk (стр 3, п 11, стр 4, п 15):

11. Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks (where possible), ensuring that an effective capital planning and monitoring program is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board on the bank's risk exposures and capital positions. Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation. In practice, the two notions are in fact closely related and the distinction between both is less important than achieving the objectives of each.

15. A functionally independent corporate operational risk function (CORF)7 is typically the second line of defense, generally complementing the business line's operational risk management activities. The degree of independence of the CORF will differ among banks. For small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the CORF is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities

Monitoring and Reporting (стр 6)

Principle 8: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

Fundamental principles of operational risk management…(стр 7)

Principle 2: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile…

27. Framework documentation should clearly:

(a) identify the governance structures used to manage operational risk, including reporting lines and accountabilities;

(b) describe the risk assessment tools and how they are used;

(c) describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;

(d) describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

(e) establish risk reporting and Management Information Systems (MIS);

(f) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives14;

(g) provide for appropriate independent review and assessment of operational risk; and

(h) require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

Governance

Senior Management (стр.9):

33. Senior management should translate the operational risk management Framework established by the board of directors into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure that the necessary resources are available to manage operational risk in line within the bank's risk appetite and tolerance statement. Moreover, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.

37. A bank's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration:

(a) Committee structure – Sound industry practice for larger and more complex organisations with a central group function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by country, business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board's risk management committee;

Risk Management Environment

Monitoring and Reporting (стр 13-14)

43. Banks are encouraged to continuously improve the quality of operational risk reporting. A bank should ensure that its reports are comprehensive, accurate, consistent and actionable across business lines and products. Reports should be manageable in scope and volume; effective decision-making is impeded by both excessive amounts and paucity of data.

44. Reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions. The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment. The results of monitoring activities should be included in regular management and board reports, as should assessments of the Framework performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory authorities should also be reported internally to senior management and the board, where appropriate.

45. Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making. Operational risk reports should include:

(a) breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;

(b) details of recent significant internal operational risk events and losses; and

(c) relevant external events and any potential impact on the bank and operational risk capital.

46. Data capture and risk reporting processes should be analysed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

Control and Mitigation (стр 14)

Principle 9: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

47. Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control programme consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities.

48. Control processes and procedures should include a system for ensuring compliance with policies. Examples of principle elements of a policy compliance assessment include:

(a) top-level reviews of progress towards stated objectives;

(b) verifying compliance with management controls;

(c) review of the treatment and resolution of instances of non-compliance;

(d) evaluation of the required approvals and authorizations to ensure accountability to an appropriate level of management; and

(e) tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy.

53. Management should ensure the bank has a sound technology infrastructure that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated and comprehensive risk management. Mergers and acquisitions resulting in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine a bank's ability to aggregate and analyse information across risk dimensions or the consolidated enterprise, manage and report risk on a business line or legal entity basis, or oversee and manage risk in periods of high growth. Management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before mergers are consummated, high growth strategies are initiated, or new products are introduced.

Role of Disclosure (стр 18).

Principle 11: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

60. A bank's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations, and evolving industry practice.

61. A bank should disclose its operational risk management framework in a manner that will allow stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.

62. A bank's disclosures should be consistent with how senior management and the board of directors assess and manage the operational risk of the bank.

63. A bank should have a formal disclosure policy approved by the board of directors that addresses the bank's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks should implement a process for assessing the appropriateness of their disclosures, including the verification and frequency of them

2.2.4. Классификация операционных рисков

2.2.4.1. Классификация событий операционного риска по видам

CRD предлагает следующую классификацию событий операционного риска по типам:

Event-Type Category	Definition
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events
Business disruption and system failures	Losses arising from disruption of business or system failures
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors

2.2.4.2. Классификация направлений деятельности

3. Базель II устанавливает следующую классификацию по направлениям деятельности:

Mapping of Business Lines

Level 1	Level 2	Activity Groups
Corporate Finance	Corporate Finance	Mergers and acquisitions, underwriting, privatisations, securitisation, research, debt (government, high yield), equity, syndications, IPO, secondary private placements
	Municipal/Government Finance	
	Merchant Banking	
	Advisory Services	
Trading & Sales	Sales	Fixed income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage
	Market Making	
	Proprietary Positions	
	Treasury	
Retail Banking	Retail Banking	Retail lending and deposits, banking services, trust and estates
	Private Banking	Private lending and deposits, banking services, trust and estates, investment advice
	Card Services	Merchant/commercial/corporate cards, private labels and retail
Commercial Banking	Commercial Banking	Project finance, real estate, export finance, trade finance, factoring, leasing, lending, guarantees, bills of exchange
Payment and Settlement[154]	External Clients	Payments and collections, funds transfer, clearing and settlement
Agency Services	Custody	Escrow, depository receipts, securities lending (customers) corporate actions
	Corporate Agency	Issuer and paying agents
	Corporate Trust	
Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open, private equity
	Non-Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open
Retail Brokerage	Retail Brokerage	Execution and full service

Table 2

Business line	List of activities	Percentage
Corporate finance	Underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis Services related to underwriting Investment advice Advice to undertakings on capital structure, industrial strategy and related matters and advice and services relating to the mergers and the purchase of undertakings Investment research and financial analysis and other forms of general recommendation relating to transactions in financial instruments	18 %
Trading and sales	Dealing on own account Money broking Reception and transmission of orders in relation to one or more financial instruments Execution of orders on behalf of clients Placing of financial instruments without a firm commitment basis Operation of Multilateral Trading Facilities	18 %
Retail brokerage (Activities with a individual physical persons or with small and medium	Reception and transmission of orders in relation to one or more financial instruments Execution of orders on behalf of clients Placing of financial instruments without a firm commitment basis	12 %

Business line	List of activities	Percentage
Commercial banking	Acceptance of deposits and other repayable funds Lending Financial leasing Guarantees and commitments	15 %
Retail banking (Activities with a individual physical persons or with small and medium sized entities meeting the criteria set out in Article 79 for the retail exposure class)	Acceptance of deposits and other repayable funds Lending Financial leasing Guarantees and commitments	12 %
Payment and settlement	Money transmission services, Issuing and administering means of payment	18 %
Agency services	Safekeeping and administration of financial instruments for the account of clients, including custodianship and related services such as cash/collateral management	15 %
Asset management	Portfolio management Managing of UCITS Other forms of asset management	12 %

3.1.1. Требования по зрелости процессов и инструментов управления операционным риском для Базового индикативного, Стандартизированного и Усовершенствованного подходов.

Согласно Базель: II bank will not be allowed to choose to revert to a simpler approach once it has been approved for a more advanced approach without supervisory approval. However, if a supervisor determines that a bank using a more advanced approach no longer meets the qualifying criteria for this approach, it may require the bank to revert to a simpler approach for some or all of its operations, until it meets the conditions specified by the supervisor for returning to a more advanced approach.

И предлагает делать оценку регуляторам по следующей градации:

Supervisory Rating Grades for Object Finance Exposures

Operating risk	Strong	Good	Satisfactory	Weak
Permits / licensing	All permits have been obtained; asset meets current and foreseeable safety regulations	All permits obtained or in the process of being obtained; asset meets current and foreseeable safety regulations	Most permits obtained or in process of being obtained, outstanding ones considered routine, asset meets current safety regulations	Problems in obtaining all required permits, part of the planned configuration and/or planned operations might need to be revised
Scope and nature of O & M contracts	Strong long-term O&M contract, preferably with contractual performance incentives, and/or O&M reserve accounts (if needed)	Long-term O&M contract, and/or O&M reserve accounts (if needed)	Limited O&M contract or O&M reserve account (if needed)	No O&M contract: risk of high operational cost overruns beyond mitigants
Operator's financial strength, track record in managing the asset type and capability to re-market asset when it comes off-lease	Excellent track record and strong re-marketing capability	Satisfactory track record and re-marketing capability	Weak or short track record and uncertain re-marketing capability	No or unknown track record and inability to re-market the asset

4. Опыт коммерческих банков, лучшие практики

4.1. Определение

В отношении операционного риска, несмотря на то, что часто берется определение, предлагаемое Базельским Комитетом, крупные банки разрабатывают собственное определение операционного риска, частично согласованное с определением Базельского Комитета. Так, репутационный риск может как включаться в определение операционного риска, так и исключаться.

Причина возможного включения репутационного риска наряду с правовым в определение операционного риска состоит в практической сложности отделения составляющих факторов репутационного и правовых рисков по конкретному случаю реализации операционного риска, а также в сложности оценки отдельных составляющих влияния этих факторов.

В любом случае, принятое Банком определение должно обеспечивать понимание связей операционного риска с правовым риском, комплаенс-риском, риском безопасности (в т.ч. информационной безопасности), репутационным риском и т.д..***Пример:***

Определение может однозначно обозначать что указанные выше риски (как и иные, не входящие в кредитный, рыночный и ликвидности) входят в операционный риск с той особенностью, что ими в рамках первой линии обороны управляют соответствующие профильные подразделения, в рамках второй линии обороны ими занимается специальное подразделение / сотрудник операционных рисков, а в рамках третьей линии обороны их курирует Служба внутреннего контроля (в соответствии с пп. 14-16 письма 69-Т от 16.05.2012).

4.2. Структура управления операционным риском

Система управления операционными рисками должна строиться на основании требований регуляторов и акционеров с учетом потребностей и масштабов бизнеса банка и приоритетных процессов.

Выделение в Банке отдельного подразделения/сотрудника, отвечающего за организацию системы управления операционными рисками, стало фактически повсеместной нормой, при этом в случае если данная задача не является для сотрудника/подразделения единственной, совокупность задач и функций указанного сотрудника/подразделения, а также его подчиненность, как правило, не содержит конфликта интересов.

Структура управления операционным риском, в которой каждое из подразделений Банка управляет операционными рисками своей деятельности, при этом обеспечивая соблюдение

требований, задаваемых системой по управлению операционными рисками, распространена не во всех банках.

В силу наличия разнообразных регуляторных требований к управлению смежными видами риска (комплаенс-риск, риск информационной безопасности, правовой риск и т.п.) подразделения банка, ответственные за управление указанными видами риска, зачастую управляют ими на условиях неполной согласованности соответствующих принципов, подходов и методологии с методологией управления операционными рисками Банка (в т.ч. в части подходов к оценке и управлению рисками).

Аудит зрелости процесса управления операционными рисками в отдельных подразделениях и в Банке может осуществлять служба внутреннего контроля и аудита.

Внутренние коммуникации в организации способствуют созданию общей культуры управления операционными рисками.

Банк доводит до сведения акционеров, регуляторов и надзорных органов, кредиторов, вкладчиков и иных клиентов, внешних аудиторов, рейтинговых агентств и других заинтересованных лиц информацию, раскрывающую используемые подходы к управлению операционным риском.

Цель управления операционным риском Банка достигается на основе системного, комплексного подхода, который подразумевает решение следующих задач:

- формирование сильной культуры операционного риск-менеджмента;
- получение оперативных и объективных сведений о состоянии и размере операционного риска;
- качественная и количественная оценка (измерение) операционного риска;
- создание системы управления операционным риском на стадии возникновения негативной тенденции, а также системы раннего предупреждения, направленной на предотвращение достижения операционным риском критически значительных для Банка размеров (минимизация риска);
- регулярный контроль профиля операционного риска и активов, подверженных действию операционного риска на основании существующей системы отчетности на всех уровнях, которые поддерживают проактивное управление операционными рисками.

4.3. Основные инструменты системы управления операционным риском

4.3.1. Идентификация и оценка рисков. Документирование этапа идентификации рисков / пересмотра перечня значимых рисков. Качественная оценка рисков. Ведение реестра рисков

Целями идентификации и оценки рисков являются:

- создание культуры управления операционным риском в самостоятельных структурных подразделениях/ филиалах Банка;
- поддержка эффективного выявления направлений деятельности и конкретных бизнес-процессов Банка, наиболее подверженных операционному риску;
- поддержка эффективного выявления наиболее существенных для Банка операционных рисков;
- обеспечение эффективного мониторинга операционных рисков на детальном уровне для всех основных направлений деятельности Банка;
- постоянное улучшение оперативного управления операционными рисками силами самих самостоятельных структурных подразделений/филиалов Банка, в том числе повышение эффективности мероприятий контроля;
- повышение эффективности самооценки самостоятельными структурными подразделениями/филиалами Банка уровня операционных рисков;

Основной задачей в ходе идентификации и оценки рисков является выделение существенных операционных рисков, т.е. рисков, возможное негативное влияние которых на банк является значимым. Критерии существенности операционного риска должны разрабатываться кредитной организацией самостоятельно.

Идентификация и оценка операционных рисков должна проводиться в следующих случаях:

- При формировании предложений по изменению бизнес-процессов (включая создание внутренних нормативных документов, описывающих такие изменения, автоматизацию отдельных функций и этапов бизнес-процессов и др.).
- При изменении организационно-штатной структуры подразделений, их компетенции и выполняемых функций.
- При перераспределении функций и функциональных обязанностей сотрудников внутри подразделения, в том числе в связи с кадровыми назначениями и перестановками.
- При появлении внешних по отношению к Банку факторов, влияющих на деятельность подразделений, действие которых будет носить долго- и среднесрочный характер (изменения в законодательстве Российской Федерации, природные катаклизмы, техногенные факторы, социальные изменения и др.).
- При реализации событий операционного риска.
- На периодической основе в рамках самостоятельной оценки подразделениями уровня операционного риска их деятельности и т.п.

В Банке должны быть разработаны документы (или определены подходы), определяющие порядок идентификации и оценки риска.

Для идентификации и оценки операционных рисков может использоваться следующая информация:

- Детальное описание анализируемого бизнес-процесса, включающее в себя последовательное, связное документирование всех подпроцессов с указанием:
- В качестве описания анализируемого бизнес-процесса могут быть использованы:
- внутренние нормативные документы, описывающие бизнес-процесс;
- карты бизнес-процессов;
- схемы деятельности;
- другие формы описания бизнес-процессов.
- Положения о подразделениях, участвующих в бизнес-процессе, должностные инструкции задействованных работников, а также данные о трудозатратах подразделения в детализации по выполняемым функциям.
- Информация из внешних источников о подверженности рискам бизнес-процессов/активов, аналогичных анализируемому, в российских и зарубежных кредитных организациях (при условии достоверного характера информации).
- Иная информация.

Для выявления рисков в отношении бизнес-процесса/материального актива последовательно рассматриваются все возможные типы риск-факторов (источников риска) согласно действующей в банке классификации риск-факторов. В отношении каждого типа риск-фактора определяется степень влияния на исследуемый бизнес-процесс/материальный актив в соответствии с критериями существенности рисков.

Идентификация операционных рисков, характерных для деятельности подразделений, осуществляется руководителями подразделений на постоянной основе.

Качественная оценка операционных рисков

Качественная оценка операционных рисков является основным подходом к оценке операционных рисков на данном этапе развития системы управления операционным риском. Банк должен осуществлять качественную оценку своих операционных рисков.

Качественная оценка включает в себя оценку вероятности реализации риска и тяжести последствий. Итоговый уровень риска при качественной оценке определяется на основании оценок вероятности его реализации и тяжести последствий, например, путём их сопоставления в таблице.

Качественная оценка операционных рисков производится путем присвоения выявленным операционным рискам уровня значимости (рейтинга). Качественная оценка операционного риска в форме рейтинга позволяет проводить более глубокий анализ операционного риска бизнес-процессов и операций, в том числе сравнивать различные варианты реализации бизнес-процессов, а также выявлять направления деятельности, наиболее подверженные операционному риску.

Для определения уровня операционного риска операции, бизнес-процесса и бизнес-направления оценивается:

- вероятность понесения Банком потерь при реализации операционного риска;
- тяжесть последствий от реализации операционного риска операции, бизнес-процесса и бизнес-направления.

Для оценки вероятности реализации риска используются шкала либо с качественными категориями (маловероятно, высоковероятно и т.п.), либо с количественными оценками частоты реализации риска (реализация риска раз в Х лет). Попадание в тот или иной диапазон шкалы также может оцениваться в баллах.

Для оценки тяжести последствий реализации риска используются шкала либо с качественными категориями (высокая тяжесть, низкая тяжесть, средняя тяжесть), либо с количественными оценками потерь в денежных единицах (диапазоны данной шкалы зависят как от размера Банка, так и от его аппетита к риску). Попадание в тот или иной диапазон шкалы также может оцениваться в баллах. По отдельной методике могут оцениваться последствия, влияющие на имидж Банка, а также комплаенс-последствия в виде санкций регулятора.

Итоговый уровень (рейтинг) операционного риска определяется путем интеграции оценок вероятности понесения Банком потерь и тяжести последствий от реализации операционного риска.

Результаты качественной оценки операционных рисков подлежат пересмотру по факту изменения бизнес-процессов и операций, в том числе реализации мероприятий по минимизации операционного риска, и включаются в состав описания рисков в реестре рисков, а также в состав отчетности об уровне операционного риска Банка.

Ведение реестра рисков

Реестр операционных рисков представляет собой перечень выявленных в Банке рисков с описанием их характеристик, включая статус работ по оптимизации.

Целью ведения реестра операционных рисков является систематизация информации о выявленных Банком рисках, их параметрах, результатах оценки и самооценки, поддержание информации об операционных рисках в актуальном состоянии. С помощью реестра операционных рисков также осуществляется контроль и мониторинг выполнения мероприятий по управлению операционными рисками.

Реестр операционных рисков включает в себя следующую информацию:

- описание операционного риска;
- риск-факторы;
- информацию о Владельце риска;
- описание контрольных процедур, направленных на минимизацию риска;
- оценку уровня операционного риска
- описание запланированных мер по управлению операционным риском и статус их исполнения;

- выбранный банком метод управления операционным риском (обоснованное принятие, перенос, минимизация, отказ от вида деятельности);

Реестр операционных рисков может включать в себя дополнительную информацию по усмотрению Банка.

Реестр операционных рисков включает информацию об операционных рисках, полученную на основании в т.ч:

- результатов самостоятельной идентификации и оценки рисков подразделениями;
- результатов внутренних проверок;
- результатов риск-аудитов;

Идентификация операционных рисков проводится не во всех банках, в ряде банков выявляются только риски, уже приводившие к негативным последствиям. Документирование выявленных рисков и их ведение в едином реестре рисков также проводится не во всех банках, в основном, данный подход применяется в основном крупными и крупнейшими банками. Основными документируемыми параметрами являются источники риска, направление деятельности, к которому относится риск, владелец риска, оценка уровня риска, метод управления и меры по управлению выявленным риском.

Основными подходами к идентификации операционных рисков, используемыми банками, является последовательное рассмотрение в отношении исследуемого процесса/продукта/направления деятельности риск-факторов (источников риска), классификация которых, как правило, формируется Банком индивидуально с учетом требований Базельского комитета.

В более продвинутой методологии идентификации рисков помимо рассмотрения отдельных источников риска также рассматриваются их сочетания, которые при одновременном воздействии взаимно усиливают негативный эффект.

4.3.2. Сбор данных о потерях

В Банке должны быть:

- реализованы механизмы сбора исторических данных о внутренних потерях в результате действия операционного риска.
- сформирована база данных (далее - БД), позволяющая вести учёт рисковых событий.
- разработаны документы (или определены подходы) по следующим направлениям:
  - - регламенты взаимодействия подразделений в процессе ведения Базы данных по учёту рисковых событий, включая критерии и требования при реализации которых рисковое событие (инцидент) регистрируется в БД.
  - - правила классификации и учета рисковых событий в Базе данных, в т.ч. правила и подходы:
  - - классификации по типу потерь;
  - - классификации по направлению деятельности;
  - - правила оценки понесенных потерь;
  - - процедуры, обеспечивающие анализ факторов, приведших к реализации рискового события и принятие решений по дальнейшему управлению соответствующим операционным риском для минимизации его негативного воздействия на кредитную организацию в дальнейшем.
  - - процедуры, обеспечивающие полноту и актуальность информации о рисковых событиях в Базе данных.
  - - прочее (на усмотрение кредитной организации)
- установлены критерии существенности – количественные и качественные показатели, при достижении которых возникает требование на внесение данных о реализовавшемся операционном риске в единую базу данных.

Полнота отражения фактов проявления операционных рисков подразделения в БД является предметом аудита со стороны служб внутреннего контроля и аудита (СВК и СВА).

4.3.3. Контрольная среда. Самооценка рисков и контролей

Критерии и условия, при соблюдении которых инициируется процесс самооценки рисков и контролей (RCSA), фиксируются во внутренних документах кредитной организации.

Например:

Процесс самооценки рисков и контролей (RCSA) инициируется в следующих случаях:

- - в плановом порядке в соответствии утвержденных планов на текущий финансовый год;
- - во внеплановом порядке - по факту попадания ключевого индикатора риска, установленного для подразделения в красную зону в течение двух отчетных периодов подряд, либо в случае фиксации рискового события уровня эскалации руководства кредитной организации;
- - при запуске нового продукта, нового процесса, новой системы или новой услуги, задействованные подразделения предварительно проводят самооценку для идентификации соответствующих операционных рисков и выработке мероприятий по их ограничению (минимизации) и контролю;
- - в процессе документирования рисков и контролей, инициированного решением Правления, коллегиальным органом, СВК.

В рамках RCSA формализуются идентифицируемые риски, оцениваются существующие контрольные процедуры и системы, с помощью которых онпи осуществляются,и разрабатываются меры по предотвращению и минимизации идентифицированных рисков.

В процессе RCSA также могут разрабатываться и описываться, экспертно оцениваться, ранжироваться сценарии для проведения сценарного анализа и стресс-тестирования;

Методологическую поддержку процесса самооценки, включая обучение персонала, занятого в самооценке, осуществляет подразделение, курирующее процесс управления операционными рисками.

На основе итоговых документов самооценки готовится план корректирующих мероприятий по ограничению (минимизации) и контролю операционных рисков.

При проведении внутренних проверок подразделения Служба внутреннего контроля/аудита проверяет соответствие указанных в документах самооценки и реально использующихся мероприятий по ограничению (минимизации) и контролю операционных рисков.

Самооценка операционных рисков подразделениями - владельцами рисков используется как инструмент оценки рисков не повсеместно, но в основном в крупных и крупнейших банках, а также в банках, система риск-менеджмента которых определяется материнским банком из числа международных кредитных организаций. Периодичность самооценки может варьироваться в диапазоне от ежегодной до ежеквартальной, различные процессы в зависимости от их значимости для Банка и присущего уровня рисков могут проходить самооценку с различной периодичностью. В рамках самооценки, как правило, риск классифицируется, выявляются его источники, проводится оценка риска. По итогам самооценки принимается решение о приемлемости уровня риска, методе и мерах по управлению риском. Участие риск-менеджмента в данном процессе, как правило, заключается в методической поддержке подразделений в ходе самооценки и рамочной верификации результатов самооценки.

4.3.4. Ключевые индикаторы риска (КИР) и ключевые индикаторы контроля (KCI)

КИР представляют собой измеримые показатели, отражающие уровень операционного риска. Использование КИР позволяет оценивать и прогнозировать изменения уровня риска, а также определять области его концентрации.

Мониторинг КИР позволяет своевременно принимать меры для сохранения приемлемого уровня соответствующего операционного риска.

В качестве типов рисков, для которых наиболее эффективен мониторинг уровня рисков с помощью КИР, можно выделить следующие:

- Риски сбоев ИТ-систем
- Риски, связанные с нарушением установленных лимитов и ограничений
- Риски, связанные с мошенническими операциями (с пластиковыми картами, кредитами, платежами и т.п.)
- Риски, связанные с некорректным проведением платежей
- Риски, связанные с исполнением Банком требований ПОД/ФТ
- Риски, связанные с текучестью персонала
- Риски, связанные с судебным делопроизводством
- Риски, связанные с жалобами клиентов (на методы взыскания, качество оказываемых услуг и т.п.)

Распределение функций по разработке КИР определяется кредитной организацией самостоятельно, при этом необходимо, чтобы КИР были акцептованы коллегиальным органом, ответственным за организацию управления операционными рисками Банка, либо одновременно:

- Подразделением, ответственным за управление операционными рисками;
- Подразделениями, риски которых измеряет КИР;
- Подразделениями, ответственными за расчет значений КИР.

Для эффективного применения КИР должны определяться следующие его характеристики:

- описание КИР;
- риск, уровень которого отражает КИР;
- алгоритм расчета КИР;
- периодичность мониторинга КИР;
- подразделение, являющееся ответственным за предоставление значений КИР.

Основной целью формирования системы КИР является создание системы раннего предупреждения об уровне повышенной концентрации операционного риска на определенном процессе.

Система КИР формируется в разрезе подразделений и процессов, при этом также могут формироваться сводные КИР, характеризующие общебанковские риски.

Основой для расчета значений показателей КИР являются показатели деятельности подразделения и данные базы данных о рисковых событиях.

Для каждого КИР на основании статистических данных и экспертных оценок определяющие пороговые уровни/ лимиты/зоны, попадание значения КИР в которые свидетельствует о том или ином уровне риска. Количество и характер зон выбираются кредитной организацией самостоятельно. В случае попадания значения КИР в зону/интервал повышенного уровня операционного риска банк должен инициировать анализ причин негативной динамики КИР и определить (при необходимости и возможности) мероприятия, направленные на управление уровнем риска. Пороговые значения должны на регулярной основе верифицироваться и, при изменении уровня и профиля рисков, надлежащим образом корректироваться для обеспечения их соответствия текущему аппетиту к риску организации.

Система пороговых уровней (лимитов) КИР должна являться составной частью риск-аппетита и служить метрикой допустимого уровня операционного риска банка.

Пороговые значения должны быть обоснованы и задокументированы, а также должны пересматриваться на регулярной основе.

В Банке должны быть разработаны документы (или определены подходы), определяющие организацию системы мониторинга операционных рисков с помощью КИР:

- Документы, определяющие порядок разработки, согласования, утверждения КИР, включая процедуры взаимодействия, функции и ответственность подразделений в указанных процессах.

- Перечень КИР, формирующих Систему КИР и подлежащих мониторингу на регулярной основе,
- Периодичность мониторинга, определяемая с учетом эффективности использования того или иного КИР.
- Полномочия подразделения по управлению операционными рисками по вводу/прекращению мониторинга того или иного КИР.

4.3.5. Сценарный анализ и стресс-тестирование

Стресс-тестирование операционного риска проводится в Банке для достижения следующих целей:

- оценка потерь, связанных с реализацией исключительных, но вероятных событий, обусловленных влиянием факторов операционного риска;
- разработка предложений по комплексу мероприятий по управлению операционными рисками по результатам оценки потерь;
- учет потерь, связанных с реализацией исключительных, но вероятных событий, обусловленных влиянием факторов операционного риска при определении величины капитала Банка, резервируемого на покрытие операционного риска.

Стресс-тестирование операционных рисков включает в себя следующие методы:

- сценарный анализ;
- анализ чувствительности.

Сценарный анализ представляет собой метод стресс-тестирования операционных рисков, заключающийся в выборе маловероятных событий операционного риска с высокой тяжестью потерь, которые могут реализоваться в будущем (сценариев) и дальнейшей оценке возможных негативных последствий их реализации для Банка.

Задачей сценарного анализа является определение и выявление воздействия сценария на бизнес-процессы, контрольные процедуры и процедуры отчетности. Примерами сценариев могут выступать такие события как долговременный простой в работе ввиду отключения электричества в здании, компьютерный вирус в сети банка, потери из-за мошеннических действий сотрудников банка или его контрагентов и др.

Анализ сценариев оценивает влияние соответствующих операционных событий. Подразделение ответственное за управлением операционным риском может определять соответствующие сценарии среди исторических событий или может устанавливать новые сценарии, определенные экспертами бизнес процесса.

Анализ сценариев – это ключевой элемент процесса управления рисками: он предназначен для оценки подверженности Банка рискам. Это также диагностический инструмент для улучшения понимания профиля (уровня) риска Банка. Данный инструмент оценивает риски, которые могут возникнуть в будущем.

Результаты сценарного анализа используются при проведении стресс-тестов и во внутренней модели оценки операционного риска.

При разработке сценариев могут использоваться любые внешние и внутренние источники данных, в том числе следующие:

- внутренние и внешние данные о существенных операционных;
- внутренние и внешние данные о событиях операционного риска;
- информация об эффективности контрольных процедур и бизнес-процессов в целом (в том числе информация, полученная по результатам риск-аудитов или самостоятельной оценки операционных рисков);
- информация о мерах по обеспечению непрерывности деятельности Банка;

Разработка сценариев осуществляется, как правило, подразделением, ответственным за управление операционными рисками при участии подразделений Банка.

Оценка сценариев может осуществляться на основе мотивированных суждений и экспертных оценок подразделений Банка, деятельность которых в той или иной степени затронута сценарием.

Количественная оценка влияния сценария, полученная с помощью сценарного анализа, должна использоваться при проведении количественной оценки операционного риска.

Анализ чувствительности оценивает непосредственное воздействие на величину капитала Банка, резервируемого на покрытие операционного риска, изменений одного или нескольких факторов операционного риска или параметров функций плотности распределения[1].

Было бы обычной практикой разделить анализа сценариев (который является техникой оценки риска) и стресс-тестирование (который является частью расчета достаточности капитала). В большинстве европейских банков анализ сценариев можно рассматривать как более сложные версии RCSA. Отдельные сценарии могут быть выбраны для в стресс-тестирования. Но стресс-тестирование также оказывает влияние на капитал (как в рамках TSA и AMA).

4.3.6. Планирование непрерывности и восстановления бизнеса

Банки осуществляют деятельность по обеспечению непрерывности и восстановления бизнеса согласно требований Приложения 5 Положения 242-П.
При этом отдельные банки ведут построение системы обеспечения непрерывности бизнеса с использованием стандартов, отличных от требований Банка России, например, стандарта BS 25999-2:2007, BS 25999-1:2006 « Управление непрерывностью деятельности», либо стандарта «Система управления непрерывностью деятельности кредитных организаций банковской системы Российской Федерации», утв. Советом АРБ от 16.12.2010.

4.3.7. Тестирование контрольных процедур и влияние на остаточный риск

Контрольные процедуры подлежат регулярному тестированию и пересмотру на предмет их влияния на остаточный риск. Целью тестирования является предоставление руководству Банка информации о корректности выполнения бизнес-процессов подразделений для своевременного выявления операционных рисков и принятия мер по их снижению.

Перечень контрольных процедур и периодичность их тестирования отражается в Матрице контрольных процедур.

Общие принципы ведения Матрицы контрольных процедур.

С целью наиболее полного охвата бизнес-процессов подразделения матрица заполняется/обновляется в следующей последовательности:

- определяются бизнес-процессы подразделения
- определяются основные риски, связанные с этими процессами; указывается уровень каждого риска.
- для каждого риска определяются существующие контрольные процедуры, способствующие его снижению;
- если контрольная процедура отсутствует либо она имеет признаки неэффективности - проектируются тесты, которые позволят проверить эффективность работы контрольной процедуры в целях снижения соответствующего ей риска;
- устанавливается периодичность тестирования.

Общие принципы разработки тестов.

Тестирование контрольной процедуры проводится по следующим направлениям:

---

1 При этом анализ чувствительности может проводиться как для функций плотности распределения потерь Банка от операционных рисков по отдельным направлениям деятельности и/или типам событий операционного риска, так и по Банку в целом. Возможно проведение отдельного анализа чувствительности для функций плотности распределения вероятности и/или тяжести потерь Банка от операционных рисков.

- Оценка соответствия контрольной процедуры уровню и характеру риска, для минимизации которого она предназначена
- Периодичность выполнения процедуры
- Качество документирования результатов выполнения процедуры

Тестирование контрольных процедур производится на основе следующих общих принципов:

- Тестирование производится на том же массиве исходной информации (документов), на котором функционирует контрольная процедура.
- Для тестирования может быть выбрано подмножество исходных данных (документов) с целью максимального охвата всех возможных типов их значений/разновидностей.
- Периодичность тестирования устанавливается таким образом, чтобы в тест были включены различные варианты значений/разновидностей исходных данных (документов).

При выявлении недостатков контрольной процедуры = в процессе, периодичность проведения её тестирования после устранения недостатков может быть установлена с более коротким периодом, с тем, чтобы убедиться в достаточности и эффективности осуществленных мероприятий по устранению недостатков.

По результатам тестирования контрольные процедуры совершенствуются с целью снижения связанных с ними рисков.

В случае, если невозможно или нецелесообразно введение/изменение контрольных процедур с целью снижения вероятности/тяжести последствий реализации риска, данный риск может быть принят.

Принятие риска возможно в случаях, если возможные потери от реализации риска приемлемы для Банка, и при этом введение/ изменение контрольной процедуры по управлению этим риском:

- требует значительных материальных затрат либо затрат труда (в частности, значительных изменений в бизнес-процессах Банка, закупки дорогостоящего оборудования, комплексной переработки программного обеспечения);
- нецелесообразно в силу запланированных значительных изменений бизнес-процесса, устраняющих либо значительно снижающих данный риск.

Тестирование контрольных процедур (в т.ч. управление периодичностью тестирования или признание нецелесообразности дальнейшего тестирования) по принятому риску продолжается в обычном порядке.

4.3.8. Система отчетности по операционным рискам

Система отчетности Банка – это совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того, чтобы своевременно обеспечивать внутренние структуры Банка и внешних контрагентов надлежащей информацией об уровне операционного риска в кредитной организации с целью эффективного управления.

Система отчетности по операционным рискам реализуется в кредитной организации с целью эффективного управления операционным риском и осуществления своевременного контроля за ним. Подразделение Банка по контролю за операционными рисками должно регулярно, как минимум один раз в квартал, готовить отчет об уровне операционного риска, и представлять его на рассмотрение Уполномоченному органу Банка (Комитету по операционным рискам, Правлению Банка, Наблюдательному Совету Банка, иное). Отчет должен быть подготовлен на основании получаемых данных/отчетов от ответственных подразделений по управлению операционным риском и/или из систем Банка, в соответствии с внутренними правилами и инструкциями, а также (если применимо) в соответствии с требованиями контролирующей/материнской структуры, в четкой, сжатой и логичной форме, а также должен содержать описание и оценку рисков Банка, предлагаемые меры по их минимизации.

Уполномоченный орган должен однозначно подтвердить, что он ознакомился с содержанием отчета, приведенные в нем данные (в т.ч. их достоверность и качество) полностью соответствуют требованиям к отчетности, включая правильность, полноту и последовательность. Соответствующие меры, которые применяются на основании этого отчета, должны быть четко и логично оформлены документально.

Входящая отчетность (при использовании подходов Стандартизированный и Продвинутый) от внутренних структур для определения уровня операционного риска должна содержать информацию по следующим направлениям:

- КИР
- Оценка/самооценка рисков
- Сценарный анализ
- Рисковые события операционного риска;
- Достаточность капитала под операционный риск
- Экономический Капитал (расчет показателей)
- Система обеспечения непрерывности деятельности
- Предлагаемые меры по уменьшению/минимизации уровня операционного риска .

Отчетность может предоставляться следующим органам/службам:

- внутренним регуляторам (регулярная/по запросу)
- Комитетам (Антикризисный, По операционным рискам, и т.д.):
- Правлению
- Наблюдательному совету
- Внутреннему Аудиту/Контролю

Периодичность предоставления отчетности внутри Банка при использовании подходов Стандартизированный и Продвинутый – не реже 1 раза в квартал, по инцидентам со значительным потенциальным/реальным убытком - оперативно, в форме внепланового отчета.

Исходящая отчетность/раскрытие (регулярная/по запросу) может предоставляться также

- Контрагентам
- Рейтинговым агентствам
- Внешним регуляторам
- Аудиторским/консалтинговым компаниям
- Контролирующим/ «материнским» структурам
- Страховым компаниям

Формат отчетности по отчетности, предоставляемой Банком в целях раскрытия, задается получателем в зависимости от цели раскрытия информации и, как правило, включает:

1. Структуру управления рисками/внутреннего контроля в Банке.
2. Принципы управления операционными рисками.
3. Используемый подход для расчета достаточности капитала под операционный риск.
4. Наличие внутренних нормативных документов, регулирующих управление операционными рисками и осуществление внутреннего контроля.
5. Наличие и зоны ответственности Коллегиальных органов, отвечающих за управление/принятие решений.
6. Раскрытие значимых инцидентов операционного риска/убытки за период.

С установленной в банке периодичностью (преимущественно не реже чем на ежеквартальной основе) руководители подразделений и филиалов готовят и предоставляют в подразделение, ответственное за управление операционным риском, информацию о случаях проявления операционных рисков в их подразделениях и возникших вследствие этого прямых и косвенных убытках. Внедрение автоматизированной системы позволяет уменьшить периодичность предоставления информации.

Пример предоставления отчетности:

На ежеквартальной основе подразделение, ответственное за управление операционным риском, подготавливает и представляет Членам Правления (в копии Службе внутреннего контроля, Службе внутреннего аудита) отчеты о текущем профиле операционного риска Кредитной организации с предложениями по корректировкам в зонах концентрации операционных рисков.

На ежеквартальной основе подразделение, ответственное за управление операционным риском, подготавливает и представляет Членам Правления (в копии Службе внутреннего контроля, Службе внутреннего аудита) отчеты с показателями КИР.

4.4. Классификация операционных рисков

Классификация по видам потерь разрабатывается кредитными организациями самостоятельно, но должна быть сопоставима с классификацией, рекомендуемой Базельским комитетом по надзору за банковской деятельностью.

Банк во внутренних документах определяет правила учета потерь от рискового события, включая потери от реализации иных рисков (кредитного, рыночного, репутационного, правового и пр.) в результате действия операционного риска. Отдельным образом регламентируется оценка и учет возмещения первоначально понесенных потерь.

Например,

Прямыми потерями называют убытки, которые являются следствием реализации события операционного риска и размер которых можно точно определить в денежном выражении.

Прямые потери, как правило, являются расходами, возникшими вследствие нарушения условий, связанных с осуществлением кредитной организацией своей деятельности (несоблюдение требований законодательства Российской Федерации, договорной и трудовой дисциплины, обычаев делового оборота и тому подобное), а также расходы, возникающие как последствия чрезвычайных обстоятельств хозяйственной деятельности. Сумма прямых потерь определяется в процессе оценки всех последствий рискового события с учетом как прямых потерь, так дополнительных затрат и расходов. Прямые потери могут быть результатом денежных потерь (наличных или безналичных), потерь (ущерба) имущества (основные средства и материальные запасы), материальных (физических) и нематериальных активов и иных ценностей.

Понятие косвенных потерь (косвенного ущерба) определяется кредитными организациями индивидуально. Должна быть возможность обеспечить соответствие (маппинг) видов потерь, используемых в Банке, видам потерь, рекомендуемым Базельским комитетом по надзору за банковской деятельностью.

При расчете косвенного ущерба в описании рискового события должны указываться количественные характеристики рискового события: объем операции, количество операций, продолжительность события, количество клиентов, возможный размер штрафа, время неработоспособности, дополнительные трудозатраты и др. в целях более точной оценки возможных убытков в будущем.

Во внутренних документах Банка устанавливаются правила мэппинга внутренних направлений деятельности к линиям Базеля II, а также правила классификации по внутренним бизнес-линиям вспомогательной, сопутствующей и обеспечительной деятельности.

4.5. Требования по зрелости процессов и инструментов управления операционным риском для Базового индикативного, Стандартизированного и Усовершенствованного подходов.

Система сбора данных о потерях должна удовлетворять следующим принципам:

- Достоверность и достаточность данных о потерях, используемых для расчета операционных рисков.

- Должны регистрироваться все инциденты операционного риска и потери (далее инциденты) с фактической суммой убытка свыше определенного порога, установленного Банком. Данный порог должен соответствовать как масштабам Банка, так и специфике его деятельности. Банк по своему усмотрению может учитывать инциденты с потенциальным убытком и инциденты, произошедшие в других банках (в качестве возможных непредвиденных / неожидаемых убытков).
- Каждый сотрудник банка должен иметь обязанность (закрепленную нормативно) сообщить Риск-менеджменту о выявленном рисковом событии. Для такого сообщения может использоваться техническая возможность регистрации обнаруженного инцидента в единой базе потерь банка (далее База потерь).
- Должна использоваться система мотивации сотрудников банка к тому, чтобы они своевременно регистрировали обнаруживаемые ими инциденты.
- Должна использоваться система идентификации тех инцидентов, которые в нарушение нормативных требований не были зарегистрированы в Базе потерь. Руководству банка должна подаваться отчетность о таких фактах.
- Записи об обнаруженных инцидентах (в Базе потерь) должны быть не доступны для изменения Администратором Базы потерь, либо должна регистрироваться вся история их изменения (логирование изменений) и сохраняться резервная копия базы на информационных ресурсах, доступных только Службе информационной безопасности банка.
- По каждому зарегистрированному инциденту должны иметься данные сотрудника банка, который занимался работой с этим инцидентом и в последующем сможет подтвердить его факт и детали.
- Банк производит оценку суммы убытка каждого инцидента по внутренним методикам. При этом расчет суммы убытка по каждому инциденту может производится по следующим правилам:

Пример формулы расчета суммы убытка приведен в Приложении 6.

К убытку от инцидентов не относятся расходы, затраченные банком на выработку мер по недопущению инцидентов, аналогичных произошедшему (мер предотвращения инцидентов), а также расходы на реализацию таких мер.

Банк должен определить порядок отражения в отчетах инцидентов, в которых сумма убытка имеет отрицательную величину (когда суммы поступлений вызванных инцидентом превышают суммы потерь).

Пример

В сводных отчетах по банку все инциденты, в которых сумма убытка имеет отрицательную величину (когда суммы поступлений вызванных инцидентом превышают суммы потерь), признаются как инциденты с нулевым убытком (для того чтобы они не искажали размера убытков от других инцидентов). Такими инцидентами могут быть, например, факты возникновения излишков в банкоматах или, например, инциденты по которым сумма возмещений превысила суммы убытков. При этом банк должен иметь возможность представить отчетность отдельно по инцидентам, где суммы поступлений вызванных инцидентом превышают суммы потерь.

Для целей точности расчета убытков от отдельных видов однотипных инцидентов, по которым прямые потери от инцидентов, как правило, отсутствуют (нарушения лимитов, сторно-проводки)) размер убытка от таких инцидентов может назначаться нормативно.

Инциденты, произошедшие в других банках, могут учитываться в качестве возможных непредвиденных убытков банка. Учет производится после изучения обстоятельств инцидента и только в случае, если банк признает, что имеется вероятность того, что аналогичные инциденты могут произойти в банке (банк осуществляет операции в рамках, которых произошел инцидент). Исходя из величины банка, в котором они произошли, Банк должен принять решение о

целесообразности масштабирования (увеличения / уменьшения) таких потерm применительно к своему банку.

Не реже 1 раза в 3 года должен проводиться внутренний и внешний аудит на предмет достоверности данных об инцидентах и потерях зарегистрированных в Базе потерь и о соответствии системы управления операционным риском, указанным в настоящем разделе требованиям.

По первому требованию Банка России банк должен быть готов предоставить все данные из Базы потерь в электронном виде.

Каждый инцидент должен быть отнесен к бизнес-линии, в которой он произошел (направления деятельности кредитной организации согласно внутренней классификации Банка с возможностью установления соответствия с категориями Приложения к Письма 76-Т) и категории инцидента (согласно внутренней классификации Банка с возможностью установления соответствия с категориями п. 1.3. Письма 76-Т).

В случаях, когда инцидент произошел во вспомогательном процессе (например, произошел в процессе кадрового делопроизводства), устанавливается назначение вспомогательной операции - бизнес-линия для, которой производилась эта операция и указывается именно эта бизнес-линия.

Пример

Если инцидент произошел в процессе кадрового делопроизводства (не связанного с бизнес-линиями) при назначении сотрудника на должность в подразделение кредитования физических лиц, значит этому инциденту назначается бизнес-линия - «Банковское обслуживание физических лиц». Если же трудоустройство сотрудника, в ходе которого произошел инцидент, осуществлялось в подразделение корпоративного кредитования, значит этому инциденту назначается бизнес-линия – «Банковское обслуживание юридических лиц». При этом в отчете об инциденте в обязательном порядке указываются пояснения подтверждающие взаимосвязь инцидента с бизнес-линией.

Если невозможно установить взаимосвязь инцидента ни с одной бизнес-линией (ни прямую, ни опосредованную), такому инциденту, назначается бизнес-линия, приносящая банку наибольшую доходность.

Принадлежность инцидента к категории определяется экспертным путем. При этом экспертное мнение является приоритетным в сравнении с формально наличествующими признаками. Например, когда инцидент (злоумышленные действия) имеет признаки того, что мог быть совершен только при помощи сотрудника банка, однако доказательств этому нет, то такой инцидент относится согласно п. 1.3. Письма 76-Т к категории «злоупотреблений или противоправных действий, осуществляемых служащими или с участием служащих кредитной организации (например, хищение, злоупотребление служебным положением, преднамеренное сокрытие фактов совершения банковских операций и других сделок, несанкционированное использование информационных систем и ресурсов).

Банк должен иметь пятилетнюю историю наблюдений внутренних данных об убытках в соответствии с требованиями Письма 15-2-1-9/2644.

4.6. Расчет VAR

Банк может ставить вопрос о применении Усовершенствованного («продвинутого») подхода (AMA), минуя использование стандартизированного подхода.

При расчете операционного риска усовершенствованным («продвинутым») подходом даётся определение непредвиденным / неожидаемым убыткам (unexpected loss), а также ожидаемымм убыткам (expected loss)

Пример:

По умолчанию непредвиденными / неожидаемыми убытками (unexpected loss) определяются те убытки, которые превышают среднее значение построенного банком несимметричного распределения суммарных потерь операционного риска. Банк по своему усмотрению может включать в эти потери инциденты других банков.

5. Консолидированная позиция ЭГ

- Определение операционного риска (включая взаимосвязь со смежными видами рисков).
- Структура управления операционным риском
- Основные инструменты системы управления операционным риском, включая
- Идентификация и оценка рисков. Документирование этапа идентификации рисков / пересмотра перечня значимых рисков. Качественная оценка операционных рисков.Ведение реестра рисков.
- Сбор данных о потерях
- Контрольная среда. Самооценка рисков и контролей
- Ключевые индикаторы риска (KRIs) и ключевые индикаторы контроля (KCI)
- Ключевые показатели эффективности управления операционным риском (KPIs)
- Сценарный анализ и стресс-тестирование
- Планирование непрерывности и восстановления бизнеса
- Тестирование контрольных процедур и влияние на остаточный риск
- Система отчетности по операционным рискам
- Классификация операционных рисков
- Классификация событий операционного риска по видам
- Классификация направлений деятельности
- Требования по зрелости процессов и инструментов управления операционным риском для Базового индикативного, Стандартизированного и Усовершенствованного подходов.

5.1. Определение операционного риска

Необходимо закрепить в нормативно-правовых актах Банка России более четкое определение операционного риска, обозначая, какие смежные риски не подпадают под данное определение (например, репутационный, стратегический), какие, напротив, попадают (например, правовой риск, риск информационной безопасности, информационно-технологический риск), а также в отношении каких рисков вопрос их включения/невключения в состав операционных рисков может быть оставлен на усмотрение кредитной организации. Предлагается включить в определение операционного риска для целей менеджмента (приоритезации рисков), но исключить из расчета капитала репутационный риск.(. to include it for management purposes (to support the prioritisation of risks) but to exclude it for capitalization purposes (since the resulting fluctuations of business demand would often already be covered under Basel 2 Pillar 2 business risk)

Предлагается оставить кредитным организациям возможность применять расширенное определение операционного риска в рамках построения систем управления операционным риском в своих организациях. Например, в случае, если определение операционного риска, принятое Банком России, включает правовой риск, но исключает репутационный, кредитные организации по своему усмотрению могут включить репутационный риск в определение операционного в рамках организации системы управления операционным риском в своей организации.

Предлагается дополнительно внести определение комплаенс-риска в нормативно правовые акты Банка России, с учетом рекомендаций Базельского Комитета «Комплаенс и комплаенс-функция в банках». Данное определение могло бы объединить существующие определения правового риска и риска потери деловой репутации, а также обеспечить последующую возможность определить единые стандарты и методы управления операционными и комплаенс рисками на уровне организации. Кроме того, наличие данного определения позволит кредитным

организациям сделать выбор в пользу полного либо частичного включения комплаенс-риска в состав операционного риска.

5.2. Структура управления операционным риском

Представляется целесообразным закрепить в нормативных документах Банка России следующие требования к структуре управления операционным риском.

Структура управления операционным риском должна строиться на основании требований регуляторов и акционеров с учетом потребностей и масштабов бизнеса и приоритетных процессов.

Структура управления операционным риском должна обеспечить эффективное распределение зон ответственности за управление теми или иными составляющими операционного риска.

Структуры управления смежными видами риска (комплаенс-риск, риск информационной безопасности, правовой риск и т.п.) должны обеспечивать управление данными видами риска на условиях согласованности соответствующих принципов, подходов и методологии с методологией управления операционными рисками Банка (в т.ч. в части подходов к оценке и управлению рисками). Так, при определении стандартов управления информационной безопасностью целесообразно определять стандарты таким образом, чтобы терминология, используемая при управлении информационной безопасностью («угроза», «риск», «инцидент» и пр.) была согласована с терминологией, используемой при управлении операционными рисками.

Для повышения качества оперативного управления операционными рисками предлагаем Банку России рекомендовать выделение в подразделениях Банка сотрудников, обеспечивающих поддержку процессов управления операционными рисками.

В нормативно-правовых актах Банка России следует предусмотреть специфику процессов с учетом масштаба деятельности кредитной организации таким образом, чтобы структура управления операционным рисков позволяла эффективно управлять операционным риском, и взаимодействовать с подразделениями Банка, отвечающими за управление смежными видами рисков.

В отношении несоблюдения политики операционного риска, мы рекомендуем баланс между дисциплинарными мерами и действиями, которые мотивируют к предоставлению отчетности потери без страха дисциплинарных мер. Только при хорошо налаженном процессе сбора данных о потерях результаты можно использовать для предоставления руководству..

5.3. Основные инструменты системы управления операционным риском

Минимальный обязательный набор основных инструментов системы управления операционным риском Банку России рекомендуется закрепить в нормативно-правовых актах. Использование остальных инструментов, рекомендованных Базельским комитетом, предлагаем оставить на усмотрение Банков, т.е. в зависимости от зрелости системы управления операционным риском и от специфики и масштабов деятельности кредитной организации Банкам можно предоставить свободу в использовании инструментов управления операционным рисков.

К обязательному набору инструментов можно отнести следующие:

5.3.1. Идентификация и оценка рисков. Документирование этапа идентификации рисков / пересмотра перечня значимых рисков Идентификация и оценка рисков. Качественная оценка рисков. Ведение реестра рисков

Предлагается также уточнить в нормативных документах Банка России следующее.

Основной задачей в ходе идентификации и оценки рисков является выделение существенных операционных рисков, т.е. рисков, возможное негативное влияние которых на банк является значимым.

Критерии существенности операционного риска должны разрабатываться кредитной организацией самостоятельно.

Внутрибанковская система оценки операционных рисков должна быть тесно интегрирована с текущими процессами управления рисками в банке, а ее результаты - составлять неотъемлемую часть процесса мониторинга и контроля структуры операционных рисков банка. В частности, информация об оценке рисков должна играть существенную роль при составлении отчетов о рисках, управленческих отчетов, внутреннем распределении капитала и анализе рисков.

Предлагается также рекомендовать Банкам иметь методики:

- распределения капитала под операционные риски основных бизнес-линий
- стимулирования улучшения корпоративного управления.

5.3.2. Сбор данных о потерях

Представляется целесообразным закрепить в нормативных документах Банка России следующие рекомендации организации сбора данных о потерях.

Кредитной организации рекомендуется накапливать внешнюю информацию о значительных убытках, понесенных кредитными организациями вследствие реализации операционного риска, включающую данные о суммах убытков, информацию о масштабе деловых операций в регионе (отрасли и так далее), в котором были понесены убытки, информацию о причинах и обстоятельствах событий, вызвавших убытки, а также прочую информацию, которая могла бы помочь в оценке актуальности этих событий для других кредитных организаций. Также рекомендуется разработать процедуру систематического выявления ситуаций, в которых аналитическая база данных о понесенных операционных убытках используется в целях оценки принятого кредитной организацией операционного риска, а также методологию учета внешней информации при оценке операционного риска.

5.3.3. Контрольная среда. Самооценка рисков и контролей

Рекомендуем Банку России закрепить в нормативно правовых актах минимальные требования и периодичность проведения самооценки рисков и контролей, однако способ проведения, детализацию и охват рекомендуем оставить на усмотрение банков.

5.3.4. Ключевые индикаторы риска (KRIs) и ключевые индикаторы контроля (KCI)

76-Т Банка России дает достаточные рекомендации кредитным организациям в области управления КИР как важнейшим инструментом мониторинга операционных рисков.

Периодичность осуществления мониторинга операционного риска ЭГ предлагает определять кредитной организации самостоятельно исходя из степени его существенности для соответствующего направления деятельности, внутренних процедур управления операционным риском или возможностей информационно-технологической системы.

5.3.5. Ключевые показатели эффективности управления операционным риском (KPIs)

76-Т Банка России дает достаточные рекомендации кредитным организациям в области ключевых показателей эффективности управления операционным риском.

Разработку системы оценки эффективности управления операционным риском рекомендуем оставить на усмотрение банков.

5.3.6. Сценарный анализ и стресс-тестирование

В нормативно-правовых актах Банка России определены понятия сценарного анализа, цели и критерии его проведения.

Правила и процедуры проведения стресс-тестирования рекомендуется оставить на усмотрение банков: либо разработать самостоятельно, либо использовать методы, принятые в международной банковской практике.

В Банке должны быть разработаны документы или определены подходы, определяющие проведение стресс-тестирования операционного риска (сценарного анализа и анализа чувствительности), раскрывающие в т.ч. следующие аспекты:

- Периодичность проведения сценарного анализа и анализа чувствительности
- Необходимость обоснования экспертных оценок и допущений, сделанных в ходе сценарного анализа и анализа чувствительности.
- Распределение функций и ответственности в процессе сценарного анализа: разработки сценариев, их анализа, согласования и акцепта результатов.

5.3.7. Планирование непрерывности и восстановления бизнеса

Предложения ЭГ касательно требований к организации системы управления непрерывностью бизнеса, которым должен удовлетворять банк, в зависимости от выбранного банком метода расчета капитала по операционный риск: метод базового индикатора, стандартизованный метод, продвинутый метод, представлены в Приложении №8.

5.3.8. Тестирование контрольных процедур и влияние на остаточный риск

Разработку процедур тестирования контрольных процедур и оценки их влияния на остаточный риск рекомендуем оставить на усмотрение банков.

5.3.9. Система отчетности по операционному риску (определение минимальных требований в зависимости от используемого подхода).

Необходимо закрепить в нормативно-правовых актах Банка России минимальные требования к системе отчетности по операционным рискам, включая периодичность, стандартный формат/наполнение отчетов с перечнем того, что должно включаться в отчеты в обязательном порядке в зависимости от используемого банком подхода к расчету достаточности капитала (согласно рекомендациям Базельского Комитета - базовый индикативный, стандартизированный, продвинутый подходы). Предложения ЭГ по данному вопросу отражены в разделе 4.3.8

Предлагается отразить взаимосвязь системы отчетности со структурой управления операционными рисками, в том числе определить зоны ответственности по подготовке отчетности, анализу результатов и принятию решений по результатам анализа на разных уровнях управления Кредитной организации.

Предлагается оставить кредитным организациям возможность использовать расширенную систему отчетности по операционным рискам в рамках построения структуры и системы управления операционным риском в своих организациях.

5.4. Классификация операционных рисков

Предлагаем Банку России определить подходы к классификациию операционных рисков (например, по риск-факторам, по видам рисковых событий и т.п.), определения направлений деятельности, в разрезе которых классифицируются риски. Такие подходы, классификации и определения должны иметь статус опциональных. При определении указанных классификаций и подходов полагаем необходимым придерживаться основных категорий риска, прописанных в рекомендациях Базельского комитета. Детализацию классификаторов операционных рисков необходимо оставить на усмотрение банков.

5.5. Требования по зрелости процессов и инструментов управления операционным риском для Базового индикативного, Стандартизированного и Усовершенствованного подходов.

Необходимо закрепить в нормативно-правовых актах Банка России четкие количественные и качественные критерии соответствия Базовому индикативному, Стандартизированному и Усовершенствованному подходу, а также критерии для проверки и одобрения Банком России критериев соответствия тому или иному подходу.

Базельский Комитет не конкретизирует подход или допущения о распределении, использующиеся для генерирования показателя операционных рисков в целях регулятивного капитала. Однако банки должны быть в состоянии продемонстрировать, что их подход учитывает потенциально значимые случаи экстремальных убытков

Предлагается оставить кредитным организациям возможность использовать подход AMA для некоторых операций и базовый индикативный подход или стандартизованный подход для остальных операций (частичное использование) при условии выполнения определенных требований.

Предлагается также допустить возможность перехода на усовершенствованный (AMA) подход минуя стадию соответствия стандартизированному подходу.

В соответствии с рекомендациями Базельского Комитета банки могут использовать усовершенствованный подход при условии соблюдения определенных минимальных требований.

При этом после получения банком разрешения на использование продвинутого подхода банку не будет позволено по своему усмотрению (без разрешения органа надзора) возвращаться к более простому подходу. Однако если Центральный Банк сочтет, что банк, использующий более продвинутый подход, больше не удовлетворяет его критериям, он может потребовать, чтобы банк вернулся к более простому подходу к некоторым или всем своим операциям до тех пор, пока не выполнит условия, установленные органами надзора для возврата к более продвинутому подходу.

В любом случае при использовании усовершенствованного подхода банки должны доказать надежность и адекватность данного подхода, т.е. должны рационально оценивать непредвиденные убытки, основываясь на комбинированном использовании внутренних и релевантных внешних данных об убытках, на сценарном анализе, а также на деловой среде банка и системе внутреннего контроля.

6. Особые мнения Экспертов

6.1. Определение операционного риска

Эксперт:

Не являются событиями операционного риска неумышленные ошибки персонала, в оценке кредитного, рыночного рисков (в т.ч. процентного, валютного, фондового), выразившиеся в неправильном определении параметров кредитной или рыночной стратегии, в том числе, в параметрах скоринговых карт или параметров «брокерских роботов». Не являются событиями операционного риска неумышленные ошибки персонала, в оценке стратегического и репутационного риска. Не являются событиями операционного риска ущерб, возникший от реализации кредитного, рыночного, стратегического и репутационного рисков.

7. Дополнительная информация

7.1. Список сокращений

Базельский комитет - комитет по банковскому надзору при Банке международных расчётов. Основными задачами Комитета являются внедрение единых стандартов в сфере банковского регулирования.

RCSA - Самооценка рисков и контролей .

КИР - Ключевые индикаторы риска.

КПЭ - Ключевые показателями эффективности.

ФУОР - Независимая корпоративная функция управления операционным риском.

ВПОДК - Внутренние процедуры оценки достаточности капитала.

7.2. Список литературы

Письмо от 24 мая 2005 г. N 76-Т «Об организации управления операционным риском в кредитных организациях»;

Письмо от 16 мая 2012 г. N 69-Т «О рекомендациях Базельского Комитета по банковскому надзору «Принципы надлежащего управления операционным риском»; Письмо от 29 июня 2011 г. N 96-Т «О методических рекомендациях по организации кредитными организациями внутренних процедур оценки достаточности капитала»; Положение от 16 декабря 2003 г. N 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»

Положение ЦБ РФ от 03 ноября 2009 N 346-П «Положение о порядке расчета размера операционного риска»

Письмо от 23 марта 2007г N 26-Т «О Методических рекомендациях по проведению проверки системы управления банковскими рисками в кредитной организации (ее филиале)».

Basel Committee on Banking Supervision: «Principles for the Sound Management of Operational Risk», June 2011

Приложения

В качестве приложений могут быть детальные методики и примеры; выдержки из положений регулирующих органов и лучших практик.

Приложение 1

1. Классификация по Типу рискового события

Внутреннее мошенничество – события операционного риска, возникшие как результат проведения мошеннических операций с участием **хотя бы одного сотрудника Банка**, включая действия сотрудников Банка, направленные на присвоение имущества Банка обманным путем, случаи умышленного несоблюдения законодательства, нормативных актов или внутренних распорядительных документов Банка, исключая случаи дискриминации.

Внешнее мошенничество – события операционного риска, возникшие как результат проведения мошеннических операций **третьей стороной, клиентом** (без участия сотрудников Банка), включая действия, направленные на похищение имущества, приобретение прав на имущество Банка обманным путем или нарушение действующего законодательства.

Кадровая политика и безопасность труда – события операционного риска, возникшие как результат нарушения законодательства о труде, безопасности труда и охране здоровья или в связи с выплатами по искам о нанесении личного ущерба или искам в связи с дискриминацией, а также вследствие прекращения трудовых отношений.

Клиенты, Продукты и Деловая практика – события операционного риска, возникшие как результат халатности сотрудников Банка в выполнении профессиональных обязательств по отношению к **конкретным клиентам** (включая доверительные отношения и квалификационные требования) или вследствие характера или свойств продукта. Нарушения норм и обычаев делового оборота.

Ущерб материальным (физическим) активам – события операционного риска, возникшие в результате природных катастроф или прочих внешних воздействий и вызвавшее уничтожение или снижение стоимости имущества, материальных активов Банка.

Нарушение функционирования бизнеса и сбои систем – события операционного риска, возникшие как результат нарушений в ведении бизнеса и системных сбоев Потери, как правило, вызваны недостатками и сбоями в работе аппаратного и программного обеспечения, телекоммуникаций и других систем, обеспечивающих функционирование бизнеса..

Организация, исполнение и управление процессами – события операционного риска, возникшие как результат срыва обработки операции или сбоев в процессе, либо вследствие взаимоотношений с торговыми контрагентами и поставщиками.

Более детальная классификация события в пределах семи базовых типов событий (по второму уровню и более) зависит от потребностей кредитной организации в соответствии с ее профилем операционного риска.

Приложение 2

2. Классификация рисковых событий по бизнес-линиям

Бизнес-линии
1.Corporate Finance (Корпоративное финансирование, включая муниципальное и государственное финансирование)
2.Trading & Sales (Операции и сделки на рынке ценных бумаг и срочных финансовых инструментов)
3. Retail Banking (Розничное банковское обслуживание и частное банковское обслуживание)
4. Commercial Banking (Коммерческое банковское обслуживание корпоративных клиентов)
5.Payment and Settlement (Платежи и расчеты)
6.Agency Services (Агентские услуги, депозитарий)
7.Asset Management (Управление активами)
8.Retail Brokerage (Розничное брокерское обслуживание)

3. Классификация рисковых событий по внутренним бизнес-линиям вспомогательной, сопутствующей и обеспечительной деятельности

Прямые потери		
	Наименование	**Характеристика**
.	Списания (write-downs)	прямое снижение стоимости активов в результате воровства, мошенничества, неразрешенной деятельности; или рыночные и кредитные потери, возникшие, как следствие событий операционного риска
.	Регрессные, транзакционные потери (loss of recourse)	потери по праву регресса; потери или ущерб, как следствие ошибок при проведении платежей, списаний, зачислений, выплат, транзакционных и кассовых ошибок и сбоев
.	Компенсации (restitution)	выплаты контрагентам или клиентам (включая проценты) в качестве компенсации и/или с целью примирения сторон
.	Правовая ответственность (legal liability)	платежи и потери в результате судебных решений и другие правовые расходы
.	Претензии регулирующих и надзорных органов (regulatory and compliance)	штрафы и пени, взыскания и пр.
.	Ущерб физическим активам (loss of or damage of assets)	прямое снижение стоимости физических активов, включая документы и свидетельства, в результате неблагоприятных событий (например, небрежность, авария, пожар, землетрясение)
.	Дополнительные затраты (additional expenditures)	восстановление хозяйственной деятельности, устранение последствий ошибок, аварий, стихийных бедствий
.	Прочее	
Косвенный ущерб		
	Наименование	Характеристика
.	Скрытые потери (latent losses)	упущенная выгода, недополученная прибыль, приостановка деятельности и пр.
.	Отсроченные вероятностные потери (contingent losses)	возможное возникновение прямых потерь в будущем с определенной вероятностью: судебные издержки, штрафы и пени, дополнительные затраты на восстановление хозяйственной деятельности и пр.
.	Индикативные события (near miss)	рисковые события свидетельствуют о снижении эффективности или качества процессов, увеличении трудозатрат, отсутствии или неэффективности контрольных процедур и пр.
.	Прочий косвенный ущерб	
.	Списания (write-downs)	кредитные потери, возникшие, как следствие событий операционного риска
.	Потенциальный или отложенный ущерб клиента	возможные потери, которые могли или могут возникнуть у клиента
.	Прямые потери, понесенные клиентом	реальные потери, понесенные клиентом в результате внешних угроз или сбоев в процессах клиента

4. Распределение событий операционного риска по бизнес-линиям

4.1. Бизнес-линия «Корпоративное финансирование, включая муниципальное и государственное финансирование (Corporate Finance)»

К бизнес-линии относят рисковые события, реализовавшиеся при оказании банковских услуг корпоративным клиентам, органам государственной власти и местного самоуправления на рынке капиталов: при решении задач развития бизнеса путем оптимизации структуры активов и повышения качества корпоративного управления, а также при оказании услуг при слиянии и поглощении и консультационных услуг.

Участниками бизнес-линии являются коммерческие организации, финансовые институты, государственные органы, муниципальные организации, надгосударственные органы, международные банковские институты.

4.2. Бизнес-линия «Операции и сделки на рынке ценных бумаг и срочных финансовых инструментов (Trading & Sales)»

К бизнес-линии относят рисковые события, реализовавшиеся при осуществлении операций и сделок на рынке срочных финансовых инструментов и рынке ценных бумаг Примерами событий относящихся к бизнес-линии является:

- некорректно принятое решение по причине неопытности сотрудника при отсутствии надлежащего контроля;
- ошибка при проведении расчетов;
- потери вследствие заключения плохо документированного контракта на деривати, покупаемый не через биржу и т.п.

Участниками бизнес-линии являются коммерческие организации, финансовые институты, государственные органы, муниципальные организации, надгосударственные органы.

4.3. Бизнес-линия «Розничное банковское обслуживание и частное банковское обслуживание (Retail Banking)»

К бизнес-линии относят рисковые события, реализовавшиеся при оказании розничных банковских услуг и частном банковском обслуживании, кроме брокерских и депозитарных услуг. Примерами событий относящихся к бизнес-линии могут быть:

- возврат комиссий/платы за ведение ссудного счета, оказание финансовых услуг по кредитному договору физического лица;
- неверно рассчитанная процентная ставка по кредиту или депозиту при обслуживании физического лица;
- похищение или взлом банкомата;
- обнаружение недостачи в банкоматах/платежных терминалах;
- осуществление мошеннических транзакций по поддельным пластиковым картам физических лиц;
- обнаружение недостачи денежных средств в кассе;
- выявление денежных купюр имеющих признаки подделки;
- воровство сотрудника денежных средств из кассы, с расчетных и депозитных счетов клиентов и т.п.

Участниками бизнес-линии являются физические лица[2].

[2] Учитывая лучшие мировые практики по ведению базы данных потерь, в частности ORX Association (Operational Risk Reporting Standards, Edition 2011), банки могут относить обслуживание клиентов малого и среднего бизнеса как к Retail Banking, так и к Commercial Banking. В К «Операционные риски» к Retail Banking относится обслуживание

4.4. Бизнес-линия «Коммерческое банковское обслуживание корпоративных клиентов (Commercial Banking)»

К бизнес-линии относятся рисковые события, реализовавшиеся при оказании коммерческих банковских услуг, предоставляемых юридическим лицам, включая активные, пассивные и часть комиссионных банковских операций. Примерами событий относящихся к бизнес-линии могут быть:

- неверно рассчитанная процентная ставка по кредиту или депозиту при обслуживании юридического лица;
- мошенничество при получении кредита юридическим лицом;
- осуществление мошеннических платежей в системе Клиент-Банк;
- воровство имущества находящегося в лизинге;
- неверное зачисление денежных средств при ошибочной идентификации юридического лица и т.п.

Участниками бизнес-линии являются юридические лица, а также муниципалитеты, государственные органы, международные организации.

4.5. Бизнес-линия «Платежи и расчеты (Payment and Settlement)»

К бизнес-линии относятся рисковые события, реализовавшиеся при осуществлении платежей и расчетов, кроме платежей и расчетов, осуществляемых в рамках обслуживания своих клиентов. В данной бизнес-линии Корпорация выступает как клиент либо контрагент. Примерами событий относящихся к бизнес-линии могут быть:

- уплата пени и неустоек по хозяйственным договорам за нарушение сроков уплаты платежей;
- неверно рассчитанный и уплаченный налог в бюджет;
- уплата пени и неустоек по договорам аренды;
- позднее начисление зарплаты по зараплатному проекту;

Участниками бизнес-линии являются коммерческие организации, финансовые институты, Правительство, муниципальные организации, международные организации.

4.6. Бизнес-линия «Агентские услуги и кастодиальные услуги, депозитарий (Agency Services)»

К бизнес-линии относятся рисковые события, реализовавшиеся при оказании агентских услуг и доверительном хранении активов и документов клиентов. Примерами событий относящихся к бизнес-линии могут быть:

- уплата пени за нарушение условий осуществления депозитарной деятельности;
- штрафы за неверное сегрегирование клиентских средств.

Участниками бизнес-линии являются коммерческие клиенты, финансовые институты, Правительство, муниципальные организации, международные организации.

4.7. Бизнес-линия «Управление активами (Asset Management)»

К бизнес-линии относятся рисковые события, реализовавшиеся при доверительном управлении фондами. Примером событий относящихся к бизнес-линии может быть:

- инвестирование в инструменты не включенные в договор о доверительном управлении.

Участниками бизнес-линии являются коммерческие клиенты, финансовые институты, Правительство, муниципальные организации, международные организации.

физических лиц. Обслуживание юридических лиц, в том числе малый и средний бизнес, относится к Commercial Banking.

4.8. Бизнес-линия «Розничное брокерское обслуживание (Retail Brokerage)»

К бизнес-линии относятся рисковые события, реализовавшиеся при исполнение брокерских операций и розничном брокерском обслуживание клиентов.

Примерами событий относящихся к бизнес-линии могут быть:

- неверное исполнение ордера клиента;
- обеспечение неправомерными гарантиями.

Участниками бизнес-линии являются физические и юридические лица.

5. Формула расчета инцидента

$$\text{Убыток от инцидента} = \sum_{\text{Ущерб основным средствам}} + \sum_{\text{Ущерб оборотным средствам}} + \sum_{\text{Расходы на расследование, расходы на работы по восстановлению функционирования осн. и обрт. средств}} + \sum_{\text{Расходы на операции, которые были прерваны инцидентом}} - \sum_{\text{Возмещение ущерба и страховые покрытия}}$$

где

Ущерб основным средствам	- это сумма ущерба нанесенного инцидентом всем Основным средствам В случае, если произошло полное выбытие Осн.средства ущерб равен его балансовой стоимости. При отсутствии балансовой стоимости ущерб равен стоимости нового Осн.средства, заменившего выбывшее. При отсутствии нового Осн.средства заменившего выбывшее ущерб определяется экспертным путем. В случае, если повреждение Осн.средства не повлекло его выбытия, ущерб равен стоимости запасных и ремонтных частей, которые были использованы для восстановления Осн. средства (стоимость работ по восстановлению Осн.средств рассчитываются в другом показателе).
Ущерб оборотным средствам	- это сумма ущерба нанесенного инцидентом всем Оборотным средствам Ущерб равен номинальной или балансовой стоимости выбывшего Оборотного средства. При отсутствии номинальной или балансовой стоимости, а также в случаях, когда номинальная стоимость не равна фактической ущерб определяется экспертным путем (стоимость работ по восстановлению Оборотных средств рассчитываются в другом показателе).
Расходы на расследование, расходы на работы по восстановлению функционирования осн. и обрт. средств	1) в сумму расходов на расследование инцидента включаются расходы банка на оплату труда сотрудников банка или третьих лиц по установлению обстоятельств инцидента, их фиксацию, выработку мер по восстановлению функционирования основных и оборотных средств. 2) в сумму расходов на работы по восстановлению функционирования основных и оборотных средств включаются расходы банка на оплату труда сотрудников банка или третьих лиц 1, занимавшихся восстановлением Основных и Оборотных средств
Расходы на операции, которые были прерваны инцидентом	- это сумма включающая в себя: 1. Расходы банка на оплату труда сотрудников банка или третьих лиц, исполнявших операцию прерванную инцидентом1 2. Расходы банка на ресурсы, использованные банком или третьими лицами для исполнения операции, прерванной инцидентом3 В сумму включаются расходы только на те операции и процессы, прерванные инцидентом, которые в последующем были проведены заново, или от проведения которых отказались в виду их нецелесообразности.
Возмещение ущерба и страховые покрытия	- это сумма полученная банком 1) от виновников инцидентов (в рамках покрытия ими убытков от совершенных ими действий) - физических и юридических лиц или органов государства выплаченная ими добровольно или по решению суда; 2) и от страховых компаний (в рамках покрытия ими убытков от произошедшего инцидента во исполнение условий договоров, ранее заключенных с банком)

[3] Стоимость ресурсов использованных банком для исполнения операции, прерванной инцидентом определяется экспертным путем.

6. OPERATIONAL RISK TEMPLATES

6.1. OPR – Operational Risk

This template provides information on the capital requirements for Operational Risk under the Basic Indicator Approach (BIA), the Standardized Approach (STA), the Alternative Standardized Approach (ASA) and the Advanced Measurement Approaches (AMA).

For the AMA, information on the use of an allocation mechanism and the capital alleviation because of insurance and other risk transfer mechanisms is also requested.

6.2. OPR Details – Operational Risk: Gross Losses by Business Lines and Event Types in the last year

This template summarizes the information (number of events, total loss amount and maximum single loss) on the gross losses suffered by the bank in the last year according to event types and/or business lines.

6.3. OPR LOSS Details – Major Operational Risk Losses recorded in the last year or which are still open.

This template provides information on the major operational risk losses recorded in the last year on a gross and net basis along with the status of whether they are ended or still open. It allows a monitoring of those losses above a threshold designated by the competent authorities, and provides information on the nature of the operational losses (event types) and on their location by business lines, as well as effectiveness of the hedging techniques used

Директива о требованиях к капиталу - The **Capital Requirements Directive (CRD)** for the financial services industry will introduce a supervisory framework in the EU which reflects the Basel II rules on capital measurement and capital standards.

7. Требования к организации системы управления непрерывностью бизнеса, которым должен удовлетворять банк, в зависимости от выбранного банком метода расчета капитала под операционный риск: метод базового индикатора, стандартизованный метод, продвинутый метод

Справочно:

В качестве требований, предъявляемых к организации системы управления непрерывностью бизнеса, предлагается использовать требования Стандарта «Система управления непрерывностью деятельности кредитных организаций банковской системы Российской Федерации», утв. Советом АРБ от 16.12.2010.

Таблица ниже составлена на базе Приложения №5 («Уровни зрелости») к стандарту, при этом, однако, распределение требований по выбранным методам расчета в ряде случаев отличается от предлагаемого Приложением распределения по уровням зрелости.

В используемой нотации "+" означает, что при выборе данного метода оценки капитала под операционный риск банк обязан соответствовать указанному в столбце 2 требованию. Пустая графа говорит о том, что при выборе данного метода оценки капитала под операционный риск соблюдение указанного в столбце 2 требования не является обязательным.

№ пункта стан-дарта	Требование к системе управления непрерывностью деятельности (с указанием номеров пунктов стандарта)	Необходимость соответствия кред. организации требованию в зависимости от выбранного метода оценки капитала под опер. риск		
		Базовый подход	Стандар-тизован-ный подход	Продви-нутый подход
1	2	3	4	5
1.	Планирование системы			
4.1	Корпоративная политика в области обеспечения НД			
4.1.1.1	В кредитной организации определена область деятельности и цели системы управления непрерывностью деятельности	+	+	+
4.1.2	В кредитной организации существует политика обеспечения НД, утвержденная Советом Директоров		+	+
4.1.2.3. 2)	Политика доведена до сведения всех сотрудников кредитной организации или работающих от ее имени		+	+
4.1.2.3. 3)	Политика регулярно пересматривается		+	+
4.2	Выделение ресурсов для управления и реализацией системы			
4.2.1.1	В кредитной организации существуют необходимые ресурсы для обеспечения непрерывности и восстановления деятельности		+	+
4.2.1.2	Роли и ответственность персонала, участвующего в создании, управлении и реализации системы должны быть четко определены и документированы		+	+
4.2.2.1	В кредитной организации сформирована группа под руководством назначенного сотрудника, ответственная за управление системой		+	+

№ пункта стан-дарта	Требование к системе управления непрерывностью деятельности (с указанием номеров пунктов стандарта)	Необходимость соответствия кред. организации требованию в зависимости от выбранного метода оценки капитала под опер. риск		
		Базовый подход	Стандар-тизован-ный подход	Продви-нутый подход
4.2.2.2	Назначенный сотрудник обладает соответствующим полномочиями и влиянием		+	+
4.2.3	В кредитной организации сформирована исполнительная группа, ответственная за внедрение и поддержание системы		+	+
4.2.4. 1)	Кредитная организация выявляет необходимые компетенции ответственных сотрудников			+
4.2.4. 2)	Кредитная организация оценивает необходимость обучения		+	+
4.2.4. 3)	Кредитная организация проводит обучение сотрудников		+	+
4.2.4. 4)	В кредитной организации осуществлена проверка того, что полученные знания достигнуты			+
4.2.4. 5)	Кредитная сохраняет записи об образовании, обучении, навыках, опыте и квалификации			+
2. Исполнение системы				
5.1	Исследование кредитной организации			
5.1	В кредитной организации определен и документирован метод оценки влияния на бизнес		+	+
5.1.1	Анализ влияния на бизнес производится кредитной организацией с учетом принятых обязательств (в т.ч. и законодательных требований)		+	+
5.1.1.1. 1)	В кредитной организации проводится оценка нарастающего объема потерь в связи с неспособностью исполнить принятые на себя обязательства	+	+	+
5.1.1.1. 2)	В кредитной организации установлено максимально допустимое время простоя критичных продуктов и услуг		+	+
5.1.1.1. 3)	В кредитной организации выявлены виды деятельности, необходимые для предоставления критичных продуктов и услуг	+	+	+
5.1.1.1. 4-5)	В кредитной организации определен нормальный и аварийный уровень ресурсов, необходимых для работы в штатном и аварийном режимах работы		+	+
5.1.1.1. 6)	В кредитной организации определено целевое время восстановления видов деятельности, от которых зависит предоставление критичных продуктов и услуг	+	+	+
5.1.1.1. 6)	Установленное целевое время меньше максимально допустимое время простоя соответствующего продукта или услуги		+	+
5.1.1.1. 7)	Определено время восстановления критичных видов деятельности до нормального (штатного) уровня		+	+
5.1.1.1. 8)	В кредитной организации определены критические виды деятельности, подлежащие первоочередному восстановлению	+	+	+

№ пункта стан-дарта	Требование к системе управления непрерывностью деятельности (с указанием номеров пунктов стандарта)	Необходимость соответствия кред. организации требованию в зависимости от выбранного метода оценки капитала под опер. риск		
		Базовый подход	Стандар-тизован-ный подход	Продви-нутый подход
5.1.1.1. 9-10)	В кредитной организации ведется список поставщиков, от которых зависят критические виды деятельности, а также внедренных у них мер управления непрерывностью деятельности		+	+
5.1.1.2. 1)	В кредитной организации определен персонал, необходимый для работы в нормальном и аварийном режимах	+	+	+
5.1.1.2. 2)	В кредитной организации определены помещения для работы в нормальном и аварийном режиме	+	+	+
5.1.1.2. 3)	В кредитной организации определен перечень информационно-коммуникационных технологических услуг, необходимый для работы в аварийном режиме		+	+
5.1.1.2. 4)	В кредитной организации определен допустимый размер потерь информации		+	+
5.1.1.2. 5)	В кредитной организации определен список поставщиков и видов снабжения, от которых зависят критические виды деятельности		+	+
5.1.1.2. 6)	В кредитной организации определен объем резерва ликвидных средств, необходимый для поддержания ликвидности на время устранения последствий инцидента (в т.ч. из-за потери деловой репутации, вызванной инцидентом)	+	+	+
5.1.1.3. 1)	В кредитной организации определены информационно-коммуникационные технологические услуги		+	+
5.1.1.3. 2)	Время восстановления информационно-коммуникационной технологической услуги не превышает время восстановления критичного вида деятельности		+	+
5.1.1.3. 3)	Список критичных информационно-коммуникационных технологических услуг согласован с руководящим системой управления непрерывности деятельности органом		+	+
5.1.1.3. 4)	Структура и компоненты информационно-коммуникационных технологических услуг в штатном и аварийном режимах работы определены и документированы			+
5.1.2	В кредитной организации проводится анализ рисков чрезвычайных ситуаций	+	+	+
5.1.2.2	Кредитная организация классифицирует риски согласно положению Правительства РФ №304 от 21.05.2007			+
5.1.2.3. 1)	Кредитная организация рассматривает сценарии недоступности ключевых или большого числа		+	+

№ пункта стан-дарта	Требование к системе управления непрерывностью деятельности (с указанием номеров пунктов стандарта)	Необходимость соответствия кред. организации требованию в зависимости от выбранного метода оценки капитала под опер. риск		
		Базовый подход	Стандар-тизован-ный подход	Продви-нутый подход
	сотрудников			
5.1.2.3. 2)	Кредитная организация рассматривает сценарии выхода из строя технических средств и информационных систем	+	+	+
5.1.2.3. 3)	Кредитная организация рассматривает сценарии нарушения коммунальной инфраструктуры (в т.ч. перебои с электроснабжением)	+	+	+
5.1.2.3. 4)	Кредитная организация рассматривает сценарии блокировки доступа к зданию	+	+	+
5.1.2.3. 5)	Кредитная организация рассматривает сценарии отказа кредитных организаций-корреспондентов и поставщиков услуг от исполнения своих обязательств	+	+	+
5.1.2.3. 6)	Кредитная организация рассматривает сценарии недоступности ключевой информации		+	+
5.1.2.4	Кредитная организация выделяет риски, которыми готова управлять самостоятельно		+	+
5.1.3	Результаты анализа влияния на бизнес и анализа рисков утверждены Правлением кредитной организации			+
5.2	Выбор мер управления рисками чрезвычайных ситуаций			
5.2.2	В кредитной организации определены схемы по поддержанию ключевых знаний и компетенций			+
5.2.3	В кредитной организации определены схемы использования запасных помещений в аварийном режиме		+	+
5.2.4	В кредитной организации определены меры по поддержанию работоспособности технических средств и информационных систем в случае выхода их из строя.	+	+	+
5.2.4	Для каждой информационно-коммуникационной технологической услуги определена свой вариант восстановления			+
5.2.5	В кредитной организации определены меры резервирования и восстановления данных (включая документы), в т.ч. периодичность создания копий, методы хранения и защиты, схемы доставки и восстановления	+	+	+
5.2.6	В кредитной организации определены меры в случае отказа кредитных организаций-корреспондентов и внешних поставщиков от выполнения своих обязательств, в т.ч. меры по поддержанию коммунальной инфраструктуры (например, электро, тепло, водоснабжения).	+	+	+
5.2.7	В кредитной организации определены меры поддержания ликвидности (меры обеспечения доступности резерва ликвидных средств),	+	+	+

№ пункта стан-дарта	Требование к системе управления непрерывностью деятельности (с указанием номеров пунктов стандарта)	Необходимость соответствия кред. организации требованию в зависимости от выбранного метода оценки капитала под опер. риск		
		Базовый подход	Стандар-тизован-ный подход	Продви-нутый подход
	необходимых для выполнения своих обязательств по предоставлению критических продуктов и услуг и поддержания минимально допустимого уровня ликвидности на время ликвидации последствий инцидента (в т.ч. договоры об оказании финансовой помощи)			
5.2.8	Меры управления рисками чрезвычайных ситуаций утверждены советом директоров кредитной организации			+
5.3	Реализация выбранных мер			
5.3.1.1	В кредитной организации сформированы орган чрезвычайного управления		+	+
5.3.1.1. 1-3)	В кредитной организации орган чрезвычайного управления подтверждает характер и масштаб инцидента, берет на себя первичный контроль (до приезда экстренных служб), организует сдерживание/подавление инцидента			+
5.3.1.1. 4)	Кредитная организация обеспечивает своевременное информирование всех заинтересованных сторон о возникновении инцидента.	+	+	+
5.3.1.1. 5)	Кредитная организация обеспечивает взаимодействие с банком России в ходе ликвидации инцидента	+	+	+
5.3.1.1. 6-7)	Кредитная организация взаимодействует с внешними экстренными и коммунальными службами в ходе локализации и устранения инцидента		+	+
5.3.1.1. 8)	Соответствующий план ОНиВД активируется в рамках аварийно-спасательных работ органом чрезвычайного управления			+
5.3.1.2	Сотрудники, входящие в состав органа чрезвычайного управления, обладают соответствующими компетенциями и полномочиями		+	+
5.3.2	В кредитной организации существуют планы экстренного реагирования, доступные соответствующим сотрудникам	+	+	+
5.3.2.3. 1-3,5)	Планы экстренного реагирования имеют цели, задачи, доступны целевой аудитории, написаны кратко и ясно, а также согласованы с действиями внешних организаций.	+	+	+
5.3.2.3. 4)	В кредитной организации определены роли и ответственность персонала, участвующего в управлении инцидентом		+	+
5.3.2.3. 6)	В кредитной организации определен порядок активации плана экстренного реагирования		+	+
5.3.2.3. 7)	Кредитная организация устанавливает порядок оповещения заинтересованных сторон (в т.ч.	+	+	+

№ пункта стан-дарта	Требование к системе управления непрерывностью деятельности (с указанием номеров пунктов стандарта)	Необходимость соответствия кред. организации требованию в зависимости от выбранного метода оценки капитала под опер. риск		
		Базовый подход	Стандар-тизован-ный подход	Продви-нутый подход
	регуляторов, внутренних сотрудников банка) о возникновении инцидента			
5.3.2.3. 9)	В кредитной организации установлен порядок действий по управлению инцидентами			+
5.3.2.3. 10)	Планы экстренного реагирования включают все необходимые детали		+	+
5.3.2.3. 11)	Кредитная организация определяет схему взаимодействия со средствами массовой информации в случае возникновения инцидента во избежание потери репутации.		+	+
5.3.2.3. 12)	Планы экстренного реагирования содержат метод регистрации ключевой информации об инциденте, принятых решениях и принятых мерах;			+
5.3.2.3. 13)	Планы экстренного реагирования содержат схему отмены тревоги и демобилизацию ответственного персонала		+	+
5.3.2.3. 14)	В кредитной организации назначен сотрудник, ответственный за поддержание и пересмотр плана экстренного реагирования (владелец плана)		+	+
5.3.2.3. 15)	План экстренного реагирования утвержден руководящим системой УНД органом		+	+
5.3.3	В кредитной организации существуют планы ОНиВД, доступные соответствующим сотрудникам	+	+	+
5.3.3.3. 1-4)	Планы ОНиВД доступны, просты, имеют цели и область применения, согласованы с действиями внешних организаций		+	+
5.3.3.3. 5)	Кредитная организация определяет роли и ответственность персонала, участвующего в восстановлении деятельности кредитной организации и в обеспечении ее работы в чрезвычайном режиме		+	+
5.3.3.3. 6)	В кредитной организации определен порядок активации Плана ОНИВД	+	+	+
5.3.3.3. 7)	Кредитная организация определяет схему аварийных коммуникаций при активации и задействовании плана ОНиВД	+	+	+
5.3.3.3. 8)	Кредитная организация устанавливает требования к минимальному объему ресурсов, необходимому в различные моменты времени для восстановления и аварийного предоставления критичных продуктов и услуг		+	+
5.3.3.3. 9)	Кредитная организация определяет последовательность действий для восстановления нарушенной деятельности и поддержанием ее в аварийном режиме (включая восстановление и предоставление информационно-технологических услуг)	+	+	+
5.3.3.3.	Планы ОНиВД содержат всю необходимую		+	+

№ пункта стан-дарта	Требование к системе управления непрерывностью деятельности (с указанием номеров пунктов стандарта)	Необходимость соответствия кред. организации требованию в зависимости от выбранного метода оценки капитала под опер. риск		
		Базовый подход	Стандар-тизован-ный подход	Продви-нутый подход
10-11)	информацию и схему регистрации ключевой информации о ходе работ, принятых решениях и принятых мерах			
5.3.3.3. 12)	В кредитной организации определена схема отмены чрезвычайного режима работы		+	+
5.3.3.3. 13)	В кредитной организации выделены сотрудники, ответственные за поддержание и пересмотр планов ОНиВД (владельцы планов)		+	+
5.3.3.3. 14)	Планы ОНиВД утверждены руководящим системой управления непрерывностью деятельности органом		+	+
5.4	Документация и записи системы			
5.4. 1)	В кредитной организации документированы цели и охват системы управления непрерывностью деятельности		+	+
5.4. 2)	В кредитной организации существует политика системы управления непрерывностью деятельности	+	+	+
5.4. 3)	В кредитной организации документированы свидетельства выделения ресурсов			+
5.4. 4,11)	В кредитной организации существует программа обучения и свидетельства ее выполнения		+	+
5.4. 5)	В кредитной организации существует отчет о проведенном анализе влияния на бизнес		+	+
5.4. 6)	В кредитной организации существует отчет об анализе рисков		+	+
5.4. 7)	В кредитной организации выбраны меры управления рисками чрезвычайных ситуаций		+	+
5.4. 8)	В кредитной организации существует документальные свидетельства формирования и функционирования органа чрезвычайного управления		+	+
5.4. 9)	В кредитной организации существуют планы экстренного реагирования	+	+	+
5.4. 10)	В кредитной организации существуют планы ОНиВД	+	+	+
5.4. 12)	В кредитной организации существует документальные свидетельства пересмотра системы со стороны Правления			+
5.4. 13)	В кредитной организации существуют программы и планы внутреннего аудита		+	+
5.4. 14)	В кредитной организации существуют программы и планы тестирования		+	+
5.4. 15)	В кредитной организации существует документальные свидетельства извлечения уроков и выявления лучших практик			+
5.5	Контроль документации и записей системы			
5.5	В кредитной организации установлены механизмы контроля документации и записей системы		+	+

№ пункта стан-дарта	Требование к системе управления непрерывностью деятельности (с указанием номеров пунктов стандарта)	Необходимость соответствия кред. организации требованию в зависимости от выбранного метода оценки капитала под опер. риск		
		Базовый подход	Стандар-тизован-ный подход	Продви-нутый подход
3. Контроль и улучшение системы				
6.1	Повышение осведомленности сотрудников			
6.1	Кредитная организация проводит регулярное обучение сотрудников в области непренывности деятельности		+	+
6.2	Пересмотр системы Правлением кредитной организации			
6.2	Правление кредитной организации регулярно пересматривает меры управления непрерывностью деятельности			+
6.2.3	По результатам пересмотра проводятся меры по улучшению системы			+
6.3	Самооценка и Внутренний аудит			
6.3.1.1-2	Кредитная организация проводит регулярные внутренние аудиты системы управления непрерывностью деятельности		+	+
6.3.1.2	Руководство знакомится с результатами аудита для принятия соответствующих мер		+	+
6.3.1.3	Кредитная организация разрабатывает и поддерживает процедуру и программу аудитов			+
6.4	Тестирование планов			
6.4.1	Кредитная организация проводит регулярное тестирование планов экстренного реагирования и планов ОНиВД	+	+	+
6.4.2	Тесты, в совокупности, охватывают всю систему управления непрерывностью деятельности			+
6.4.2. 2)	В кредитной организации установлена программа проведения тестов			+
6.4.2. 5)	В кредитной организации четко определены цели каждого теста		+	+
6.4.2. 6)	В кредитной организации определена группа наблюдателей, следящих за ходом тестирования			+
6.4.2. 7)	Кредитная организация готовит отчет о проведении каждого теста		+	+
6.5	Извлечение уроков и выявление лучших практик			
6.5.1	Кредитная организация проводит анализ инцидентов, происшедших во время проведения тестирования		+	+
6.5.2	Кредитная организация извлекает уроки из происшествия и проводит соответствующие улучшения		+	+
6.5.3	Кредитная организация стремится к применению лучших мировых практик в области обеспечения непрерывности деятельности.		+	+
6.6	Упреждающие и корректирующие действия			
6.6	В кредитной организации внедрены механизмы упреждающих и корректирующих действий			+