

20.07.2012 № 23-14/40

Банки

Структурные подразделения  
Национального банка  
Республики Беларусь  
(по списку)

О совершенствовании  
управления операционным  
риском в банках

Национальный банк в рамках осуществления надзора за деятельностью банков проводит регулярную оценку систем управления рисками в банках и уровня этих рисков. В целях изучения состояния систем управления операционным риском (далее – СУОР) банков Национальный банк в апреле 2012 г. провел анкетирование банковской системы по вопросам управления операционным риском.

Результаты анкетирования показали, что в целом органы управления банков осознают существенность воздействия операционного риска на деятельность банка и необходимость дальнейшего совершенствования подходов к управлению данным риском. В этих целях в банках созданы и периодически пересматриваются соответствующие локальные нормативные правовые акты (далее – ЛНПА) и процедуры управления операционным риском. В рамках данных процедур наблюдается активизация работы по описанию бизнес-процессов банков, а также классификации деятельности по направлениям (бизнес-линиям). Банки стремятся к оценке (измерению) реальной величины присущего им операционного риска и проявляют все больший интерес к созданию и использованию общей внешней базы данных операционных инцидентов на приемлемых условиях. Во многих банках определены индикаторы операционного риска, созданы соответствующие механизмы отчетности, осуществляется контроль операционного риска. Разработанные в банках планы действий на случай непредвиденных обстоятельств охватывают основные области

проявления операционного риска, приводящего к нарушению непрерывности деятельности банка. Наблюдается также активизация работы по проведению банками стресс-тестирования операционного риска.

Вместе с тем анализ результатов анкетирования выявил ряд следующих недостатков:

отсутствие в некоторых банках стратегии управления рисками, в том числе операционным;

отсутствие в большинстве банков (56%) установленного допустимого (безопасного) уровня операционного риска (далее – толерантности к риску), а среди банков, установивших его, – отсутствие в большинстве случаев (57%) отражения данного уровня в стратегии управления рисками, в том числе операционным;

отсутствие в большинстве банков (66%) автоматизированных систем учета, измерения, расчета величины операционного риска и составления итоговой агрегированной пруденциальной и управленческой отчетности по нему;

отсутствие в некоторых банках организации соответствующего профессионального обучения специалистов, ответственных за управление операционным риском, в то время как в целом по банковской системе (примерно в 50% случаев) опыт работы таких специалистов в области управления рисками является непродолжительным (1 – 3 года);

отсутствие в различных банках организации работы по таким направлениям совершенствования СУОР, как описание бизнес-процессов и выделение направлений деятельности, разработка детальной классификации (кодификации) операционных инцидентов; принятие мер реагирования на операционные инциденты, использование внешних источников информации об операционных инцидентах; оценка операционного риска, в том числе с использованием нескольких различных методов оценки; ограничение (снижение) и контроль принимаемых банками рисков в сфере банковских информационных технологий (далее – ИТ-рисков); создание и пересмотр сценариев стресс-тестирования; создание, тестирование и пересмотр планов действий на случай непредвиденных обстоятельств; проведение независимой оценки СУОР банков внутренним и (или) внешним аудитом;

отсутствие в некоторых банках, использующих аутсорсинг, подходов к управлению связанным с ним риском, предусматривающих совершенствование ЛНПА банка, формирование отчетности, ограничение (снижение) и контроль такого риска, создание сценариев

стресс-тестирования, а также оценку качества управления риском, связанным с аутсорсингом, в процессе проведения внутреннего аудита;

отсутствие в большинстве банков (53%) при определении направлений совершенствования СУОР оценки (анализа) эффективности предполагаемых расходов.

Быстрое развитие рынка банковских услуг, появление большого количества новых банковских продуктов, основанных в том числе на использовании сложных современных информационных технологий, развитие сетей банков, возрастающий темп роста банковских активов, увеличение объемов банковских операций и количества операционных инцидентов в банках, обуславливающие рост принимаемого банками операционного риска, требуют принятия соответствующих мер по преодолению выявленных недостатков, что предполагает дальнейшее совершенствование СУОР банков, а также подходов к управлению операционным риском.

Для достижения этих целей, предусматривающих создание эффективно функционирующей СУОР, банкам следует руководствоваться требованиями к организации управления рисками в банках, установленными в нормативных правовых актах Национального банка, рекомендациями, изложенными в письмах Национального банка об организации систем управления рисками в банках, о совершенствовании управления рисками, связанными с аутсорсингом в сфере финансовых услуг, и о совершенствовании практики стресс-тестирования, а также приведенными ниже рекомендациями. Помимо этого, банкам целесообразно учитывать наилучшую международную практику управления операционным риском, обобщенную в обновленном документе Базельского комитета по банковскому надзору "Принципы надлежащего управления операционным риском". В связи с этим, Национальный банк направляет неофициальный перевод документа "Principles for the sound management of operational risk", оригинальный текст которого доступен на сайте Банка международных расчетов [www.bis.org](http://www.bis.org) в глобальной компьютерной сети Интернет.

По мнению Национального банка, надлежащим образом сформированная СУОР предусматривает решение следующих задач:

создание надлежащей организационной структуры СУОР;

интеграция СУОР в общую систему управления рисками банка, внутреннего контроля и корпоративного управления;

разработка соответствующих ЛНПА по управлению операционным риском;

создание и использование эффективных процедур управления операционным риском;

проведение периодической и независимой проверки (оценки) эффективности СУОР;

раскрытие соответствующей информации об управлении операционным риском в банке.

Ответственность за организацию СУОР несет совет директоров банка (наблюдательный совет), осуществляющий общее руководство созданием такой системы путем определения принципов и подходов к управлению операционным риском. Совет директоров (наблюдательный совет) утверждает стратегию управления рисками банка, в том числе операционным, а также определяет толерантность к риску с учетом текущего финансового положения банка и осуществляемых им видов деятельности.

Снижению вероятности возникновения потерь от операционных инцидентов, улучшению работы по предотвращению их последствий, а также улучшению контроля операционного риска способствует внедрение и поддержание во всех подразделениях банка корпоративной культуры управления операционным риском. С этой целью совету директоров (наблюдательному совету) следует утвердить кодекс профессиональной этики и определить стандарты профессионального и ответственного поведения, а также инструменты мотивации сотрудников банка.

Совет директоров (наблюдательный совет) контролирует деятельность исполнительного органа банка, ответственного за разработку, внедрение и поддержание во всех структурных подразделениях банка последовательных, детализированных политики, методики и процедур управления операционным риском. В свою очередь, исполнительный орган в процессе практического внедрения СУОР в соответствии с утвержденной советом директоров (наблюдательным советом) стратегией разрабатывает ЛНПА банка по управлению операционным риском, устанавливает четкое распределение ответственности, полномочий, а также порядок их осуществления, организует систему информационных потоков и определяет механизмы взаимодействия между структурными подразделениями банка и порядок принятия решений, исключающие возникновение конфликта интересов.

Исполнительный орган формирует организационную структуру СУОР с учетом размера и организационно-функциональной структуры банка, а также масштабов и особенностей осуществляемых банком операций и видов деятельности.

В небольших банках с простой организационно-функциональной структурой целесообразно использовать в максимальной степени

централизованную модель управления, предусматривающую сосредоточение функций управления операционным риском в рамках отдельного специального подразделения по управлению рисками. В более крупных банках со сложной организационно-функциональной структурой наряду с другими профильными подразделениями по управлению отдельными видами риска может создаваться профильное подразделение и (или) назначаться должностное лицо, ответственное за управление операционным риском. При этом для обеспечения возможности получения целостного представления о риск-профиле банка целесообразно предусмотреть создание централизованного подразделения по управлению рисками банка в целом, координирующего деятельность профильных подразделений по управлению отдельными рисками, в том числе операционным.

Вне зависимости от используемой модели организации управления операционным риском банк может назначать должностных лиц, координирующих управление данным риском в различных подразделениях банка. Такие лица могут назначаться как из числа сотрудников данных подразделений, так и из числа специалистов подразделения по управлению рисками банка (профильного подразделения по управлению операционным риском).

В соответствии с лучшей международной практикой при совете директоров (наблюдательном совете) целесообразно создать комитет по рискам, в функции которого входят общее руководство и обеспечение деятельности системы управления рисками в банке в целом и, в частности, СУОР.

Комитет по рискам, как правило, возглавляет лицо, обладающее достаточной компетенцией в области управления рисками и являющееся независимым директором. В состав такого комитета могут входить как члены совета директоров (наблюдательного совета), так и иные лица, обладающие достаточной квалификацией и опытом в области управления бизнесом, финансами, управления рисками, в том числе должностное лицо, ответственное за управление рисками в банке, а также должностное лицо, ответственное за управление операционным риском, если такое должностное лицо в банке назначено.

Для эффективного функционирования СУОР банк должен быть обеспечен необходимыми техническими средствами, оборудованием, современными компьютерными системами и технологиями. Это предполагает осуществление соответствующих инвестиций в технологическую и техническую инфраструктуру как на первом этапе построения СУОР, так и в процессе ее функционирования, предусматривая своевременное обновление и замену устаревших

технологий, технических средств и программного обеспечения. Кроме того, к управлению операционным риском следует привлекать достаточное количество сотрудников, имеющих необходимый опыт, квалификацию, а также технические навыки. Данных сотрудников необходимо наделить соответствующими полномочиями, в том числе предусматривающими право выносить суждение о необходимости ограничения или отказа от принятия операционного риска в процессе принятия руководством банка управленческих решений. К тому же необходимо предусмотреть надлежащее обучение сотрудников банка по вопросам управления операционным риском. Обучение следует проводить на всех уровнях организационной структуры банка в соответствии с занимаемой должностью и исполняемыми обязанностями сотрудников. При этом целесообразно организовать работу по получению руководителями и (или) специалистами банка, непосредственной обязанностью которых является управление операционным риском, сертификатов международного образца в области управления рисками (например, сертификаты Professional Risk Manager, Financial Risk Manager).

Построение СУОР следует осуществлять в неразрывной связи с процессами управления другими рисками на всех уровнях организационной структуры банка. Эффективное взаимодействие специалистов, ответственных за управление операционным, кредитным, рыночным и другими рисками банка, а также лиц, ответственных за приобретение услуг третьей стороны (например, в случае аутсорсинга), позволяет предотвратить несогласованность и дублирование в управлении рисками. Помимо этого, при интеграции СУОР в общую систему управления рисками необходимо предусмотреть интегрированный подход к управлению рисками новых банковских продуктов, видов деятельности, процессов и систем.

Составной частью общей системы управления рисками являются также эффективная оценка и всесторонний внутренний контроль функционирования СУОР, что предполагает утверждение советом директоров (наблюдательным советом) банка соответствующих процедур контроля за СУОР, исключающих возникновение конфликта интересов в деятельности банка между подразделениями (должностными лицами), генерирующими операционный риск, и подразделениями (должностными лицами), осуществляющими контроль за ним.

Организационную структуру СУОР, политику, методiku и процедуры управления операционным риском необходимо закрепить в соответствующих ЛНПА банка, в которых также следует отразить

систему терминов и определений, используемых при управлении операционным риском; определить толерантность банка к риску; политики, методики и процедуры управления риском новых банковских продуктов, видов деятельности, процессов и систем, ИТ-риском и риском, связанным с аутсорсингом; случаи и периодичность пересмотра и изменения политики управления операционным риском банка.

В целях создания и использования эффективных процедур управления операционным риском банку необходимо предусмотреть надлежащую организацию процессов выявления (идентификации) и оценки (измерения), мониторинга, формирования отчетности, ограничения (снижения), контроля, стресс-тестирования операционного риска, а также обеспечения непрерывности деятельности банка.

Первым этапом управления операционным риском в банке является выявление (идентификация) риска. Данная процедура способствует своевременному обнаружению потенциально уязвимых к воздействию операционного риска участков деятельности банка и предусматривает организацию работы по следующим направлениям:

классификация источников операционного риска, а также разработка детальной классификации операционных инцидентов;

определение направлений деятельности (бизнес-линий) банка и классификация по ним деятельности банка;

определение критериев отнесения того или иного инцидента к конкретному классу операционных инцидентов, в том числе к нескольким классам, а также направлениям деятельности (бизнес-линиям) в соответствующей доле;

составление карты бизнес-процессов банка и описание каждого входящего в нее бизнес-процесса.

Выявление (идентификацию) операционных рисков необходимо осуществлять на всех этапах деятельности банка, начиная с определения банком своих стратегических целей и установления целевых параметров и ориентиров деятельности, с учетом как внутренних, так и внешних факторов возникновения операционного риска.

К внутренним факторам относятся специализация банка, профессиональный уровень работников, надежность организации документооборота, защита и предотвращение утечки информации и иные факторы, обусловленные деятельностью банка.

К внешним факторам относятся изменения в правовом регулировании, поведение клиентов, надежность контрагентов, воздействие технологического прогресса на безопасность банковских операций и иные факторы, не зависящие от деятельности банка.

На следующем этапе управления операционным риском проводится его оценка, которая представляет собой анализ информации о вероятности наступления операционных инцидентов и потерь от операционных инцидентов. На основе использования различных методов данной оценки проводится количественное измерение операционного риска, присущего деятельности банка. Банк может самостоятельно разрабатывать методы оценки риска или использовать следующие методы, наиболее часто применяемые в международной банковской практике:

- статистические;
- балльно-весовые;
- моделирование (сценарный анализ).

Статистические методы оценки основаны на анализе распределения потерь банка от операционных инцидентов и позволяют сделать прогноз возможных потерь банка, исходя из ретроспективного анализа размеров ранее понесенных банком потерь от операционных инцидентов. При применении этих методов в качестве исходных данных используется информация, накопленная в аналитической базе данных операционных инцидентов банка.

Балльно-весовые методы предполагают проведение самооценки риска банка, а также самооценки контроля риска.

Самооценка риска предусматривает оценку процессов, лежащих в основе операций банка, на наличие слабых мест и недостатков, способных привести к возникновению операционного риска, с учетом возможных последствий его воздействия.

Сущность самооценки контроля риска заключается в оценке операционного риска в сопоставлении с мерами по его контролю и ограничению (снижению). При этом сравниваются величины присущего и остаточного операционного риска банка, то есть риска до и после установления мер по его контролю и ограничению (снижению), что позволяет оценить эффективность использования данных мер.

В обоих случаях предполагается определение относительной значимости информативных показателей, выбранных в процессе проведения самооценки, путем анкетирования сотрудников банка и (или) на основе вынесения мотивированного суждения экспертов. Показатели сводятся в таблицы и оцениваются с использованием различных шкал перевода полученных оценок значимости показателей в баллы (например, в зависимости от суммы возможных потерь, вероятности возникновения потерь, надежности применяемых процедур контроля). В результате обработки полученных баллов определяются итоговые оценки, на основании чего составляются карты операционного



риска в различных разрезах: по подразделениям, направлениям деятельности (бизнес-линиям), бизнес-процессам, отдельным операциям банка, а также в других разрезах в зависимости от установленных целей проведения самооценки.

В рамках метода моделирования (сценарного анализа) на основе экспертного анализа определяются возможные сценарии возникновения инцидентов или обстоятельств, приводящих к потерям, после чего разрабатывается модель распределения частоты возникновения и размеров убытков, которая используется для оценки операционного риска. Моделирование, как и другие методы оценки операционного риска, может осуществляться в различных разрезах, а также предполагает использование результатов проводимого в банке стресс-тестирования операционного риска.

С целью получения более полного представления о риск-профиле банка целесообразно использовать различные методы оценки операционного риска, проводить сравнительный анализ результатов их применения, а также анализ результатов проверок аудита (как внутреннего, так и внешнего). Кроме того, банк может сравнивать полученные количественные оценки операционного риска с возникающими в дальнейшей деятельности банка потерями от операционных инцидентов, что позволяет определить эффективность процесса оценки операционного риска, а также используемых процедур контроля. Банк также может проводить сравнение количественных оценок операционного риска с его расчетной величиной с целью определения точности оценки размера операционного риска при расчете достаточности капитала, а также определения размера завышения или занижения требований к капиталу на покрытие операционного риска. На основании такого анализа банком может приниматься решение о целесообразности перехода к применению более сложного метода расчета величины операционного риска. В общем случае, несмотря на то, что использование более сложных подходов является более затратным для банка, оно позволяет снизить требования к капиталу на покрытие операционного риска, повышает эффективность управления данным риском, а также точность прогнозирования возможных потерь от операционных инцидентов.

Важной составляющей эффективной СУОР является мониторинг операционного риска, предоставляющий возможность быстрого выявления и исправления недостатков в политике, процессах и процедурах управления операционным риском. Мониторинг заключается в проведении в постоянном режиме на всех уровнях организационной структуры банка работы по сбору и анализу

информации о потерях от операционных инцидентов, возникающих в деятельности банка, что достигается путем создания и ведения внутренней базы данных банка об операционных инцидентах.

В процессе формирования такой базы данных целесообразно организовать работу по восстановлению информации об инцидентах и потерях, возникших в банке в прошлые периоды деятельности, до начала осуществления сбора данных о потерях от операционных инцидентов. Кроме того, следует собирать сведения о таких потерях из внешних источников информации. Банку следует по мере возможности совершать обмен данными о возникновении потерь с другими банками, анализировать соответствующую информацию, полученную в том числе из внешних баз данных, которые предоставляют наиболее полную и актуальную информацию о внешних операционных инцидентах и потерях, а также средств массовой информации. Сбор и анализ таких данных предоставляет дополнительную информацию о последствиях операционных инцидентов, ранее не возникавших в деятельности самого банка, что позволяет предвидеть и исследовать области возможного возникновения операционного риска, а также заранее предусмотреть возможные меры защиты от его воздействия. К тому же подобные сведения могут использоваться при проведении стресс-тестирования операционного риска и способствуют выявлению недостатков в системе внутреннего контроля банка.

Необходимым условием эффективности проводимого мониторинга является определение (расследование) причин каждого операционного инцидента, возникшего в деятельности банка. Однако работа в данном направлении не должна становиться причиной излишнего документооборота и неэффективной организации процессов деятельности банка.

Детальный анализ информации о потерях от операционных инцидентов предполагает оценку более широкого, чем установлено требованиями Национального банка, перечня потерь от операционных инцидентов.

В соответствии с требованиями Национального банка оцениваются понесенные, а также потенциальные потери от операционных инцидентов. При этом оценка понесенных потерь предполагается в разрезе их количественного (понесенные прямые потери) и качественного (понесенные косвенные потери) влияния на деятельность банка. В свою очередь, потенциальные потери банка также могут оцениваться в разрезе потенциальных прямых и потенциальных косвенных потерь, что дает представление о том, какие прямые и (или)

косвенные потери от операционного инцидента банк мог понести, но не понес в результате благоприятного стечения обстоятельств.

В дополнение банком может проводиться оценка условных потерь и упущенных выгод. Оценка условных потерь направлена на получение сведений о максимальных возможных потерях, которых банк избежал благодаря реализации заранее предусмотренных планов (процедур) предотвращения операционных инцидентов, и позволяет оценить эффективность таких планов (процедур). Условные потери также могут оцениваться в разрезе условных прямых и условных косвенных потерь. Упущенные выгоды представляют собой измеряемые количественным образом доходы, которые планировались банком к получению, но не были получены (были недополучены) в результате операционного инцидента. При этом к упущенным выгодам не относятся убытки или возможные расходы банка.

Банку следует уделять особое внимание анализу небольших потерь в результате инцидентов, возникающих с высокой частотой, а также крупных потерь в результате инцидентов, происходящих с низкой частотой.

В процессе проведения мониторинга определяются ключевые индикаторы рисков банка, представляющие собой систему показателей (параметров) и (или) статистических данных, используемых для наблюдения за основными факторами рисков. В рамках данной системы следует предусмотреть создание отдельных ключевых индикаторов операционного риска (далее – КИОР), которые позволяют предвидеть риск возможных потерь и ориентированы на выявление потенциальных источников операционного риска.

Помимо КИОР банку следует разработать систему ключевых показателей эффективности деятельности (далее – КПЭД), отражающих состояние происходящих в банке процессов и позволяющих выявлять недостатки и ошибки деятельности, а также возможные потери.

Банку необходимо создать систему КИОР и КПЭД, охватывающую все направления деятельности, подверженные воздействию операционного риска, в первую очередь операции, приостановка или отказ от осуществления которых окажет значительное негативное влияние на финансовое состояние и эффективность банка. При этом для каждого из индикаторов риска и показателей деятельности следует установить лимиты и (или) пороговые значения.

Система КИОР и КПЭД должна быть взаимосвязана с механизмами реагирования на изменение индикаторов риска и показателей деятельности. Это позволит банку оперативно принимать соответствующие управленческие решения в случае приближения

величины принимаемого операционного риска отдельных операций, видов сделок, направлений деятельности к пороговым значениям или лимитам либо в случае их превышения, а также вносить корректировки в процедуры ограничения (снижения) риска.

Банку следует проводить периодический пересмотр системы КИОР и КПЭД, в том числе установленных лимитов и (или) пороговых значений индикаторов и показателей риска, и при необходимости дополнять ее новыми индикаторами и показателями риска, особенно в случае начала осуществления новых видов деятельности или иного существенного изменения, влияющего на риск-профиль банка.

Результаты, получаемые в процессе управления операционным риском, являются основой регулярного информирования органов управления банка. Для этих целей банк разрабатывает систему внутренней отчетности по операционному риску, соответствующую требованиям содержательности, информативности, удобства восприятия и своевременности представления данных. Следует создать такие механизмы отчетности, которые бы позволяли представлять информацию соответствующим органам управления банка в зависимости от сумм и значимости (существенности) потерь от операционных инцидентов, а также срочности реагирования или оперативности принятия решений и мер ограничения (снижения) операционного риска.

В управленческой отчетности по операционному риску следует отражать подробную информацию о последних существенных операционных инцидентах и потерях банка, а также существенных внешних событиях, повлиявших на деятельность банка, которые привели к увеличению расходов и (или) уровня риска банка. В отчетности необходимо отражать сведения о любом возможном влиянии операционного риска на капитал банка.

Процессы составления пруденциальной и управленческой отчетности по операционному риску, в том числе процессы получения исходной информации для отчетов, подлежат периодическому пересмотру и соответствующей переработке в случае появления изменений в деятельности, существенно влияющих на уровень операционного риска банка. Помимо этого, управленческую отчетность следует анализировать с точки зрения ее эффективности при оценке управления операционным риском, а также с точки зрения совершенствования принципов, процедур и практики управления операционным риском.

Банку следует разработать и применять на постоянной основе комплекс мер, направленных на снижение вероятности наступления

операционных инцидентов, приводящих к потерям, и (или) на уменьшение величины таких потерь, что достигается в процессе проведения контроля операционного риска.

Организация процесса контроля подразумевает осуществление предварительного, текущего и последующего контроля операционного риска банка.

На стадии предварительного контроля основными мерами ограничения (снижения) операционного риска являются подбор квалифицированных кадров; подготовка и обучение сотрудников в области управления операционным риском; разработка четких, детальных и недвусмысленных должностных инструкций, порядков осуществления операций, исключающих возникновение конфликта интересов; предварительный анализ рискованности и эффективности проводимых операций, в том числе осуществляемых банком впервые. Предварительный контроль операционного риска новых банковских продуктов также предполагает наличие разработанных ЛНПА до начала предоставления новых продуктов. Предварительный контроль ИТ-риска предусматривает обеспечение банка необходимыми техническими средствами, оборудованием, компьютерными системами и технологиями в соответствии со стратегией деятельности банка, позволяющими функционировать в том числе и в стрессовых условиях.

В процессе осуществления текущего контроля целесообразно использовать следующие основные меры по ограничению (снижению) операционного риска:

- установление и соблюдение ограничений (лимитов) на осуществление отдельных направлений деятельности, видов сделок, отдельных операций;

- отказ от осуществления отдельных операций, видов сделок;

- выявление направлений деятельности и отдельных операций, по которым получена прибыль значительно выше или ниже планируемых показателей с целью проверки реальности и объективных причин ее получения (неполучения);

- регулярная проверка и сверка осуществленных операций и данных бухгалтерского учета;

- разработка типовых форм договоров;

- стандартизация бизнес-процессов;

- передача риска или его части третьей стороне (аутсорсинг);

- страхование риска.

При этом в целях принятия решения о целесообразности ограничения объемов или отказа от осуществления отдельных операций, видов сделок, операционный риск которых банк не в

состоянии контролировать, следует провести оценку возможных потерь от дальнейшего проведения данных операций и видов сделок.

Поскольку аутсорсинг также является источником операционного риска, связанного с деятельностью третьей стороны, необходимо разработать надежные методы управления таким риском, принимая во внимание, что банк сохраняет риски, связанные с договорными отношениями с поставщиком услуг, включая риск расторжения договора на оказание услуг.

При использовании таких инструментов ограничения (снижения) операционного риска, как страхование, банку следует учитывать реальное снижение риска или его передачу в другие сферы деятельности, а также возможность возникновения новых рисков (например, риска контрагента). В связи с тем, что страхование риска не способно в полной мере заменить надлежащую практику управления и контроля операционного риска, банкам следует рассматривать его в качестве инструмента дополняющего, но не исключającego всесторонний внутренний контроль операционного риска.

Осуществление текущего контроля предполагает также проведение работы по выявлению недостатков систем автоматизации операций банка и сопутствующего им программного обеспечения с целью их оперативного устранения. Кроме того, необходимо на постоянной основе осуществлять текущий контроль безопасности и непрерывности деятельности, а также присущего банку ИТ-риска. В этих целях целесообразно предусмотреть:

- соблюдение иерархии и поддержание безопасности доступа к материальным активам, базам данных, иной информации, предназначенной для служебного пользования;

- разработку и реализацию планов действий в случае непредвиденных (кризисных) ситуаций;

- создание дублирующих (резервных) автоматизированных систем и (или) устройств;

- создание резервных вычислительных центров, в том числе удаленных;

- создание и использование автономных систем электропитания.

В процессе управления ИТ-риском необходимо использовать в работе технические кодексы установившейся практики Республики Беларусь в области банковских технологий, в частности, технические кодексы "Банковские технологии. Управление рисками в сфере информационных технологий", "Банковские технологии. Внутренний контроль и аудит информационных систем", а также международные стандарты управления информационными технологиями.

Особое внимание следует уделять контролю ИТ-риска при осуществлении реорганизации банка в форме слияния, преобразования, выделения или разделения, а также в случае реализации банком стратегии быстрого наращивания активов, предоставления новых продуктов и использования аутсорсинга.

На стадии последующего контроля основными мерами ограничения (снижения) операционного риска являются меры двойного контроля, например, проверка соответствия документов установленным формам и проверка соответствия выполняемых сотрудниками функций должностным инструкциям. Кроме того, в процессе последующего контроля осуществляется совершенствование системы внутреннего контроля, а также пересмотр существующих правил, принципов и подходов к управлению операционным риском.

В рамках осуществления процедур управления операционным риском банкам следует также проводить стресс-тестирование операционного риска для определения источников возможных потерь на основе различных сценариев, что способствует более глубокому пониманию риск-профиля банка. В случае использования банком аутсорсинга следует также предусмотреть создание отдельных сценариев и проведение стресс-тестирования операционного риска, связанного с аутсорсингом (например, для оценки возможных последствий в случае невыполнения поставщиком услуг своих обязательств). В этих целях банк может прибегнуть к использованию информации внешних баз данных операционных инцидентов.

Банку следует установить и соблюдать периодичность проведения стресс-тестирования. Кроме того, необходимо периодически пересматривать существующие и разрабатывать новые сценарии стресс-тестирования операционного риска, в том числе в связи с возникновением в деятельности банка непредвиденных (кризисных) ситуаций.

Результаты стресс-тестирования необходимо своевременно представлять на рассмотрение руководству банка для принятия соответствующих решений по ограничению (снижению) операционного риска или определения иных мер контроля. Наряду с информацией, полученной в процессе управления операционным риском, результаты стресс-тестирования следует учитывать при стратегическом планировании развития деятельности банка, в том числе планировании величины капитала, совершенствовании стратегии, политики и процедур по управлению операционным риском.

Обеспечение непрерывности деятельности банка предполагает разработку планов действий банка на случай непредвиденных

обстоятельств. В процессе разработки таких планов необходимо предусмотреть соблюдение следующих процедур:

согласование планов с заинтересованными сторонами, деятельность которых будет затронута в случае осуществления данных планов;

утверждение планов органами управления банка;

проверка работоспособности планов (тестирование);

регулярный пересмотр (переработка) и создание новых планов, в том числе в случае изменения объемов операций банка, выпуска новых банковских продуктов, осуществления новых видов деятельности, появления новых процессов и систем в деятельности банка.

В дополнение к этим процедурам с целью исключения конфликта интересов и дублирования обязанностей сотрудников в планах следует четко определить полномочия органов управления, подразделений и должностных лиц банка по выполнению мер, предусмотренных такими планами.

Планы действий на случай непредвиденных обстоятельств должны обеспечивать непрерывность функционирования и восстановление работоспособности основных программно-технических комплексов автоматизированных банковских и информационных систем, платежных (расчетных) систем, а также систем, поддерживаемых внешним поставщиком услуг и других систем, работающих в критических для банка областях деятельности. В таких планах необходимо предусмотреть действия банка на случай возможного неблагоприятного воздействия внешних факторов окружающей среды, как например, в случае стихийных бедствий и техногенных катастроф. Кроме того, особое внимание следует обратить на наличие возможностей восстановления записей на машинном и бумажном носителях, необходимых для нормального функционирования банка.

Банку следует проводить периодическую оценку эффективности функционирования (верификацию) СУОР или отдельных ее составляющих сотрудниками банка, не зависящими от оцениваемых ими процессов или систем. Помимо этого, банку необходимо проводить периодическую проверку внутренним аудитом полноты применения и эффективности установленных процедур управления операционным риском банка, а также организовать проведение независимой проверки СУОР с привлечением внешнего аудита или другой третьей стороны, обладающей соответствующей квалификацией. Результаты проведенных проверок (оценок) необходимо учитывать в процессах разработки и совершенствования стратегии, политики и процедур по управлению операционным риском.



В случае если банк является головной организацией банковской группы (банковского холдинга), органам управления такого банка необходимо предусмотреть формирование в рамках банковской группы (банковского холдинга) единообразных подходов к управлению операционным риском, позволяющих получать информацию о реальном уровне данного риска как по банковской группе (банковскому холдингу) в целом, так и по отдельным ее (его) участникам. Для достижения этой цели следует разработать соответствующие политику и процедуры, предусматривающие осуществление в рамках банковской группы (банковского холдинга) на постоянной основе обмена информацией, мониторинга, контроля, стресс-тестирования операционного риска, а также проведение периодической проверки (оценки) эффективности управления операционным риском на консолидированной основе.

Банку рекомендуется периодически осуществлять раскрытие информации, позволяющее заинтересованным сторонам оценивать его подходы к управлению операционным риском, а также самостоятельно определять эффективность СУОР банка. При этом объем и вид раскрываемой информации определяются в соответствии с объемом, риск-профилем и сложностью осуществляемых банком операций. В связи с этим банку необходимо установить подходы к определению характера раскрываемой информации, а также порядок осуществления внутреннего контроля ее раскрытия.

Регулярное раскрытие банком информации о подходах к управлению операционным риском создает для него дополнительные конкурентные преимущества, повышая доверие к банку со стороны пользователей этой информации, а также способствует усилению рыночной дисциплины и развитию лучшей практики управления операционным риском в банковской системе.

Национальный банк в рамках осуществления надзора за деятельностью банков проводит регулярную оценку уровня операционного риска в банках. При формировании Национальным банком мотивированного суждения об эффективности организации и функционирования СУОР, а также уровне операционного риска банка, использование банком рекомендаций, изложенных в документе Базельского комитета по банковскому надзору "Принципы надлежащего управления операционным риском" и настоящем письме, в процессе управления операционным риском и при совершенствовании СУОР будут рассматриваться как фактор, улучшающий качество управления операционным риском.

В связи с выходом настоящего письма не применяется в работе письмо Национального банка Республики Беларусь "Об использовании в работе принципов управления операционным риском" от 26 января 2006 г. № 23-14/13.

Приложение: на 33 л. в 1 экз.

Базельский комитет по банковскому надзору

**Принципы надлежащего управления операционным риском**

Июнь 2011

Банк международных расчетов

## Члены подгруппы операционного риска группы по внедрению стандартов

**Председатель: Mitsutoshi Adachi, Банк Японии**

Управление пруденциального регулирования, Австралия	Michael Booth
Национальный банк Бельгии	Jos Meuleman
Центральный банк Бразилии, Бразилия	Wagner Almeida
Служба управляющих финансовыми институтами, Канада	James Dennison Aina Liepins
Комиссия по регулированию банковской деятельности Китая	Meng Luo
Банк Франции	Jean-Luc Quémar
Немецкий федеральный банк, Германия	Marcus Haas
Федеральное управление финансового надзора (BaFin), Германия	Frank Corleis
Резервный банк Индии	Rajinder Kumar
Банк Италии	Marco Moscadelli
Банк Японии	Madoka Miyamura
Агентство финансовых услуг, Япония	Tsuyoshi Nagafuji
Комиссия по надзору за финансовым сектором, Люксембург	Didier Bergamo
Банк Нидерландов	Claudia Zapp
Комиссия по финансовому надзору, Польша	Grazyna Szwajkowska
Центральный банк Российской Федерации	Irina Yakimova
Резервный банк ЮАР	Jan van Zyl
Банк Испании	María Ángeles Nieto
Управление финансового надзора, Швеция	Agnieszka Arshamian
Управление надзора за финансовыми рынками, Швейцария	Paul Harpes
Управление по финансовому регулированию и надзору, Великобритания	Andrew Sheen Khim Murphy
Федеральная корпорация по страхованию вкладов, США	Alfred Seivold
Совет управляющих федеральной резервной системы, США	Adrienne Townes Haden Kenneth G. Fulton
Федеральный резервный банк Бостона, США	Patrick de Fontnouvelle
Федеральный резервный банк Нью-Йорка, США	Ronald Stroz
Управление контроля денежного обращения, США	Carolyn DuChene Maurice Harris
Управление надзора за сберегательными учреждениями, США	Eric Hirschhorn
Институт финансовой стабильности	Amarendra Mohan
Секретариат Базельского комитета по банковскому надзору, Банк международных расчетов	Andrew Willis

## Содержание

Введение

Роль органов надзора

Принципы управления операционным риском

Основополагающие принципы управления операционным риском

Руководство

    Совет директоров

    Высшее руководство

Среда управления риском

    Идентификация и оценка

    Мониторинг и отчетность

    Контроль и ограничение (снижение)

    Устойчивость и непрерывность деятельности

Роль раскрытия информации

Приложение: справочные материалы

## **Принципы надлежащего управления операционным риском и роль надзорного органа**

### **Введение**

1. В документе "Sound Practices for the Management and Supervision of Operational Risk" (далее – Надлежащие практики), опубликованном в феврале 2003г., Базельский комитет по банковскому надзору (далее – Комитет) четко определил основные принципы управления операционным риском для банков и органов надзора. Впоследствии, в документе 2006 г. "International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version" (общеизвестном как Базель II), Комитет предопределил дальнейшее развитие надлежащей практики в банковской сфере<sup>1</sup>. С тех пор банки и органы надзора расширили круг своих знаний и накопили опыт создания базовых структур управления операционным риском (далее – БСУОР). Свой вклад в знания банковской сферы и органов надзора, а также в становление надлежащей практики внесли примеры сбора данных о потерях, изучение количественного влияния и ряд обзоров практики банковской сферы, охватывающих вопросы руководства, данных и моделирования.

2. В ответ на эти изменения, Комитет принял решение обновить Надлежащие практики 2003 г. с целью отражения усовершенствованных подходов к надлежащему управлению операционным риском, используемых сегодня в банковской сфере. Данный документ – "Принципы надлежащего управления операционным риском и роль надзорного органа" – объединяет развитие надлежащей практики и подробно описывает одиннадцать принципов надлежащего управления операционным риском, охватывая (1) руководство, (2) среду управления риском и (3) роль раскрытия информации. С изданием обновленного документа, Комитет усиливает надлежащие практики 2003 года специфическими принципами управления операционным риском, соответствующими надлежащей практике банковской сферы. Данные принципы совершенствовались путем постоянного обмена информацией между органами надзора и представителями банковской сферы, начиная с 2003 года. "Принципы надлежащего управления операционным риском и роль надзорного органа" замещают

---

<sup>1</sup>Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version, Раздел V (Операционный риск), пункт 646, Базель, июнь 2006.

Надлежащие практики 2003 года и становятся документом, на который ссылается Базель II в пункте 651.

3. Текущая работа Комитета в области операционного риска ведется также на основе документа "A Framework for Internal Control Systems in Banking Organisations" (Базельский комитет, сентябрь 1998). Кроме того, важными источниками информации, которые следует учитывать банкам при разработке политик, процессов и систем управления операционным риском, являются документы "Core Principles for Effective Banking Supervision" (Базельский комитет, октябрь 2006) и "Core Principles Methodology" (Базельский комитет, октябрь 2006), предназначенные для органов надзора, а также принципы, определенные Комитетом в Компоненте 2 (Процесс надзорной оценки) Базель II.

4. Органы надзора будут продолжать стимулировать банки "двигаться по цепочке возможных подходов, постепенно развивая все более сложные системы и практики измерения операционного риска"<sup>2</sup>. Следовательно, учитывая то обстоятельство, что закрепленные в данном документе принципы определены развитием надлежащей практики банковской сферы, органы надзора ожидают постоянного совершенствования банками своих подходов к управлению операционным риском. Кроме того, в документе приведены основные элементы БСУОР банка. Данные элементы не следует рассматривать по отдельности – они должны быть компонентами, интегрированными в общую систему банка по управлению операционным риском.

5. Комитет полагает, что принципы, приведенные в данном документе, устанавливают надлежащие практики относительно всех банков. Комитет подразумевает, что, применяя эти принципы, банк будет учитывать риск-профиль, характер, масштабы, а также сложность своей деятельности.

### **Роль органов надзора**

6. Органы надзора, прямо или косвенно, проводят регулярные независимые оценки политик, процессов и систем банка, связанных с операционным риском, как отдельных составляющих общей оценки БСУОР. Органы надзора должны быть убеждены в наличии

---

<sup>2</sup>BCBS (2006), пункт 646.

соответствующих механизмов, позволяющих получать необходимую информацию о развитии банка.

7. Надзорные оценки операционного риска охватывают все сферы деятельности, отраженные в принципах управления операционным риском. Также органы надзора стремятся убедиться в наличии у банков-участников финансовых групп процессов и процедур, обеспечивающих надлежащее управление операционным риском на интегрированной основе по группе в целом. В соответствии с установленными процедурами при проведении данной оценки может осуществляться сотрудничество и обмен информацией с другими органами надзора в необходимых случаях<sup>3</sup>. В процессе оценки некоторые органы надзора могут прибегнуть к использованию внешнего аудита<sup>4</sup>.

8. К недостаткам, выявленным в процессе надзорной оценки, может быть применен ряд мер. Органы надзора используют инструменты, наилучшим образом соответствующие особенностям банка и его операционной среде. Для получения текущей информации об операционном риске органы надзора могут предусмотреть установление для банков и внешнего аудита механизмов представления отчетности напрямую (например, внутренняя управленческая отчетность банка по операционному риску может на регулярной основе представляться в органы надзора).

9. Используя мониторинг и оценку последних преобразований, а также планов дальнейшего развития банка, органы надзора продолжают принимать активное участие в стимулировании его деятельности по постоянному внутреннему развитию. Кроме того, для предоставления банку в рамках обратной связи полезной информации о состоянии проделанной им работы, данная деятельность может сопоставляться с аналогичной деятельностью других банков. В дальнейшем, информация о причинах (в той степени, насколько они определены), почему конкретная деятельность по развитию оказалась неэффективной, может предоставляться банку в общем виде для содействия процессу планирования.

---

<sup>3</sup>В соответствии с документами Комитета "High-level principles for the cross-border implementation of the New Accord", август 2003, и "Principles for home-host supervisory cooperation and allocation mechanisms in the context of Advanced Measurement Approaches (AMA)", ноябрь 2007.

<sup>4</sup>Для дальнейшего изучения вопроса см. документ Комитета "The relationship between banking supervisors and bank's external auditors", январь 2002.



## Принципы управления операционным риском

10. Операционный риск<sup>5</sup> присущ всем банковским продуктам, видам деятельности, процессам и системам, а эффективное управление операционным риском всегда было основополагающим элементом программы управления рисками банка. В результате, надлежащее управление операционным риском является отражением эффективности работы Совета директоров и высшего руководства по управлению портфелем банковских продуктов, видами деятельности, процессами и системами банка. Издавая данный документ, Комитет стремится обеспечить повышение эффективности управления операционным риском во всей банковской системе.

11. Управление рисками, как правило, включает в себя процесс идентификации рисков банка, измерение воздействия этих рисков (где возможно), обеспечение наличия программы эффективного планирования капитала и мониторинга, мониторинг позиций под риском и определение на постоянной основе соответствующих потребностей в капитале, принятие мер по контролю или ограничению (снижению) воздействия рисков, отчетность Совету директоров и высшему руководству о подверженности банка рискам и позициях капитала. В свою очередь, внутренний контроль является неотъемлемой частью повседневной деятельности банка и предназначен для подтверждения (насколько это возможно) эффективности и результативности его деятельности, достоверности, своевременности и полноты информации, а также соответствия действий банка законодательству и установленным правилам. На практике эти два направления тесно взаимосвязаны друг с другом, и их разграничение имеет меньшее значение, чем достижение целей каждого из направлений.

12. Надлежащее внутреннее регулирование формирует основу эффективной БСУОР. Несмотря на сходство внутренних подходов руководства к управлению операционным, кредитным или рыночным рисками, проблемы управления операционным риском могут отличаться от проблем управления другими рисками.

---

<sup>5</sup>Операционный риск определяется как риск потерь в результате несоответствующих или ошибочных внутренних процессов, действий сотрудников и систем или внешних событий. Это определение включает правовой риск, но исключает стратегический и репутационный риски.

13. Комитет наблюдает применение надлежащих практик управления во все большем количестве банков. Общепринятая банковская практика надлежащего управления операционным риском зачастую полагается на три линии защиты – (i) управление бизнес-линиями (отдельными направлениями деятельности), (ii) независимая служба по управлению операционным риском банка и (iii) независимую проверку.<sup>6</sup> В зависимости от характера, размера, сложности банка, а также риск-профиля его деятельности, степень формализации построения этих трех линий защиты будет отличаться. Однако во всех случаях служба по управлению операционным риском должна быть полностью интегрирована в общую структуру управления рисками банка.

14. В практике банковской сферы первой линией защиты является управление бизнес-линиями. Это означает, что надлежащее управление операционным риском предусматривает обязанность руководства бизнес-линий по идентификации и управлению рисками, присущими продуктам, видам деятельности, процессам и системам, за которые оно несет ответственность.

15. Функционально независимая служба операционного риска банка (independent corporate operational risk function, далее – CORF)<sup>7</sup> является, как правило, второй линией защиты, в основном дополняющей деятельность руководства по управлению операционным риском бизнес-линий. Степень независимости CORF различается между

---

<sup>6</sup>Согласно положениям Базельского документа "Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches", июнь 2011, независимая проверка включает следующие компоненты:

**Верификация** БСУОР проводится периодически, как правило, внутренним или внешним аудитом банка, однако возможно привлечение другой независимой внешней стороны, имеющей соответствующую квалификацию. Верификация позволяет проверить эффективность всей БСУОР, соответствующей политикам, утвержденным Советом директоров, а также оценить независимость и соответствие процессов валидации установленным политикам банка.

**Валидация** обеспечивает достаточную надежность систем количественного измерения, используемых в банке, а также целостность исходных данных, допущений, процессов и выходных данных. В частности, независимый процесс валидации должен предоставлять расширенные гарантии того, что методика измерения операционного риска позволяет рассчитывать требования к капиталу на покрытие операционного риска, достоверно отражающие профиль операционного риска банка. В дополнение к количественным аспектам внутренней валидации, в общем процессе большое значение имеет валидация методики моделей операционного риска, а также вводимых в эти модели и получаемых из них данных.

<sup>7</sup>Во многих юрисдикциях независимой службе операционного риска банка соответствует служба по управлению операционным риском банка.

банками. В небольших банках независимость может быть достигнута путем разделения обязанностей и независимой проверки процессов и служб. В более крупных банках CORF будет предусматривать структуру подотчетности, не зависящую от бизнес-линий, генерирующих риск, а также нести ответственность за разработку, поддержание и постоянное развитие подходов к управлению операционным риском в банке. Данная служба может охватывать процессы измерения операционного риска и процессы отчетности, предусматривать комитеты по рискам, а также обязанность по представлению отчетности Совету директоров. Основной функцией CORF является критическое рассмотрение исходных данных бизнес-линий, используемых для систем управления, измерения риска и отчетности, а также выходных данных этих систем. Для того чтобы CORF эффективно исполняла свои многочисленные обязанности, в ней должно быть занято достаточное для этого количество сотрудников, обладающих навыками управления операционным риском.

16. Третья линия защиты заключается в независимой проверке и критическом рассмотрении контроля, процессов и систем управления операционным риском банка. Сотрудники, осуществляющие данные проверки, должны быть компетентны и надлежащим образом подготовлены, а также не вовлечены в развитие, создание и функционирование БСУОР. Проверку может проводить аудит или сотрудники, не зависящие от проверяемых процессов или систем, а также внешняя сторона, имеющая соответствующую квалификацию.

17. При использовании для управления операционным риском модели трех линий защиты, структура и деятельность последних зачастую различаются в зависимости от портфеля банковских продуктов, видов деятельности, процессов и систем; размера банка; а также подходов к управлению рисками. Важными характеристиками надежного управления операционным риском являются сильная культура управления риском и хорошее взаимодействие между тремя линиями защиты.

18. Степень охвата внутренним аудитом должна быть достаточной для независимого подтверждения того, что БСУОР создана в соответствии с поставленными целями и функционирует эффективно<sup>8</sup>. В тех случаях, когда для проведения аудита применяется аутсорсинг, Высшее

---

<sup>8</sup>Документ Комитета, "Internal Audit in Banks and the Supervisor's Relationship with Auditors", август 2001, определяет роль внутреннего и внешнего аудита.

руководство должно учитывать эффективность предполагаемого соглашения, а также целесообразность использования такого аудита в качестве третьей линии защиты.

19. Внутренний аудит должен предусматривать вынесение профессионального суждения об общей целесообразности применения и адекватности БСУОР, а также связанных с ней процессов управления, по банку в целом. Внутренний аудит должен оценивать соответствие БСУОР не только утвержденным руководством политикам и процедурам, но также и организационным потребностям и ожиданиям надзорных органов. Например, внутренний аудит не должен определять свойственные банку риск-аппетит или толерантность к риску, однако обязан проверять надежность процессов установления данных предельных показателей, а также причины и способы их корректировки в ответ на изменение обстоятельств.

20. Ввиду развития управления операционным риском и постоянного изменения условий деятельности, руководство должно обеспечивать достаточную надежность политик, процессов и систем БСУОР. Совершенствование управления операционным риском будет зависеть от степени, в которой учитывается мнение сотрудников банка, ответственных за управление операционным риском, а также готовности высшего руководства к принятию своевременных действий в ответ на их предостережения.

### **Основополагающие принципы управления операционным риском**

Принцип 1: Совет директоров должен взять на себя руководство по созданию сильной культуры управления рисками. Совет директоров и высшее руководство<sup>9</sup> банка должны создать корпоративную культуру, которая сопровождается надежным управлением рисками,

---

<sup>9</sup>В данном документе речь идет о структуре управления, включающей Совет директоров и высшее руководство. Комитету известно, что в разных странах имеются значительные различия законодательного и регулирующего характера в отношении функций Совета директоров и высшего руководства. В некоторых странах Совету принадлежат основные, если не исключительные, функции по контролю исполнительного органа (высшего руководства, общего руководства), чтобы обеспечить выполнение последним своих задач. По этой причине в некоторых случаях он называется Наблюдательным советом. Это означает, что у него нет исполнительских функций. В других странах, наоборот, Совет обладает широкой компетенцией и утверждает общую структуру управления банком. Учитывая эти различия, в данном документе такие понятия, как "Совет директоров" и "высшее руководство", используются не для того, чтобы дать юридическое толкование, а чтобы определить две функции по принятию решений в банке.

поддерживает и обеспечивает соответствующие стандарты и стимулы профессионального и ответственного поведения. В связи с этим непосредственной обязанностью Совета директоров является обеспечение наличия сильной культуры управления операционным риском<sup>10</sup> во всех структурных подразделениях банка.

Принцип 2: Банки должны разрабатывать, внедрять и поддерживать БСУОР, полностью интегрированную в общие процессы управления рисками банка. БСУОР для управления операционным риском, выбранная отдельным банком, будет зависеть от ряда факторов, включающих характер, размер, сложность, а также риск-профиль банка.

## **Руководство<sup>11</sup>**

### **Совет директоров**

Принцип 3: Совет директоров должен устанавливать, утверждать и периодически пересматривать БСУОР. Совет директоров должен контролировать работу высшего руководства для обеспечения эффективного применения политик, процессов и систем на всех уровнях принятия решений.

Принцип 4: Совет директоров должен утверждать и пересматривать риск-аппетит и толерантность к операционному риску<sup>12</sup>, определяющие характер, типы и уровни операционного риска, который банк готов принять.

### **Высшее руководство**

---

<sup>10</sup>Под внутренней культурой управления операционным риском принято понимать совокупность индивидуальных и корпоративных ценностей, отношений, компетенций и поведения, которые определяют предпочтения банка в управлении операционным риском и стиль такого управления.

<sup>11</sup>См. также документ Комитета "Principles for enhancing corporate governance", октябрь 2010.

<sup>12</sup>"Риск-аппетит" заключается в определении высшего уровня величины риска, который банк склонен принять, исходя из соотношения показателей риск/доходность; также часто используется в значении "перспективный взгляд на принятие риска". "Толерантность к риску" заключается в более точном определении уровня отклонений, которые банк согласен принять, исходя из целей деятельности, что часто рассматривается как величина риска, к принятию которой банк подготовлен. В данном документе понятия используются как синонимы.

Принцип 5: Высшее руководство должно разрабатывать и представлять на утверждение Совету директоров четкую, эффективную и надежную структуру управления с четко установленным, прозрачным и последовательным разграничением ответственности. Высшее руководство несет ответственность за последовательное внедрение и поддержание во всех структурных подразделениях банка политик, процессов и систем управления операционным риском, присущем всем значимым продуктам, видам деятельности, процессам и системам банка, в соответствии с риск-аппетитом и толерантностью к риску.

## **Среда управления риском**

### **Идентификация и оценка**

Принцип 6: Высшее руководство должно обеспечивать идентификацию и оценку операционного риска, присущего всем значимым продуктам, видам деятельности, процессам и системам банка, для того, чтобы убедиться в достаточном понимании присущих банку рисков и способствующих их появлению причин.

Принцип 7: Высшее руководство должно обеспечивать наличие процесса утверждения всех новых продуктов, видов деятельности, процессов и систем, в полной мере оценивающего операционный риск.

### **Мониторинг и отчетность**

Принцип 8: Высшее руководство должно внедрить процесс регулярного мониторинга профиля операционного риска и областей существенной подверженности потерям. Для уровней Совета директоров, высшего руководства и руководства бизнес-линий должны быть предусмотрены соответствующие механизмы отчетности, способствующие проактивному (упреждающему) управлению операционным риском.

### **Контроль и ограничение (снижение)**

Принцип 9: В банках должна быть создана сильная среда контроля, в которую входят политики, процессы и системы, надлежащий внутренний контроль, а также соответствующие стратегии ограничения (снижения) и/или передачи риска.

### **Устойчивость и непрерывность деятельности**

Принцип 10: В банках должны быть разработаны планы обеспечения непрерывности и устойчивости деятельности для поддержания способности работать на непрерывной основе, а также ограничения потерь в случае возникновения событий, влекущих серьезные нарушения непрерывности функционирования.

### **Роль раскрытия информации**

Принцип 11: Раскрытие информации должно предоставлять заинтересованным сторонам возможность оценивать подход банка к управлению операционным риском.

### **Основополагающие принципы управления операционным риском**

**Принцип 1: Совет директоров должен взять на себя руководство по созданию сильной культуры управления рисками. Совет директоров и высшее руководство банка должны создать корпоративную культуру, которая сопровождается надежным управлением рисками, поддерживает и обеспечивает соответствующие стандарты и стимулы профессионального и ответственного поведения. В связи с этим непосредственной обязанностью Совета директоров является обеспечение наличия сильной культуры управления операционным риском во всех структурных подразделениях банка.**

21. Банки, с сильной культурой управления рисками и этикой деловой практики менее подвержены непредвиденному, наносящему ущерб воздействию операционных инцидентов (событий операционного риска), а также лучше приспособлены к эффективной работе с возникающими инцидентами. Действия Совета директоров и высшего руководства, политики, процессы и системы образуют основу культуры надлежащего управления рисками.

22. Совет директоров должен установить кодекс поведения или политику этики, в которых четко определены требования к поддержанию высшего стандарта честности и этических ценностей, а также выявлять приемлемую деловую практику и недопустимые конфликтные ситуации. Четко определенные ожидаемые результаты и подотчетность обеспечивают понимание сотрудниками банка своей роли, ответственности, а также полномочий при управлении рисками. Сильная и последовательная поддержка этического поведения и

управления рисками со стороны высшего руководства значительно усиливает кодексы поведения и этики, политику вознаграждений, а также программы обучения. Политика вознаграждений должна быть согласована с установленными риск-аппетитом и толерантностью к риску, долгосрочной стратегией деятельности банка, его финансовыми задачами, а также общей безопасностью и надежностью банка. Кроме того, банк должен соответствующим образом соблюдать соотношение риска и вознаграждений<sup>13</sup>.

23. Высшее руководство должно обеспечивать доступность соответствующего уровня обучения управлению операционным риском на всех уровнях организационной структуры банка. Проводимое обучение должно соответствовать служебному положению, роли и должностным обязанностям отдельных сотрудников, для которых оно предназначено.

**Принцип 2: Банки должны разрабатывать, внедрять и поддерживать БСУОР, полностью интегрированную в общие процессы управления рисками банка. БСУОР для управления операционным риском, выбранная отдельным банком, будет зависеть от ряда факторов, включающих характер, размер, сложность, а также риск-профиль банка.**

24. Основополагающей предпосылкой надлежащего управления рисками является понимание Советом директоров и руководящими сотрудниками банка характера и сложности рисков, присущих портфелю банковских продуктов, услугам и видам деятельности банка. Данное условие является особенно важным для операционного риска, так как он присущ всем банковским продуктам, видам деятельности, процессам и системам.

25. Необходимой составляющей для понимания характера и сложности операционного риска является наличие элементов БСУОР, полностью интегрированных в общие процессы управления рисками банка. БСУОР должна быть надлежащим образом интегрирована в процессы управления рисками на всех уровнях организационной

---

<sup>13</sup>См. также документ Комитета "Report on the range of methodologies for the risk and performance alignment of remuneration", май 2011; документ Форума по финансовой стабильности "Principles for sound compensation practices", апрель 2009; а также документ Совета по финансовой стабильности "FSB principles for sound compensation practices – implementation standards", сентябрь 2009.



структуры банка, включая уровни группы и бизнес-линий; а также в новые банковские продукты, виды деятельности, процессы и системы. Кроме того, результаты оценки операционного риска банка должны учитываться в процессах разработки общей стратегии деятельности банка.

26. БСУОР должна быть всесторонне и надлежащим образом задокументирована в утвержденных Советом директоров политиках, а также включать определения операционного риска и потерь от операционных инцидентов. Банки, которые надлежащим образом не описывают и не классифицируют операционный риск и подверженность банка потерям, могут значительно снизить эффективность своей БСУОР.

27. Документация по БСУОР должна четко:

- (a) определять структуры руководства, используемые для управления операционным риском, в том числе направления отчетности и подотчетность;
- (b) описывать инструменты оценки риска и способы их использования;
- (c) описывать установленные банком значения риск-аппетита и толерантности к риску, пороговые значения или лимиты риска, присущего банку, и остаточного риска, а также утвержденные стратегии и инструменты ограничения (снижения) риска;
- (d) описывать подходы к установлению и мониторингу пороговых значений или лимитов риска, присущего банку, и остаточного риска;
- (e) устанавливать порядок отчетности по риску и управленческие информационные системы (MIS);
- (f) предусматривать общую систематизацию понятий операционного риска для обеспечения последовательности идентификации риска, оценки его воздействия и целей управления риском<sup>14</sup>;
- (g) предусматривать соответствующую независимую проверку и оценку операционного риска; а также
- (h) устанавливать требования по пересмотру и соответствующей переработке политик в случае любого существенного изменения профиля операционного риска банка.

---

<sup>14</sup>Непоследовательная систематизация понятий операционного риска может увеличить вероятность ошибок идентификации и классификации рисков или разделения обязанностей по оценке, мониторингу, контролю и ограничению (снижению) рисков.

## Руководство

### Совет директоров

**Принцип 3: Совет директоров должен устанавливать, утверждать и периодически пересматривать БСУОР. Совет директоров должен контролировать работу высшего руководства для обеспечения эффективного применения политик, процессов и систем на всех уровнях принятия решений.**

28. Совет директоров должен:

- (a) сформировать культуру управления, в том числе вспомогательные процессы, для понимания характера и масштабов операционного риска, присущего стратегии и видам деятельности банка, а также развивать всестороннюю, динамичную среду управленческого надзора и контроля, полностью интегрированную в общую систему управления рисками по банку в целом или в полной мере согласованные с ней;
- (b) обеспечивать высшее руководство четкими указаниями и распоряжениями относительно принципов, лежащих в основе БСУОР, а также утверждать разработанные последним соответствующие политики;
- (c) регулярно анализировать БСУОР для подтверждения того, что банк идентифицировал и управляет операционным риском, возникающим вследствие изменений на внешнем рынке и воздействия других внешних факторов, а также операционными рисками, связанными с новыми продуктами, видами деятельности, процессами или системами, включая изменения риск-профиля и приоритетов (например, изменяющийся объем операций);
- (d) обеспечивать эффективную независимую проверку БСУОР аудитом или другими надлежащим образом подготовленными сторонами; а также
- (e) обеспечивать использование руководством преимуществ развития лучшей практики управления операционным риском<sup>15</sup>.

29. Сильный внутренний контроль является важным аспектом управления операционным риском, и для создания сильной среды контроля Совет директоров должен определить четкие линии

---

<sup>15</sup>См. также документ Комитета "International Convergence of Capital measurement and Capital Standards: A Revised framework – Comprehensive version", пункт 718 (xci).

ответственности и подотчетности руководства. Среда контроля должна обеспечивать соответствующую независимость/разделение обязанностей между службами по управлению операционным риском, бизнес-линиями и службами поддержки.

**Принцип 4: Совет директоров должен утверждать и пересматривать риск-аппетит и толерантность к операционному риску, определяющие характер, типы и уровни операционного риска, который банк готов принять.**

30. В процессе утверждения и пересмотра риск-аппетита и толерантности к риску Совет директоров должен рассматривать все существенные риски, степень нерасположенности банка к принятию рисков, его текущее финансовое состояние и стратегическое направление деятельности. Установленные риск-аппетит и толерантность к риску должны заключать в себе различные значения риск-аппетита по банку в целом, а также должна обеспечиваться их совместимость. Совет директоров должен утверждать соответствующие пороговые значения или лимиты для специфических операционных рисков, а также общие значения риск-аппетита и толерантности к операционному риску.

31. Совет директоров должен регулярно пересматривать актуальность лимитов и установления риск-аппетита и толерантности к операционному риску в целом. Данный пересмотр должен учитывать изменения внешней среды, существенный рост деятельности или объема операций, качество среды контроля, эффективность управления риском или стратегий его ограничения (снижения), понесенные потери, а также частоту, объем или характер несоблюдения лимитов. Совет директоров должен контролировать соблюдение руководством установленного риск-аппетита и толерантности к риску и обеспечивать своевременное обнаружение и устранение нарушений.

### **Высшее руководство**

**Принцип 5: Высшее руководство должно разрабатывать и представлять на утверждение Совету директоров четкую, эффективную и надежную структуру управления с четко установленным, прозрачным и последовательным разграничением ответственности. Высшее руководство несет ответственность за последовательное внедрение и поддержание во всех структурных**

**подразделениях банка политик, процессов и систем управления операционным риском, присущим всем значимым продуктам, видам деятельности, процессам и системам банка, в соответствии с риск-аппетитом и толерантностью к риску.**

32. Высшее руководство несет ответственность за установление и поддержание надежных механизмов критического рассмотрения, а также эффективных процессов решения проблем. В состав данных процедур должны входить способы предоставления информации о проблемах, способы отслеживания и, при необходимости, вынесения проблем на более высокие уровни иерархии для обеспечения их решения. Банки должны располагать возможностью продемонстрировать удовлетворительную работу подхода, основанного на трех линиях защиты, а также показать, каким образом Совет директоров и высшее руководство обеспечивают внедрение и применение данного подхода надлежащим и приемлемым образом.

33. Высшее руководство должно реализовывать установленную Советом директоров БСУОР в отдельных политиках и процедурах, внедрение и верификация которых могут осуществляться в различных подразделениях банка. Высшее руководство должно четко определять полномочия, границы ответственности и порядок отчетности с целью стимулирования и поддержания подотчетности, а также обеспечения наличия необходимых ресурсов для управления операционным риском в соответствии с установленными риск-аппетитом и толерантностью к риску. Кроме того, высшее руководство должно обеспечивать соответствие процесса управленческого надзора рискам, присущим деятельности подразделений банка.

34. Высшее руководство должно обеспечивать координацию и эффективное взаимодействие сотрудников, ответственных за управление операционным риском, сотрудников, ответственных за управление кредитным, рыночным и другими рисками, а также тех, кто несет ответственность за приобретение услуг внешних сторон, таких как страхование рисков или аутсорсинг. Несоблюдение данной процедуры может привести к значительным несоответствиям или дублированию в общей программе управления рисками банка.

35. Сотрудники CORF должны обладать достаточным статусом в банке для того, чтобы эффективно исполнять свои обязанности, специфика которых должна быть четко отражена в названиях

должностей данных сотрудников, соответствующих должностям сотрудников других служб по управлению рисками, такими как кредитный, рыночный и риск ликвидности.

36. Высшее руководство должно привлекать к управлению деятельностью банка сотрудников, обладающих необходимыми опытом, техническими возможностями и доступом к ресурсам. Сотрудники, ответственные за мониторинг и проверку на соответствие политике банка в области управления рисками, должны быть независимы от проверяемых ими подразделений банка.

37. Структура управления банка должна соответствовать характеру, масштабам, сложности, а также риск-профилю деятельности банка. При разработке структуры управления операционным риском банку необходимо иметь в виду следующее:

- (a) Структура комитета – Надлежащая практика банковской сферы для более крупных и более сложных банков, имеющих головную организацию группы и отдельные структурные подразделения, заключается в использовании для контроля за всеми рисками созданного Советом директоров на корпоративном уровне комитета по рискам, которому подотчетен созданный на уровне управления банком комитет по операционному риску. В зависимости от характера, размера и сложности банка, корпоративный комитет по рискам может получать исходные данные от комитетов по операционному риску в разрезе стран, видов деятельности или функциональных областей. Менее крупные и менее сложные банки могут использовать более простую организационную структуру, позволяющую осуществлять контроль за операционным риском непосредственно на уровне комитета по управлению рисками при Совете директоров;
- (b) Состав комитета – Надлежащая практика банковской сферы для комитетов по операционному риску (или комитета по рискам в менее крупных банках) предусматривает включение в их состав ряда специалистов, обладающих опытом в управлении деятельностью организации, финансовом управлении, а также независимом управлении рисками. В состав комитета также могут входить независимые члены Совета директоров, не являющиеся исполнительными лицами, что представляет собой обязательное условие в законодательствах некоторых стран; и

- (с) Деятельность комитета – Заседания комитета должны проводиться с надлежащей периодичностью, с обеспечением достаточного времени и ресурсов, что позволит эффективно рассматривать вопросы и принимать решения. Отчеты о работе комитета должны быть достаточными для того, чтобы проверить и оценить ее эффективность.

## **Среда управления риском**

### **Идентификация и оценка**

**Принцип 6: Высшее руководство должно обеспечивать идентификацию и оценку операционного риска, присущего всем значимым продуктам, видам деятельности, процессам и системам банка, для того, чтобы убедиться в достаточном понимании присущих банку рисков и способствующих их появлению причин.**

38. Идентификация и оценка риска являются основополагающими характеристиками эффективной системы управления операционным риском. Эффективная идентификация рисков учитывает как внутренние<sup>16</sup>, так и внешние<sup>17</sup> факторы. Надлежащая оценка рисков способствует лучшему пониманию банком своего риск-профиля, а также позволяет наиболее эффективно распределять ресурсы и определять стратегии управления рисками.

39. Примерами инструментов, которые могут использоваться для идентификации и оценки риска, являются:

- (а) Результаты аудиторских проверок: Акцентируя внимание в основном на недостатках и слабых местах контроля, результаты аудиторских проверок могут также давать представление о присущем банку риске, возникающем в результате воздействия внутренних или внешних факторов;
- (б) Сбор и анализ информации о потерях из внутренних источников: Данные о потерях от операционных инцидентов банка предоставляют существенную информацию, позволяющую оценить его подверженность операционному риску, а также

---

<sup>16</sup>Например, структура банка, характер его деятельности, качество человеческих ресурсов, организационные изменения и текучесть кадров.

<sup>17</sup>Например, изменения в окружающей среде и банковской сфере, достижения в области технологий.

эффективность внутреннего контроля банка. Анализ случаев возникновения потерь может давать представление о причинах крупных потерь, а также предоставлять информацию о том, являются ли ошибки контроля единичными либо систематическими<sup>18</sup>. Кроме того, для получения более полного представления о своей подверженности операционному риску, банки могут собирать и отслеживать информацию о вкладе операционного риска в потери, связанные с кредитным и рыночным рисками;

- (c) Сбор и анализ информации о потерях из внешних источников: Внешние данные содержат сведения об общих суммах потерь от операционных инцидентов, датах, возмещениях, а также соответствующую информацию о причинах возникновения потерь от операционных инцидентов в других организациях. Внешние данные о потерях могут сопоставляться с внутренней информацией о потерях банка или использоваться для исследования возможных недостатков среды контроля либо с целью учета не выявленных ранее областей риска;
- (d) Оценки риска: При оценке риска, также часто упоминаемой как самооценка риска (или RSA), банк оценивает процессы, лежащие в основе операций банка, на предмет наличия возможных угроз и уязвимостей с учетом потенциального воздействия последних. Для похожего подхода – самооценки контроля риска (или RSCA) – характерна оценка присущего банку риска (имеется в виду риск до осуществления контроля), эффективности среды контроля и остаточного риска (имеется в виду подверженность риску после осуществления контроля). Карты оценок, составленные на основе RSCA путем взвешивания остаточных рисков, служат инструментом преобразования выходных данных RSCA в систему показателей, дающих относительную ранжированную оценку среды контроля;
- (e) Составление карты бизнес-процессов: Карты бизнес-процессов определяют основные стадии бизнес-процессов, операций и организационные функции. Данные карты также позволяют выявить основные места концентрации риска в общем бизнес-процессе. Карты процессов могут показывать единичные риски, взаимозависимость рисков, а также области недостающего

---

<sup>18</sup>Составление карты данных о потерях банка путем их распределения потерь по первому уровню бизнес-линий и в зависимости от классов случаев возникновения потерь, определенных в Приложениях 8 и 9 Базеля II, 2006 г., в частности, в более крупных банках, может упростить сопоставление внутренних данных банка о потерях с внешними.

- контроля или управления рисками. Кроме того, карты помогают определить приоритеты дальнейших действий руководства;
- (f) Индикаторы риска и показатели эффективности: Индикаторы риска и показатели эффективности – это система показателей и/или статистических данных, дающих представление о подверженности банка рискам. Индикаторы риска, часто упоминающиеся как Ключевые индикаторы риска (KRI), используются для наблюдения за основными причинами воздействия наиболее существенных для банка рисков. Показатели эффективности, часто упоминающиеся как Ключевые показатели эффективности (KPI), отражают состояние происходящих процессов, что в свою очередь дает представление о недостатках и ошибках функционирования, а также о возможных потерях. Индикаторы риска и показатели эффективности зачастую используются вместе с триггерами эскалации для предупреждения о приближении уровней рисков к пороговым значениям или лимитам либо превышении их, а также для предложений в планы ограничения (снижения) рисков;
  - (g) Сценарный анализ: Сценарный анализ – это процесс получения экспертных оценок от руководителей бизнес-линий и сотрудников, ответственных за управление рисками, для выявления возможных операционных инцидентов и определения их потенциального воздействия. Сценарный анализ является эффективным инструментом, позволяющим оценить возможные источники существенного операционного риска, а также определить потребность в дополнительных мерах по ограничению (снижению) риска или контролю управления риском. Учитывая субъективность сценарного анализа, для обеспечения целостности и последовательности данного процесса необходима надежная структура управления;
  - (h) Измерение: Более крупные банки могут количественно измерять свою подверженность операционному риску с помощью модели, определяющей его воздействие, в которой в качестве исходных данных применяются данные, полученные при использовании инструментов оценки риска. Итоговые данные модели могут быть использованы при расчете экономического капитала, а также распределены по бизнес-линиям для увязки риска и доходности; а также
  - (i) Сравнительный анализ: Сравнительный анализ заключается в сравнении результатов, полученных при использовании различных инструментов оценки риска, для более полного



отражения профиля операционного риска банка. Например, сравнение частоты возникновения и существенности данных из внутренних источников с картами самооценки контроля риска (RCSA) может способствовать определению эффективности процессов самооценки. Для достижения лучшего понимания степени подверженности банка возможным проявлениям риска данные сценарного анализа можно сравнивать с внутренними и внешними данными.

40. Банк должен обеспечить надлежащий учет операционного риска во внутренних механизмах ценообразования и оценки эффективности своей деятельности. В сферах, где операционный риск не учитывается, побуждения к принятию риска могут не соответствовать риск-аппетиту и толерантности к риску.

**Принцип 7: Высшее руководство должно обеспечивать наличие процесса утверждения всех новых продуктов, видов деятельности, процессов и систем, в полной мере оценивающего операционный риск.**

41. В целом, подверженность банка операционному риску увеличивается при осуществлении им новых видов деятельности или разработке новых продуктов; выходе на новые рынки; внедрении новых бизнес-процессов или технологических систем; и (или) осуществлении деятельности, географически удаленной от главного офиса банка. Кроме того, уровень риска может возрасти при переходе операций, процессов и систем, связанных с новыми продуктами, от начального этапа к этапу, когда осуществление новых операций становится существенным источником доходов банка или критическим для его деятельности. Начиная с первого этапа работы над новым продуктом, банк должен обеспечивать надлежащую инфраструктуру контроля управления риском, а также ее соответствие темпам развития или изменения операций, процессов и систем, связанных с новыми продуктами.

42. В банке должны быть предусмотрены политики и процедуры анализа и утверждения новых продуктов, видов деятельности, процессов и систем. Процесс анализа и утверждения должен охватывать:

- (a) риски, присущие новым продуктам, услугам или видам деятельности;
- (b) изменение профиля операционного риска, риск-аппетита и толерантности к операционному риску, включая риск, свойственный уже существующим продуктам или видам деятельности;
- (c) необходимые контроль, процессы управления риском, а также стратегии ограничения (снижения) риска;
- (d) остаточный риск;
- (e) изменение соответствующих пороговых значений или лимитов; а также
- (f) процедуры и системы показателей для измерения, мониторинга и управления риском нового продукта или вида деятельности.

Процесс утверждения должен также предусматривать осуществление соответствующих инвестиций в человеческие ресурсы и технологическую инфраструктуру до предоставления новых продуктов. Для выявления любых существенных отклонений от ожидаемого риск-профиля, а также управления какими-либо непредвиденными рисками, в банке должен проводиться мониторинг процесса внедрения новых продуктов, видов деятельности, процессов и систем.

## **Мониторинг и отчетность**

**Принцип 8: Высшее руководство должно внедрить процесс регулярного мониторинга профиля операционного риска и областей существенной подверженности потерям. Для уровней Совета директоров, высшего руководства и руководства бизнес-линий должны быть предусмотрены соответствующие механизмы отчетности, способствующие проактивному (упреждающему) управлению операционным риском.**

43. Банкам рекомендуется постоянно совершенствовать качество отчетности по операционному риску. Банк должен обеспечивать полноту, достоверность, последовательность и действенность своей отчетности по бизнес-линиям и продуктам. Отчетность должна быть управляемой по своим масштабам и объему; как излишняя, так и недостаточная информация препятствуют эффективному принятию решений.

44. Отчетность должна быть своевременной, и банк должен быть в состоянии составлять ее как в обычных, так и в стрессовых рыночных

условиях. Частота представления отчетности, отражающей принимаемые банком риски, должна соответствовать темпам и характеру изменений операционной среды. Результаты мониторинга, а также оценки БСУОР службой внутреннего аудита и/или службами по управлению рисками, должны включаться в периодическую отчетность для руководства и Совета директоров. Кроме того, в соответствующих случаях отчеты, составленные органами надзора и/или для них, должны представляться внутри банка высшему руководству и Совету директоров.

45. Отчеты по операционному риску могут содержать внутренние финансовые и операционные показатели, показатели соответствия установленным нормам, а также информацию внешнего рынка или окружающей среды о событиях и обстоятельствах, существенных для принятия решений. Отчетность по операционному риску должна включать:

- (a) случаи несоблюдения банком установленного риск-аппетита и толерантности к операционному риску, в том числе пороговых значений и лимитов;
- (b) подробную информацию о последних существенных внутренних операционных инцидентах и потерях; а также
- (c) информацию о существенных внешних событиях и любом возможном влиянии на капитал банка, предназначенный для покрытия операционного риска.

46. Процессы сбора данных и составления отчетности по риску должны периодически анализироваться с целью постоянного совершенствования управления риском, а также развития политик, процедур и практик управления риском.

### **Контроль и ограничение (снижение)**

**Принцип 9: В банках должна быть создана сильная среда контроля, в которую входят политики, процессы и системы, надлежащий внутренний контроль, а также соответствующие стратегии ограничения (снижения) и/или передачи риска.**

47. Внутренний контроль должен быть нацелен на обеспечение объективного подтверждения эффективности банковских операций, безопасности активов банка, а также составления им надежной

финансовой отчетности и соблюдения действующих законодательных и нормативных актов. Программа надлежащего внутреннего контроля состоит из пяти компонентов, интегрированных в процесс управления риском: среда контроля, оценка риска, осуществление контроля, информация и взаимодействие, мониторинг<sup>19</sup>.

48. Процессы и процедуры контроля должны включать систему подтверждения соответствия политикам банка. К основным элементам оценки соответствия политикам относятся:

- (a) анализ достижения поставленных целей руководством высшего уровня;
- (b) проверка на соответствие управленческому контролю;
- (c) анализ действий и принимаемых решений по случаям несоответствия;
- (d) оценка необходимых одобрений и разрешений для обеспечения подотчетности соответствующему уровню управления;
- (e) отслеживание информации о санкционированном несоблюдении пороговых значений или лимитов, действиях руководства не в интересах банка или других отклонениях от политики.

49. Эффективная среда контроля также требует соответствующего разделения обязанностей. Задачи, приводящие к возникновению конфликта интересов между отдельными сотрудниками или группами сотрудников, в отсутствие двойного контроля или других мер воздействия могут повлечь сокрытие потерь, ошибок или ненадлежащих действий. Поэтому банк должен осуществлять идентификацию, минимизацию, а также независимую тщательную проверку и мониторинг областей возможных конфликтов интересов.

50. В дополнение к разделению обязанностей и двойному контролю, банки должны обеспечивать наличие других традиционных элементов внутреннего контроля, позволяющих надлежащим образом управлять операционным риском. Данные элементы включают:

- (a) четко установленные полномочия и/или процедуры одобрения;
- (b) тщательный мониторинг соблюдения установленных пороговых значений или лимитов риска;

---

<sup>19</sup>Более подробное описание внутреннего контроля приведено в документе Комитета "Framework for Internal Control Systems in Banking Organisations", сентябрь 1998.

- (c) безопасность использования и доступа к активам и учетным записям банка;
- (d) надлежащий уровень обеспеченности кадрами и обучение сотрудников для поддержания профессионального опыта;
- (e) постоянные процессы выявления бизнес-линий или продуктов, доходы по которым не соответствуют объективным ожиданиям<sup>20</sup>;
- (f) регулярную верификацию и сверку операций банка с данными бухгалтерского учета; и
- (g) политику предоставления отпусков руководителям и сотрудникам, предусматривающую освобождение от обязанностей на период не менее двух недель подряд.

51. Эффективное использование и надлежащее внедрение технологий может вносить свой вклад в среду контроля. Например, автоматизированные процессы, в отличие от выполняемых вручную, менее предрасположены к ошибкам. Однако автоматизированные процессы приносят риски, для управления которыми должны быть предусмотрены программы надлежащего управления технологиями и рисками инфраструктуры.

52. Использование продуктов, операций, процессов и каналов поставки, связанных с технологиями, подвергает банк стратегическому, операционному и репутационному рискам, а также возможности понести существенные финансовые потери. Следовательно, в банке должен быть предусмотрен интегрированный подход к идентификации, измерению, мониторингу и управлению технологическими рисками.<sup>21</sup> В основе надлежащего управления технологическим риском лежат подходы, используемые при управлении операционным риском и включающие:

- (a) руководство и управленческий контроль, позволяющие убедиться в том, что технологии, включая соглашения об аутсорсинге, соответствуют целям деятельности банка и поддерживают их;
- (b) политики и процедуры, способствующие идентификации и оценке риска;

---

<sup>20</sup>Например, в случаях, когда риск предположительно низкий и низкая маржа торговой деятельности генерирует высокие доходы, может возникнуть вопрос, не стало ли получение данных доходов результатом нарушения внутреннего контроля.

<sup>21</sup>См. также документы Комитета "Risks in Computer and Telecommunication System", июль 1989, и "Risk Management Principles for Electronic Banking", май 2001.

- (с) установление риск-аппетита и толерантности к риску, а также определение ожидаемых результатов деятельности, что способствует осуществлению контроля рисков и управлению ими;
- (d) создание эффективной среды контроля и использование стратегий передачи риска в целях его ограничения (снижения); а также
- (e) процессы мониторинга, проверяющие на соответствие установленным политикой пороговым значениям или лимитам.

53. Руководство должно обеспечить наличие надлежащей технологической инфраструктуры<sup>22</sup>, соответствующей требованиям текущей и долгосрочной деятельности банка, путем создания мощностей, достаточных для функционирования как в обычных условиях рынка, так и в критические периоды стресса; обеспечения целостности, защиты и доступности данных и систем; поддержания подхода к всестороннему управлению риском на интегрированной основе. Слияния и поглощения, приводящие к фрагментированной и разрозненной инфраструктуре, меры по снижению затрат или недостаток инвестиций могут оказать негативное влияние на способность банка собирать и анализировать информацию о риске с разных сторон или на консолидированной основе; управлять риском и представлять отчетность по нему как в разрезе бизнес-линий, так и всей структуры банка, или осуществлять управление и контроль за риском в периоды значительного роста. Руководство должно на постоянной основе осуществлять соответствующие вложения капитала или, в противном случае, предусматривать надежную инфраструктуру, в особенности перед завершением слияний, началом реализации стратегий быстрого роста или вводом новых продуктов.

54. Аутсорсинг<sup>23</sup> – это привлечение третьей стороны – аффилированной с группой или неаффилированной сторонней организации – для выполнения отдельных видов работ (деятельности) от имени банка. Аутсорсинг может использоваться при обработке операций или в бизнес-процессах. Несмотря на то, что аутсорсинг способствует управлению расходами, предоставлению специальных знаний, расширению предложения продуктов и улучшению услуг, он также влечет риски, управление которыми руководство банка должно

---

<sup>22</sup>Технологическая инфраструктура подразумевает физическое и логическое сочетание информационных технологий и систем связи, отдельных компонентов аппаратных средств и программного обеспечения, данных, а также операционных сред.

<sup>23</sup>См. также документ Совместного Форума Комитета "Outsourcing in Financial Services", февраль 2005.

осуществлять. Совет директоров и высшее руководство несут ответственность за понимание операционных рисков, связанных с аутсорсингом, и обеспечение эффективных политик и практик управления риском, связанным с аутсорсингом. Политики и деятельность по управлению риском, связанным с аутсорсингом, должны включать:

- (a) процедуры определения целесообразности и способов передачи отдельных видов деятельности в аутсорсинг;
- (b) процессы руководства принципом должной осмотрительности при выборе возможных поставщиков услуг;
- (c) формирование надлежащей структуры аутсорсинга, включающей права собственности на информацию и обеспечение ее конфиденциальности, в том числе прекращение прав;
- (d) программы управления и мониторинга рисков, связанных с аутсорсингом, в том числе с финансовым состоянием поставщика услуг;
- (e) создание эффективной среды контроля в банке и у поставщика услуг;
- (f) разработку работоспособных планов действий на случай непредвиденных обстоятельств; а также
- (g) исполнение комплексных контрактов и (или) соглашений об оказании услуг с четким разграничением ответственности между поставщиком услуг и банком.

55. В случаях, когда внутренний контроль не соответствует необходимому уровню управления риском, а отказ от риска не является целесообразным, руководство в дополнение к контролю может привлекать другую сторону для передачи ей риска, как, например, при страховании. Совет директоров должен определять максимально возможный размер величины потерь, который банк склонен и способен принимать в соответствии со своими финансовыми возможностями, а также проводить ежегодную проверку программы управления рисками банка и страхованием. Несмотря на то, что банки должны самостоятельно определять свою потребность в отдельных видах страхования или передаче риска, законодательства многих стран предусматривают обязательные требования, которые должны соблюдаться<sup>24</sup>.

---

<sup>24</sup>См. также документ Комитета "Recognising the risk-mitigating impact of insurance in operational risk modelling", октябрь 2010.

56. Поскольку передача риска является несовершенной заменой надлежащему контролю и программам управления рисками, банки должны рассматривать ее в качестве инструмента дополняющего, но не замещающего всесторонний внутренний контроль операционного риска. Наличие механизмов быстрой идентификации, определения и устранения различных недостатков, связанных с операционным риском, может значительно снижать воздействие данного риска. Кроме того, следует тщательно рассматривать, насколько реально снижается риск, передается в другие сферы или сектора деятельности либо создаются новые риски (например, риск контрагента) при использовании таких инструментов ограничения (снижения), как страхование.

### **Устойчивость и непрерывность деятельности**

**Принцип 10: В банках должны быть разработаны планы обеспечения непрерывности и устойчивости деятельности для поддержания способности работать на непрерывной основе, а также ограничения потерь в случае возникновения событий, влекущих серьезные нарушения непрерывности функционирования.<sup>25</sup>**

57. Банки подвержены событиям, оказывающим негативное воздействие, часть из которых может повлечь серьезные последствия и в итоге привести к неспособности банка исполнять отдельные обязательства. Инциденты, наносящие ущерб или приводящие к недоступности услуг банка, телекоммуникационных или информационных технологических инфраструктур, либо пандемическое явление, влияющее на человеческие ресурсы, могут привести банк к существенным финансовым потерям так же, как и более крупные нарушения функционирования финансовой системы. С целью обеспечения устойчивости к риску, банк должен разработать планы обеспечения непрерывности деятельности, учитывая характер, объемы и сложность операций. Данные планы должны учитывать различные типы вероятных или приближенных к реальности сценариев непредвиденных обстоятельств, к которым банк может быть уязвим.

58. Управление непрерывностью деятельности должно сочетать в себе анализ воздействия на деятельность банка, стратегии восстановления, тестирование, программы обучения, ознакомления, а также

---

<sup>25</sup>Более подробное описание надлежащих принципов обеспечения непрерывности деятельности приведено в Документе Комитета "High-level principles for business continuity", август 2006.



взаимодействия и управления в кризисных условиях. Банк должен определять критические операции<sup>26</sup>, основные внутренние и внешние зависимости<sup>27</sup>, а также соответствующие уровни устойчивости. Вероятные сценарии нарушений деятельности должны оцениваться с точки зрения негативного воздействия на финансовое состояние, операции и репутацию банка, а итоговая оценка риска должна являться основой для определения приоритетов и целей восстановления деятельности банка. В планах обеспечения непрерывности деятельности должны быть определены стратегии действий на случай непредвиденных обстоятельств, процедуры восстановления и возобновления деятельности, а также планы взаимодействия, обеспечивающие предоставление информации руководству, сотрудникам банка, регуляторным органам, клиентам, поставщикам и, при необходимости, государственным органам.

59. Банк должен периодически пересматривать планы обеспечения непрерывности деятельности для поддержания соответствия стратегий действий на случай непредвиденных обстоятельств текущим операциям, рискам и угрозам, требованиям к устойчивости, а также приоритетам восстановления. В банке должны быть внедрены программы обучения и ознакомления с целью обеспечения эффективного исполнения планов действий на случай непредвиденных обстоятельств. Банк должен проводить периодическую проверку работоспособности планов для поддержания соответствия целей восстановления и возобновления деятельности временным ограничениям данных процессов. По возможности банк должен проводить проверку работоспособности планов восстановления и обеспечения непрерывности деятельности с привлечением основных поставщиков услуг. Результаты официальной проверки работоспособности должны доводиться до сведения руководства.

## **Роль раскрытия информации**

**Принцип 11: Раскрытие информации должно предоставлять заинтересованным сторонам возможность оценивать подход банка к управлению операционным риском.**

---

<sup>26</sup>Операции банка включают средства, человеческие ресурсы и процессы предоставления продуктов и оказания услуг или осуществления основных видов деятельности, а также технологические системы и данные.

<sup>27</sup>Внешние зависимости включают коммунальные предприятия, вендоров и третьих сторон-поставщиков услуг.

60. Раскрытие банком соответствующей информации об управлении операционным риском может способствовать прозрачности и развитию лучшей практики банковской сферы через рыночную дисциплину. Объем и вид раскрываемой информации должны соответствовать объему, риск-профилю и сложности операций банка, а также развивающейся практике банковской сферы.

61. Способ раскрытия банком информации о своих подходах к управлению операционным риском должен позволять заинтересованным сторонам определять, насколько эффективно банк проводит идентификацию, оценку, мониторинг и контроль/ограничение (снижение) операционного риска.

62. Раскрытие информации должно соответствовать применяемым высшим руководством и Советом директоров способам оценки операционного риска и управления им<sup>28</sup>.

63. Банк должен располагать официальной политикой раскрытия информации, утвержденной Советом директоров, в которой установлен подход банка к определению характера раскрываемой информации, а также внутренний контроль процесса ее раскрытия. Кроме того, банки должны внедрить процесс оценки правомерности раскрытия информации, включая обоснование и периодичность данного раскрытия<sup>29</sup>.

---

<sup>28</sup>Базельский Комитет по банковскому надзору, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version", Раздел V (Операционный риск), п. 646, Базель, июнь 2006, п. 810.

<sup>29</sup>Базельский Комитет по банковскому надзору, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version", Раздел V (Операционный риск), п. 646, Базель, июнь 2006, п. 821.

## Приложение

### Справочные материалы

A Framework for Internal Control Systems in Banking Organisations (BCBS, сентябрь 1998)

Internal audit in banks and the supervisor's relationship with auditors (BCBS, август 2001)

The relationship between banking supervisors and bank's external auditors (BCBS, январь 2002)

Core Principles for Effective Banking Supervision (BCBS, октябрь 2006)

Core Principles Methodology (BCBS, октябрь 2006)

High-Level Principles for Business Continuity (BCBS, август 2006)

Outsourcing in financial services (Joint Forum, февраль 2005)

Risk Management Principles for Electronic Banking (BCBS, май 2001)

Risks in Computer and Telecommunication Systems (BCBS, июль 1989)

Principles for Enhancing Corporate Governance (BCBS, октябрь 2010)

Recognising the risk-mitigating impact of insurance in operational risk modelling (BCBS, октябрь 2010)

High-level principles for the cross-border implementation of the New Accord (BCBS, август 2003)

Principles for home-host supervisory cooperation and allocation mechanisms in the context of Advanced Measurement Approaches (AMA) (BCBS, ноябрь 2007)