Термины и сокращения

BCBS — Basel Committee on Banking Supervision — Базельский комитет по банковскому надзору.

BIS — Bank for International Settlements — Банк международных расчётов.

ORMF — Operational Risk Management Framework — система управления операционным риском.

CORF — Common Operational Resilience Framework — единая система операционной устойчивости.

RCSA — Risk and Control Self-Assessment — самооценка рисков и контролей.

KRI — Key Risk Indicator — ключевой индикатор риска.

BIA — Business Impact Analysis — анализ влияния на деятельность.

BCP — Business Continuity Plan — план непрерывности деятельности.

RTO — Recovery Time Objective — целевое время восстановления.

RPO — Recovery Point Objective — целевая точка восстановления.

ICT — Information and Communication Technology — информационно-коммуникационные технологии.

MIS — Management Information System — управленческая информационная система.

FSB — Financial Stability Board — Совет по финансовой стабильности.

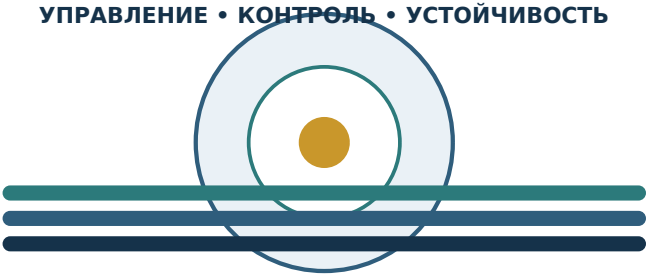
AMA — Advanced Measurement Approaches — усовершенствованные подходы к измерению.

Глоссарий добавлен в редакции PSR Online 115. Далее следует исходный русский перевод.

БАЗЕЛЬСКИЙ КОМИТЕТ ПО БАНКОВСКОМУ НАДЗОРУ

Пересмотр принципов надлежащего управления операционным риском

Март 2021



Полный неофициальный перевод на русский язык
в формате электронной книги PDF

Источник: Bank for International Settlements (BIS) • ISBN
978-92-9259-468-8

О переводе

Это неофициальный русский перевод документа Basel Committee on Banking Supervision «Revisions to the Principles for the Sound Management of Operational Risk» (март 2021). Нумерация принципов, пунктов и примечаний сохранена. Термины ORMF, CORF, ICT/ИКТ, BCP, BIA, RTO и RPO при первом употреблении раскрываются и далее используются в сокращённом виде.

> *Для нормативного, юридического или надзорного применения следует сверяться с англоязычным оригиналом BIS. Иллюстративные схемы в этой версии являются редакционными и добавлены только для удобства чтения; они не являются частью оригинального документа.*

Ключевые термины: операционный риск; операционная устойчивость; три линии защиты; риск-аппетит и толерантность; внутренний контроль; ИКТ-риск; непрерывность деятельности; передача риска и страхование.

Содержание

Пересмотр принципов надлежащего управления операционным риском

1. Введение

Базельский комитет по банковскому надзору (далее - «Комитет») впервые представил свои «Принципы надлежащего управления операционным риском» (далее - «Принципы») в 2003 году, а затем пересмотрел их в 2011 году с учётом уроков глобального финансового кризиса 2007-2009 годов. В 2014 году Комитет провёл обзор практики внедрения Принципов.[1] Целями обзора были: (i) оценить, в какой степени банки внедрили Принципы; (ii) выявить существенные пробелы во внедрении; и (iii) выделить новые и заслуживающие внимания практики управления операционным риском в банках, которые на тот момент не были охвачены Принципами.

Обзор 2014 года показал, что ряд принципов внедрён недостаточно полно и для облегчения их практического применения требуются дополнительные рекомендации в следующих областях:

a) инструменты выявления и оценки риска, включая самооценку рисков и контролей (RCSA), ключевые индикаторы риска, внешние данные об убытках, картирование бизнес-процессов, сравнительный анализ и мониторинг планов действий, сформированных по результатам применения различных инструментов управления операционным риском;

b) программы и процессы управления изменениями, включая их эффективный мониторинг;

c) реализация модели трёх линий защиты, прежде всего более чёткое распределение ролей и обязанностей;

d) надзор со стороны совета директоров и высшего руководства;

e) формулирование заявлений о риск-аппетите и толерантности к операционному риску;

f) раскрытие информации о рисках.

Комитет также признал, что Принципы 2011 года недостаточно полно отражали некоторые важные источники операционного риска, в частности риски, возникающие в сфере информационно-коммуникационных технологий (ИКТ).[2] Поэтому в пересмотренный документ включён отдельный принцип, посвящённый управлению ИКТ-риском. Другие изменения были внесены для согласования документа с новой рамочной системой операционного риска в реформах Базель III.[3]

Учитывая возросший потенциал серьёзных нарушений банковской деятельности из-за пандемий, стихийных бедствий, разрушительных киберинцидентов или технологических отказов, Комитет также разработал принципы операционной устойчивости,[4] которые перекликаются с рядом принципов настоящего документа.

[1] BCBS, Review of the Principles for Sound Management of Operational Risk, октябрь 2014 г., www.bis.org/publ/bcbs292.pdf.

[2] Риски ненадлежащего поведения и юридические риски, включая риски, связанные с отмыванием денег или финансированием терроризма, по-прежнему остаются важными вопросами. В этом контексте финансовым организациям следует продолжать совершенствовать способность управлять операционным риском.

[3] BCBS, Basel III: finalising post-crisis reforms, декабрь 2017 г., www.bis.org/bcbs/publ/d424.pdf.

[4] «Операционная устойчивость» определяется как способность банка обеспечивать выполнение критически важных операций в условиях нарушения деятельности. Такая способность позволяет банку выявлять угрозы и потенциальные сбои и защищаться от них, реагировать и

адаптироваться, восстанавливаться после нарушающих событий и извлекать из них уроки, чтобы минимизировать влияние на выполнение критически важных операций. При рассмотрении операционной устойчивости банк должен исходить из того, что нарушения произойдут, и учитывать свой общий риск-аппетит и допустимый уровень нарушения деятельности. «Допустимый уровень нарушения» - это уровень нарушения от любого вида операционного риска, который банк готов принять в диапазоне тяжёлых, но правдоподобных сценариев. См. BCBS, Principles for operational resilience, март 2021 г., www.bis.org/bcbs/publ/d516.htm.

2. Компоненты управления операционным риском

Принципы, изложенные в этом документе для банков, охватывают корпоративное управление; среду управления рисками; информационно-коммуникационные технологии; планирование непрерывности деятельности; а также роль раскрытия информации. Эти элементы не следует рассматривать изолированно: они являются взаимосвязанными компонентами рамочной системы управления операционным риском (operational risk management framework, ORMF) и общей системы управления рисками группы, включая операционную устойчивость.

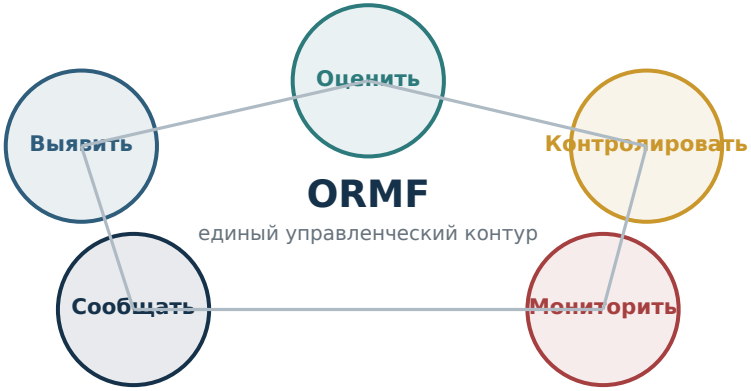


Иллюстрация: операционный риск управляется как непрерывный цикл - от выявления и оценки до контроля, мониторинга и отчётности.

Публикуя этот документ, Комитет стремится повысить эффективность управления операционным риском во всей банковской системе. По мнению Комитета, Принципы отражают надлежащие практики, применимые ко всем банкам. Вместе с тем при их внедрении банкам рекомендуется учитывать характер, размер, сложность и профиль риска своей деятельности.

3. Управление операционным риском

1. В рамках требований к капиталу операционный риск определяется как риск убытков вследствие неадекватных или неработающих внутренних процессов, действий людей и систем либо внешних событий. Это определение включает юридический риск, но исключает стратегический и репутационный риски.

2. Операционный риск присущ всем банковским продуктам, видам деятельности, процессам и системам, а эффективное управление им является фундаментальным элементом программы управления рисками банка. Надлежащее

управление операционным риском отражает эффективность совета директоров и высшего руководства в управлении портфелем продуктов, видов деятельности, процессов и систем. В необходимых случаях при управлении операционным риском банку следует также учитывать стратегический и репутационный риски.

3. Хотя управление операционным риском и операционная устойчивость преследуют разные цели, они тесно взаимосвязаны. Эффективная система управления операционным риском и высокий уровень операционной устойчивости совместно снижают частоту и последствия событий операционного риска.

4. Надлежащее управление рисками позволяет банку лучше понимать и снижать свой профиль риска. Управление рисками включает выявление рисков банка; измерение и оценку подверженности этим рискам там, где это возможно; постоянный мониторинг подверженности и соответствующей потребности в капитале; принятие мер по контролю или снижению подверженности; а также отчётность перед высшим руководством и советом директоров о рисках и капитальных позициях банка. Внутренние контроли обычно встроены в повседневную деятельность банка и предназначены, насколько это возможно, для обеспечения эффективности и результативности деятельности, надёжности, своевременности и полноты информации, а также соблюдения применимых законов и нормативных требований.

5. Надлежащее внутреннее корпоративное управление является основой эффективной ORMF. Управление операционным риском имеет сходства с управлением кредитным и рыночным риском, но также обладает особенностями. Функция корпоративного управления операционным риском должна быть полностью

интегрирована в общую структуру управления рисками банка.

6. Банки обычно опираются на три линии защиты: (i) руководство бизнес-подразделений;[5] (ii) независимую корпоративную функцию управления операционным риском (corporate operational risk management function, CORF);[6] и (iii) независимое подтверждение.[7] Степень формализации этих трёх линий зависит от характера, размера и сложности банка, а также от профиля риска его деятельности.

Иллюстрация: три линии защиты различаются ролями, но должны работать в единой системе управления риском.

7. Банк должен обеспечить, чтобы каждая линия защиты:

a) имела достаточные ресурсы - бюджет, инструменты и персонал;

b) имела чётко определённые роли и обязанности;

c) получала постоянное и достаточное обучение;

d) поддерживала надлежащую культуру управления рисками во всей организации;

e) взаимодействовала с другими линиями защиты, усиливая ORMF.

Если в одном бизнес-подразделении присутствуют функции как первой, так и второй линии защиты, банк должен документально определить и разделить их обязанности, особо подчёркивая независимость второй линии.

8. Комитет отмечал, что, несмотря на широкое внедрение модели трёх линий защиты, неясность ролей и обязанностей иногда снижает её эффективность.[8] Поэтому пересмотр Принципов дополнительно подчёркивает необходимость применять эту модель адекватно и соразмерно для управления всеми подкатегориями операционного риска, включая ИКТ-риск.

9. В отраслевой практике первой линией защиты является руководство бизнес-подразделений. Надлежащее управление операционным риском исходит из того, что руководство бизнес-подразделения отвечает за выявление и управление рисками, присущими продуктам, видам деятельности, процессам и системам, за которые оно отвечает. В банке должна быть политика, чётко определяющая роли и обязанности соответствующих бизнес-подразделений.[9] К обязанностям эффективной первой линии защиты по формированию надлежащей культуры управления операционным риском относятся:

a) выявление и оценка существенности операционных рисков, присущих соответствующим бизнес-подразделениям, с использованием инструментов управления операционным риском;

b) создание надлежащих контролей для снижения присущих операционных рисков и оценка конструкции и эффективности этих контролей с помощью инструментов управления операционным риском;

c) сообщение о недостатке у бизнес-подразделений ресурсов, инструментов или обучения, необходимых для выявления и оценки операционных рисков;

d) мониторинг и отчётность по профилям операционного риска бизнес-подразделений[10] и обеспечение соблюдения установленного заявления о риск-аппетите и толерантности;

e) отчётность об остаточных операционных рисках, не сниженных контролями, включая события операционных убытков, недостатки контролей, недостатки процессов и несоблюдение установленных допусков по операционному риску.

10. Функционально независимая CORF обычно является второй линией защиты. К обязанностям эффективной второй линии относятся:

a) формирование независимой позиции относительно: (i) выявленных бизнес-подразделениями существенных операционных рисков; (ii) конструкции и эффективности ключевых контролей; и (iii) толерантности к риску;

b) критическая оценка релевантности и последовательности применения бизнес-подразделениями инструментов управления операционным риском, измерительных процедур и систем отчётности, а также документирование доказательств такой действенной критической оценки;

c) разработка и поддержание политик, стандартов и руководств по управлению и измерению операционного риска;

d) проверка и участие в мониторинге и отчётности по профилю операционного риска;

e) разработка и проведение обучения по операционному риску и развитие риск-осведомлённости.

11. Степень независимости CORF может различаться между банками. В небольших банках независимость может обеспечиваться разделением обязанностей и независимой проверкой процессов и функций. В крупных банках CORF

должна иметь структуру подчинённости, независимую от бизнес-подразделений, создающих риск, и отвечать за проектирование, сопровождение и постоянное развитие ORMF в банке. Для оценки операционных рисков и контролей CORF обычно привлекает соответствующие корпоративные контрольные функции, например комплаенс, юридическую службу, финансы и ИТ. Банк должен иметь политику, которая чётко определяет роли и обязанности CORF с учётом размера и сложности организации.

12. Третья линия защиты предоставляет совету директоров независимое подтверждение надлежащего характера ORMF банка. Сотрудники этой функции не должны участвовать в разработке, внедрении и эксплуатации процессов управления операционным риском, выполняемых первыми двумя линиями. Проверки третьей линии обычно проводятся внутренним и/или внешним аудитом банка, но могут также выполняться иными надлежащим образом квалифицированными независимыми внешними сторонами. Объём и частота проверок должны быть достаточными для охвата всей деятельности и всех юридических лиц банка. Эффективная независимая проверка должна:

a) проверять конструкцию и внедрение систем управления операционным риском и связанных процессов корпоративного управления через первую и вторую линии защиты, включая независимость второй линии;

b) проверять процессы валидации, чтобы убедиться в их независимости и реализации в соответствии с установленными политиками банка;

c) убеждаться, что используемые банком системы количественной оценки достаточно надёжны: (i) обеспечивают целостность входных данных, допущений, процессов и методологии и (ii) формируют оценки

операционного риска, достоверно отражающие профиль операционного риска банка;

d) убеждаться, что руководство бизнес-подразделений своевременно, точно и надлежащим образом реагирует на выявленные вопросы и регулярно отчитывается совету директоров или его профильным комитетам по открытым и закрытым вопросам;

e) давать заключение об общей пригодности и достаточности ORMF и связанных процессов корпоративного управления во всём банке. Помимо проверки соблюдения утверждённых советом директоров политик и процедур, независимая проверка должна оценивать, соответствует ли ORMF потребностям и ожиданиям организации - например, корпоративному риск-аппетиту и толерантности, необходимости адаптации к изменяющимся условиям деятельности - а также законодательным и нормативным требованиям, договорным обязательствам, внутренним правилам и нормам этического поведения.

13. Поскольку управление операционным риском развивается, а деловая среда постоянно меняется, высшее руководство должно обеспечивать достаточную надёжность политик, процессов и систем ORMF, чтобы управлять риском и своевременно и надлежащим образом реагировать на операционные убытки. Совершенствование управления операционным риском в значительной степени зависит от готовности высшего руководства действовать проактивно и оперативно и надлежащим образом реагировать на вопросы, поднимаемые специалистами по операционному риску.

[5] Термин «бизнес-подразделение» используется широко и включает связанные функции поддержки, корпоративные и/или общие сервисные функции, например финансы, управление персоналом, операционную деятельность и технологии. Управление рисками и внутренний аудит не включаются, если иное прямо не указано.

[6] Помимо независимой функции управления операционным риском, ко второй линии защиты обычно также относится функция комплаенс.

[7] Независимое подтверждение включает верификацию и валидацию. Верификация ORMF проводится периодически, обычно внутренним и/или внешним аудитом банка, но может выполняться и квалифицированными независимыми внешними сторонами. Верификация проверяет эффективность ORMF в целом и процессов валидации. Валидация обеспечивает достаточную надёжность систем количественной оценки и подтверждает целостность входных данных, допущений, методологий, процессов и результатов. Валидация критически важна для хорошо функционирующей ORMF.

[8] См. BCBS, Cyber resilience: range of practices, декабрь 2018 г., https://www.bis.org/bcbs/publ/d454.pdf.

[9] В сложных банковских структурах к «соответствующим бизнес-подразделениям», вероятно, относятся и функции поддержки, например подразделения информационных систем.

[10] Профили операционного риска описывают подверженность бизнес-подразделений операционному риску и оценки их контрольной среды, а также диапазон потенциальных последствий - от ожидаемых до тяжёлых убытков. Такие профили обычно дают руководству и совету директоров представление о подверженности операционному риску на уровне, достаточном для принятия решений и осуществления надзора.

4. Принципы надлежащего управления операционным риском

Принцип 1. Совет директоров должен играть ведущую роль в формировании сильной культуры управления рисками, которую реализует высшее руководство.[11] Совет директоров и высшее руководство должны создавать корпоративную культуру, основанную на надлежащем управлении рисками, устанавливать стандарты и стимулы для профессионального и ответственного поведения и обеспечивать соответствующее обучение сотрудников вопросам управления рисками и этики.

14. Банки с сильной культурой управления рисками и этичного ведения бизнеса менее подвержены разрушительным событиям операционного риска и лучше подготовлены к эффективному реагированию на такие события. Действия совета директоров и высшего руководства, а также политики, процессы и системы управления рисками банка формируют основу надлежащей культуры управления рисками.

15. Совет директоров должен утвердить кодекс поведения или политику в области этики для управления риском ненадлежащего поведения. Такой кодекс или политика должны распространяться как на сотрудников, так и на членов совета директоров; устанавливать чёткие ожидания в отношении добросовестности и высочайших этических стандартов; определять допустимые деловые практики; запрещать конфликты интересов и ненадлежащее предоставление финансовых услуг, независимо от того, носит ли нарушение умышленный или неосторожный

характер. Кодекс или политика должны регулярно пересматриваться и утверждаться советом директоров и подтверждаться сотрудниками; надзор за их применением должен осуществляться старшим комитетом по этике или иным комитетом уровня совета директоров; документ должен быть общедоступным, например на сайте банка. Для отдельных должностей, например дилеров казначейства или высшего руководства, может устанавливаться отдельный кодекс поведения.

16. Руководство должно чётко формулировать ожидания и ответственность, чтобы сотрудники банка понимали свои роли и обязанности в управлении рисками, а также полномочия для принятия соответствующих действий.

17. Политика вознаграждения должна быть согласована с заявлением банка о риск-аппетите и толерантности, а также с общими требованиями безопасности и устойчивости, и должна надлежащим образом балансировать риск и вознаграждение.[12]

18. Высшее руководство должно обеспечить соответствующий уровень обучения по операционному риску на всех уровнях организации, включая руководителей бизнес-подразделений, руководителей внутренних контролей и старших руководителей. Содержание обучения должно учитывать уровень должности, роль и ответственность конкретных участников.

19. Сильная и последовательная поддержка управления операционным риском и этичного поведения со стороны совета директоров и высшего руководства убедительно подкрепляет кодексы поведения и этики, стратегии вознаграждения и программы обучения.

Принцип 2. Банки должны разработать, внедрить и поддерживать рамочную систему управления операционным риском, полностью интегрированную в общие процессы управления рисками банка. Конкретная ORMF зависит от ряда факторов, включая характер, размер, сложность и профиль риска банка.

20. Совет директоров и руководство банка должны понимать характер и сложность рисков, присущих портфелю банковских продуктов, услуг, видов деятельности и систем. Это является фундаментальной предпосылкой надлежащего управления рисками и особенно важно для операционного риска, поскольку он присущ всем продуктам, видам деятельности, процессам и системам.

21. Компоненты ORMF должны быть полностью интегрированы первой линией защиты в общие процессы управления рисками банка, надлежащим образом проверяться и подвергаться критической оценке второй линией, а также независимо проверяться третьей линией. ORMF должна быть встроена во все уровни организации, включая группу и бизнес-подразделения, а также новые бизнес-инициативы, продукты, виды деятельности, процессы и системы. Кроме того, результаты оценки операционного риска банка должны учитываться в общем процессе разработки бизнес-стратегии.

22. ORMF должна быть всесторонне и надлежащим образом документирована в политиках, утверждённых советом директоров, и включать определения операционного риска и операционного убытка. Недостаточно чёткое описание и классификация операционного риска и подверженности убыткам может существенно снизить эффективность ORMF.

23. Документация ORMF должна чётко:

a) определять структуры корпоративного управления, используемые для управления операционным риском, включая линии подчинённости и ответственность, а также полномочия и состав комитетов по управлению операционным риском;

b) содержать ссылки на соответствующие политики и процедуры управления операционным риском;

c) описывать инструменты выявления и оценки рисков и контролей, а также роли и обязанности трёх линий защиты при их использовании;

d) описывать принятые банком риск-аппетит и толерантность к операционному риску; пороги, триггеры существенной деятельности или лимиты для присущего и остаточного риска; а также утверждённые стратегии и инструменты снижения риска;

e) описывать подход банка к обеспечению надлежащего проектирования, внедрения и эффективной работы контролей;

f) описывать подход банка к установлению и мониторингу порогов или лимитов для присущей и остаточной подверженности риску;

g) предусматривать учёт рисков и контролей, реализованных всеми бизнес-подразделениями, например в библиотеке контролей;

h) устанавливать системы риск-отчётности и управленческой информации (MIS), формирующие своевременные и точные данные;

i) предусматривать единую таксономию терминов операционного риска для согласованности выявления риска, оценки подверженности и целей управления риском во всех бизнес-подразделениях.[13] Таксономия может разграничивать подверженность операционному

риску по типам событий, причинам, существенности и бизнес-подразделениям, где она возникает; также она может отмечать риски, которые частично или полностью представляют собой юридический риск, риск ненадлежащего поведения, модельный риск и ИКТ-риск, включая киберриск, а также риски на границе кредитного или рыночного риска;

j) предусматривать надлежащую независимую проверку и критическую оценку результатов процесса управления рисками;

k) требовать пересмотра и обновления политик по мере необходимости на основе постоянной оценки качества контрольной среды с учётом внутренних и внешних изменений или при любом существенном изменении профиля операционного риска банка.

Корпоративное управление[14]

Совет директоров

Принцип 3. Совет директоров должен утверждать и периодически пересматривать рамочную систему управления операционным риском и обеспечивать, чтобы высшее руководство эффективно внедряло политики, процессы и системы ORMF на всех уровнях принятия решений.

24. Совет директоров должен:

a) формировать культуру управления рисками и обеспечивать наличие в банке надлежащих процессов для понимания характера и масштаба операционного риска, присущего текущим и планируемым стратегиям и видам деятельности банка;

b) обеспечивать всесторонний и динамичный надзор за процессами управления операционным риском и их

полную интеграцию в общую систему управления всеми рисками организации либо координацию с ней;

c) давать высшему руководству чёткие указания относительно принципов, лежащих в основе ORMF, и утверждать соответствующие политики, разработанные высшим руководством для реализации этих принципов;

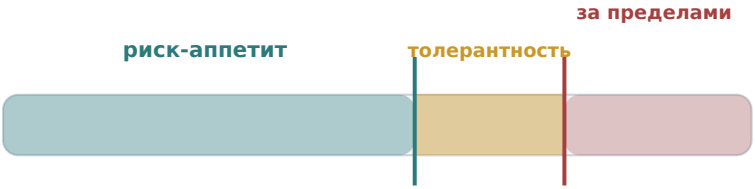
d) регулярно пересматривать и оценивать эффективность ORMF и утверждать её, чтобы убедиться, что банк выявляет и управляет операционным риском, возникающим из-за внешних рыночных изменений и иных факторов среды, а также рисками, связанными с новыми продуктами, видами деятельности, процессами или системами, включая изменения профилей риска и приоритетов, например изменение объёмов бизнеса;

e) обеспечивать эффективную независимую проверку ORMF третьей линией защиты - аудитом или иными надлежащим образом подготовленными независимыми внешними сторонами;

f) обеспечивать, чтобы по мере развития лучших практик руководство использовало соответствующие достижения.[15]

25. Сильные внутренние контроли являются критически важным элементом управления операционным риском. Совет директоров должен устанавливать чёткие линии управленческой ответственности и подотчётности за создание сильной контрольной среды. Контроли должны регулярно пересматриваться, мониториться и тестироваться, чтобы подтверждать их продолжающуюся эффективность. Контрольная среда должна обеспечивать надлежащую независимость и разделение обязанностей между функциями управления операционным риском, бизнес-подразделениями и функциями поддержки.

Принцип 4. Совет директоров должен утверждать и периодически пересматривать заявление о риск-аппетите и толерантности к операционному риску,[16] которое описывает характер, виды и уровни операционного риска, которые банк готов принять.



Границы должны быть понятны, измеримы там, где это возможно, и смотреть вперёд.

Иллюстрация: риск-аппетит задаёт целевую область принятия риска, толерантность - допустимое отклонение; выход за границы требует реакции.

26. Заявление о риск-аппетите и толерантности к операционному риску должно разрабатываться под руководством совета директоров и быть связано с краткосрочными и долгосрочными стратегическими и финансовыми планами банка. С учётом интересов клиентов и акционеров банка, а также регуляторных требований эффективное заявление должно:

a) быть простым для коммуникации и, следовательно, понятным всем заинтересованным сторонам;

b) включать ключевую исходную информацию и допущения, лежавшие в основе бизнес-планов банка на момент утверждения;

c) содержать формулировки, ясно объясняющие мотивы принятия либо избегания определённых видов риска, и

устанавливать границы или индикаторы - количественные или качественные - для мониторинга таких рисков;

d) обеспечивать соответствие стратегий и лимитов риска бизнес-подразделений и юридических лиц, где это применимо, общебанковскому заявлению о риск-аппетите;

e) быть ориентированным на будущее и, где применимо, подвергаться сценарному анализу и стресс-тестированию, чтобы банк понимал, какие события способны вывести его за пределы заявленных риск-аппетита и толерантности.

27. Совет директоров должен утверждать и регулярно пересматривать приемлемость лимитов и общего заявления о риск-аппетите и толерантности к операционному риску. Такой пересмотр должен учитывать текущие и ожидаемые изменения внешней среды, включая регуляторный контекст во всех юрисдикциях присутствия; текущий или предстоящий существенный рост объёмов бизнеса или деятельности; качество контрольной среды; эффективность стратегий управления или снижения риска; опыт убытков; а также частоту, объём или характер нарушений лимитов. Совет директоров должен контролировать соблюдение заявления руководством и обеспечивать своевременное выявление и устранение нарушений.

Высшее руководство

Принцип 5. Высшее руководство должно разработать для утверждения советом директоров чёткую, эффективную и надёжную структуру корпоративного управления с хорошо определёнными, прозрачными и последовательными линиями ответственности. Высшее руководство отвечает за последовательное внедрение и поддержание по всей организации политик, процессов и систем управления операционным риском во всех существенных продуктах, видах деятельности, процессах и системах банка в соответствии с заявлением банка о риск-аппетите и толерантности.

28. Высшее руководство отвечает за создание и поддержание надёжных механизмов критической оценки и эффективных процессов решения проблем. Они должны включать системы регистрации, отслеживания и, при необходимости, эскалации вопросов до их разрешения. Банк должен уметь продемонстрировать, что подход трёх линий защиты работает удовлетворительно, и объяснить, каким образом совет директоров, независимый комитет совета по аудиту и высшее руководство обеспечивают его надлежащее внедрение и функционирование.

29. Высшее руководство должно преобразовать утверждённую советом директоров ORMF в конкретные политики и процедуры, которые можно внедрять и проверять в различных бизнес-подразделениях. Полномочия, ответственность и линии отчётности должны быть распределены ясно, чтобы поддерживать подотчётность и обеспечивать наличие ресурсов, необходимых для управления операционным риском в соответствии с риск-аппетитом и толерантностью банка. Кроме того,

высшее руководство должно обеспечить, чтобы процесс управленческого надзора соответствовал рискам, присущим деятельности конкретного бизнес-подразделения.

30. Высшее руководство должно обеспечивать эффективную координацию и коммуникацию сотрудников, отвечающих за операционный риск, с сотрудниками, отвечающими за кредитный, рыночный и иные риски, а также с теми, кто отвечает за закупку внешних услуг, включая страховую передачу риска и иные отношения с третьими сторонами, в том числе аутсорсинг. Отсутствие такой координации может привести к существенным пробелам или дублированию в общей программе управления рисками банка.

31. Руководители CORF должны занимать в банке достаточно высокий статус для эффективного выполнения своих обязанностей; в идеале это подтверждается должностным уровнем, сопоставимым с руководителями функций управления кредитным, рыночным риском и риском ликвидности.

32. Высшее руководство должно обеспечить, чтобы деятельность банка выполнялась сотрудниками, обладающими необходимым опытом, техническими компетенциями и доступом к ресурсам. Сотрудники, контролирующие и обеспечивающие соблюдение риск-политики организации, должны иметь полномочия, независимые от подразделений, за которыми они осуществляют надзор.

33. Структура корпоративного управления банка должна соответствовать характеру, размеру, сложности и профилю риска его деятельности. При проектировании структуры управления операционным риском банк должен учитывать:

а) Структуру комитетов. Надлежащая отраслевая практика для крупных и сложных организаций с центральной

групповой функцией и отдельными бизнес-подразделениями - использование созданного советом директоров общекорпоративного комитета по рискам, который осуществляет надзор за всеми рисками и которому подотчётен управленческий комитет по операционному риску. В зависимости от характера, размера и сложности банка общекорпоративный комитет может получать информацию от комитетов по операционному риску по странам, бизнес-направлениям или функциональным областям. Более небольшие и менее сложные организации могут использовать более плоскую структуру, в которой операционный риск контролируется непосредственно комитетом совета директоров по рискам;

b) Состав комитетов. Надлежащая отраслевая практика предполагает, что в состав комитетов по операционному риску - либо комитета по рискам в небольших банках - входят участники с разноплановой экспертизой, охватывающей бизнес-деятельность, финансы, юридические, технологические и регуляторные вопросы, а также независимое управление рисками.[17]

c) Работу комитетов. Заседания должны проводиться с достаточной частотой, а время и ресурсы должны позволять продуктивное обсуждение и принятие решений. Документирование работы комитетов должно быть достаточным для последующей проверки и оценки их эффективности.

[11] Документ исходит из управленческой структуры, состоящей из совета директоров и высшего руководства. Комитет признаёт существенные различия между законодательными и регуляторными системами разных стран. В одних странах совет в основном или исключительно надзирает за исполнительным органом и может называться наблюдательным советом, не выполняя исполнительных функций; в других совет имеет более широкие полномочия и задаёт общую рамку управления банком. Поэтому термины «совет директоров» и «высшее руководство» используются здесь не для обозначения конкретных юридических конструкций, а как названия двух функций

принятия решений в банке.

[12] См. также BCBS, Report on the range of methodologies for the risk and performance alignment of remuneration, май 2011 г.; Financial Stability Forum, Principles for sound compensation practices, апрель 2009 г.; Financial Stability Board, FSB principles for sound compensation practices - implementation standards, сентябрь 2009 г.; а также инструментарий FSB Strengthening Governance Frameworks to Mitigate Misconduct Risk, апрель 2018 г.

[13] Несогласованная таксономия терминов операционного риска повышает вероятность того, что риски не будут выявлены и классифицированы или не будет определена ответственность за их оценку, мониторинг, контроль и снижение. Для киберриска в качестве отправной точки следует использовать Cyber Lexicon Совета по финансовой стабильности, опубликованный в ноябре 2018 г.

[14] См. также BCBS, Principles for enhancing corporate governance, октябрь 2010 г.

[15] См. документ Комитета 2006 г. International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version, пункт 718(xci).

[16] См. Corporate governance guidelines Комитета 2015 г., использующие определение FSB из Principles for an effective risk appetite framework 2013 г.: риск-аппетит - совокупный уровень и виды риска, которые банк заранее готов принять в пределах своей способности нести риск для достижения стратегических целей и бизнес-плана. «Толерантность к риску» - допустимое отклонение относительно установленного риск-аппетита.

[17] См. Corporate governance principles for banks Комитета 2015 г. - дополнительные требования к составу комитетов.

Среда управления рисками

Выявление и оценка

Принцип 6. Высшее руководство должно обеспечивать всестороннее выявление и оценку операционного риска, присущего всем существенным продуктам, видам деятельности, процессам и системам, чтобы присущие риски и стимулы были хорошо понятны.

34. Выявление и оценка риска являются фундаментальными характеристиками эффективной системы управления операционным риском и напрямую способствуют операционной устойчивости. Эффективное выявление риска учитывает как внутренние, так и внешние факторы. Надлежащая оценка риска позволяет банку лучше понимать свой профиль риска и наиболее эффективно распределять ресурсы и выбирать стратегии управления рисками.

35. К числу инструментов, используемых для выявления и оценки операционного риска, относятся:[18]

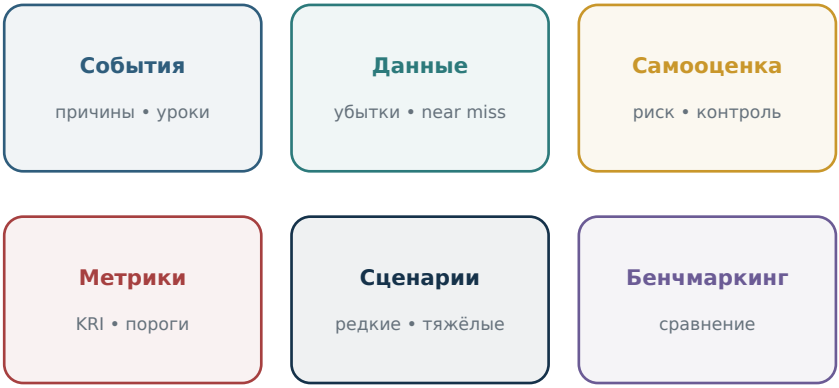


Иллюстрация: набор инструментов должен давать не одну оценку, а взаимно дополняющие сигналы о риске и качестве контролей.

a) Управление событиями. Когда в банке происходит событие операционного риска, его выявление, анализ, сквозное управление и отчётность должны следовать заранее определённому набору протоколов. Надлежащий подход обычно включает анализ событий для выявления новых операционных рисков, понимания первопричин и слабостей контролей и формирования ответных мер, предотвращающих повторение аналогичных событий. Эта информация используется в самооценке и особенно при оценке эффективности контролей.

b) Данные о событиях операционного риска. Банки часто ведут комплексный набор данных, который включает все существенные события, произошедшие в банке, и служит основой для оценки операционного риска. Обычно он содержит внутренние данные об убытках, события, едва не приведшие к убыткам (near miss), а где это возможно - внешние данные об операционных убытках, поскольку они информативны в отношении рисков, общих для отрасли. События обычно классифицируются по таксономии,

определённой политиками ORMF и единообразно применяемой во всём банке. Данные обычно включают дату события - дату возникновения, обнаружения и бухгалтерского признания - и, для событий с убытком, финансовый эффект. Если доступна информация о первопричинах, её желательно также включать. По возможности банкам рекомендуется собирать и использовать внешние данные о событиях операционного риска во внутреннем анализе.

c) Самооценки. Банки часто проводят самооценку операционных рисков и контролей на разных уровнях. Обычно оцениваются присущий риск - до учёта контролей, эффективность контрольной среды и остаточный риск - после учёта контролей; используются количественные и качественные элементы. Качественная часть учитывает как вероятность, так и последствия рискового события при определении рейтингов присущего и остаточного риска. Самооценки могут использовать картирование бизнес-процессов для выявления ключевых этапов процессов, видов деятельности и организационных функций, а также связанных рисков и слабых мест контроля. Оценки должны содержать достаточно подробные сведения о бизнес-среде, операционных рисках, первопричинах, контролях и оценке их эффективности, чтобы независимый проверяющий мог понять, как банк получил соответствующие рейтинги. Для свода этих сведений может вестись реестр рисков, позволяющий сформировать содержательное представление об общей эффективности контролей и облегчить надзор со стороны высшего руководства, комитетов по рискам и совета директоров.

d) Система мониторинга и подтверждения контролей. Включение соответствующей системы мониторинга и подтверждения контролей обеспечивает

структурированный подход к оценке, проверке, постоянному мониторингу и тестированию ключевых контролей. Анализ должен подтверждать, что контроли надлежащим образом спроектированы под выявленные риски и эффективно работают. Он также должен оценивать достаточность покрытия контролями, включая адекватные стратегии предотвращения, обнаружения и реагирования. Мониторинг и тестирование должны соответствовать различным операционным рискам и ключевым контролям в разных областях бизнеса.

e) Метрики. Используя данные о событиях операционного риска и оценки рисков и контролей, банки часто разрабатывают метрики для оценки и мониторинга своей подверженности. Это могут быть простые индикаторы, например число событий, или более сложные модели подверженности, когда это оправдано. Метрики дают сигналы раннего предупреждения о текущей работе бизнеса и контрольной среды и используются для отчётности по профилю операционного риска. Эффективные метрики явно связаны с соответствующими рисками и контролями. Наблюдение за метриками и их динамикой относительно согласованных порогов или лимитов даёт ценную информацию для управления рисками и отчётности.

f) Сценарный анализ. Это метод выявления, анализа и измерения диапазона сценариев, включая события с низкой вероятностью и тяжёлыми последствиями, некоторые из которых способны вызвать крупные операционные убытки. Обычно он проводится в форме рабочих сессий экспертов, в которых участвуют высшее руководство, бизнес-руководители, старшие специалисты по операционному риску и представители других функций - комплаенса, управления персоналом, ИТ-риска и др. - для определения факторов и диапазона последствий

потенциальных событий. В качестве входных данных обычно используются релевантные внутренние и внешние данные об убытках, результаты самооценок, сведения из системы мониторинга и подтверждения контролей, прогнозные метрики, анализ первопричин и процессная модель, если она применяется. Сценарный анализ может формировать диапазон последствий потенциальных событий и оценки воздействия для целей управления рисками, дополняя инструменты, основанные на исторических данных или текущих оценках. Его можно интегрировать с планами аварийного восстановления и непрерывности деятельности при тестировании операционной устойчивости. Из-за субъективности сценарного процесса для его целостности и последовательности особенно важны надёжная система корпоративного управления и независимая проверка.

g) Бенчмаркинг и сравнительный анализ. Они сопоставляют результаты различных инструментов измерения и управления рисками внутри банка, а также метрики банка с показателями других организаций отрасли. Сравнения помогают лучше понять профиль операционного риска. Например, сопоставление частоты и тяжести внутренних убытков с результатами самооценки может показать, насколько эффективно работает самооценка. Данные сценариев можно сравнивать с внутренними и внешними данными об убытках для лучшего понимания тяжести потенциальной подверженности рисковым событиям.

36. Банки должны обеспечивать, чтобы результаты применения инструментов оценки операционного риска:

a) основывались на точных данных, целостность которых обеспечивается надёжным корпоративным управлением и устойчивыми процедурами верификации и валидации;

b) надлежащим образом учитывались во внутренних механизмах ценообразования и измерения эффективности, а также при оценке бизнес-возможностей;

c) при необходимости становились основанием для планов действий или корректирующих планов, мониторинг которых осуществляет CORF.

37. Эти инструменты оценки также могут напрямую поддерживать подход банка к операционной устойчивости, особенно процедуры управления событиями, самооценки и сценарного анализа, поскольку позволяют выявлять и мониторить угрозы и уязвимости критически важных операций. Банки должны использовать результаты этих инструментов для совершенствования контролей и процедур операционной устойчивости в соответствии с Принципами операционной устойчивости Комитета.[19]

Принцип 7. Высшее руководство должно обеспечивать, чтобы процесс управления изменениями банка был всесторонним, надлежащим образом обеспеченным ресурсами и чётко распределённым между соответствующими линиями защиты.

38. Как правило, подверженность банка операционному риску меняется, когда банк инициирует изменения: начинает новые виды деятельности или разрабатывает новые продукты и услуги; выходит на незнакомые рынки или в новые юрисдикции; внедряет новые либо изменяет существующие бизнес-процессы или технологические системы; и/или ведёт деятельность географически удалённо от головного офиса. Управление изменениями должно оценивать эволюцию связанных рисков во времени - от возникновения до прекращения, например на всём жизненном цикле продукта.[20]

39. Банк должен иметь политики и процедуры, определяющие процесс выявления, управления, критической оценки, утверждения и мониторинга изменений на основе согласованных объективных критериев. Реализация изменений должна контролироваться специальными надзорными контролями. Политики и процедуры управления изменениями должны регулярно и независимо пересматриваться и обновляться и ясно распределять роли и обязанности в соответствии с моделью трёх линий защиты, в частности:

a) первая линия защиты должна проводить оценку операционных рисков и контролей новых продуктов, видов деятельности, процессов и систем, включая выявление и оценку требуемых изменений на этапах принятия решения и планирования, реализации и поствнедренческого анализа;

b) вторая линия защиты - CORF - должна критически оценивать оценки операционных рисков и контролей первой линии и контролировать внедрение надлежащих контролей или корректирующих действий. CORF должна охватывать все фазы процесса и обеспечивать надлежащее участие всех релевантных контрольных функций, например финансов, комплаенса, юридической службы, бизнеса, ИКТ и управления рисками.

40. Банк должен иметь политики и процедуры проверки и утверждения новых продуктов, видов деятельности, процессов и систем. Процесс проверки и утверждения должен учитывать:

a) присущие риски - включая юридические, ИКТ- и модельные риски - при запуске новых продуктов, услуг, видов деятельности и операций на незнакомых рынках, а также при внедрении новых процессов, персонала и систем, особенно при аутсорсинге;

b) изменения профиля операционного риска, риск-аппетита и толерантности банка, включая изменение риска существующих продуктов или видов деятельности;

c) необходимые контроли, процессы управления рисками и стратегии снижения риска;

d) остаточный риск;

e) изменения соответствующих порогов или лимитов риска;

f) процедуры и метрики для оценки, мониторинга и управления риском новых продуктов, услуг, видов деятельности, рынков, юрисдикций, процессов и систем.

41. До внедрения изменений процесс проверки и утверждения должен включать подтверждение достаточных инвестиций в человеческие ресурсы и технологическую инфраструктуру. Изменения должны мониториться во время и после внедрения, чтобы выявлять любые существенные отклонения от ожидаемого профиля операционного риска и управлять неожиданно возникшими рисками.

42. По возможности банки должны вести централизованный реестр своих продуктов и услуг, включая переданные на аутсорсинг, чтобы облегчить мониторинг изменений.

[18] Перечень не является исчерпывающим и не отражает всего разнообразия и степени сложности возможных методов анализа. Его следует рассматривать как ориентировочный, а не ограничивающий.

[19] Эти контроли и процедуры должны быть согласованы с выявлением угроз и уязвимостей и выполняться параллельно с ним в рамках подхода к операционной устойчивости, описанного в Принципе 2 документа Комитета Principles for operational resilience, март 2021 г.

[20] Жизненный цикл продукта или услуги включает различные стадии: разработку, текущие изменения, сохранение ранее действующих условий и закрытие. Уровень риска может, например, возрастать, когда новые продукты, виды деятельности, процессы или системы переходят от начального масштаба к уровню, создающему существенную выручку или критически важные для бизнеса операции.

Мониторинг и отчётность

Принцип 8. Высшее руководство должно внедрить процесс регулярного мониторинга профилей операционного риска и существенных подверженностей операционному риску. На уровнях совета директоров, высшего руководства и бизнес-подразделений должны действовать надлежащие механизмы отчётности, поддерживающие проактивное управление операционным риском.

43. Банк должен обеспечивать полноту, точность, согласованность и практическую применимость отчётности по всем бизнес-подразделениям и продуктам. Для этого первая линия защиты должна обеспечивать отчётность по любым остаточным операционным рискам, включая события операционного риска, недостатки контролей, недостатки процессов и несоблюдение допусков по операционному риску. Объём и содержание отчётов должны быть управляемыми и давать представление о профиле операционного риска банка и соблюдении заявления о риск-аппетите и толерантности; эффективному принятию решений мешают как избыток данных, так и их недостаток.

44. Отчётность должна быть своевременной, а банк должен уметь формировать отчёты как в нормальных, так и в стрессовых рыночных условиях.[21] Частота отчётности должна соответствовать уровню рисков, а также скорости и характеру изменений операционной среды. Результаты мониторинга должны включаться в регулярные отчёты руководству и совету директоров, как и оценки ORMF, выполненные внутренним/внешним аудитом и/или функциями управления рисками. Отчёты, формируемые надзорными органами или для них, где это уместно, также

должны доводиться внутри банка до высшего руководства и совета директоров.

45. Отчёты по операционному риску должны описывать профиль операционного риска банка, включая внутренние финансовые, операционные и комплаенс-индикаторы, а также внешнюю рыночную или иную информацию о событиях и условиях, релевантных для принятия решений. Отчёты должны включать:

a) нарушения заявления банка о риск-аппетите и толерантности, а также порогов, лимитов или качественных требований;

b) обсуждение и оценку ключевых и возникающих рисков;

c) подробности недавних существенных внутренних событий операционного риска и убытков, включая анализ первопричин;

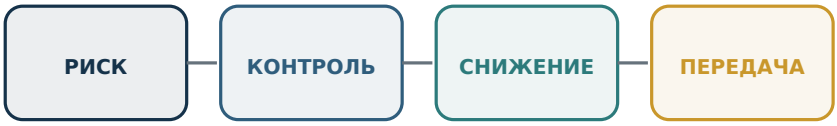
d) релевантные внешние события или изменения регулирования и их потенциальное влияние на банк.

46. Процессы сбора данных и риск-отчётности должны периодически анализироваться с целью повышения эффективности управления рисками и дальнейшего совершенствования политик, процедур и практик управления рисками.

[21] Отчётность должна соответствовать Principles for effective risk data aggregation and risk reporting Комитета: https://www.bis.org/publ/bcbs239.pdf.

Контроль и снижение риска

Принцип 9. Банки должны иметь сильную контрольную среду, использующую политики, процессы и системы; надлежащие внутренние контроли; а также надлежащие стратегии снижения и/или передачи риска.



Страхование дополняет внутренний контроль, но не заменяет его.

Иллюстрация: передача риска, включая страхование, находится после качественного внутреннего контроля и рассматривается как его дополнение.

47. Внутренние контроли должны быть спроектированы так, чтобы с разумной степенью уверенности обеспечивать эффективную и результативную работу банка; сохранность его активов; формирование надёжной финансовой отчётности; и соблюдение применимых законов и нормативных требований. Надлежащая программа внутреннего контроля состоит из четырёх компонентов, являющихся неотъемлемой частью процесса управления рисками: оценка риска, контрольные мероприятия, информация и коммуникация, мониторинговые мероприятия.[22]

48. Контрольные процессы и процедуры должны включать систему обеспечения соблюдения политик, нормативных

требований и законов. К основным элементам оценки соблюдения политик относятся:

a) проверки высшего уровня хода достижения установленных целей;

b) проверка соблюдения управленческих контролей;

c) проверка мер по устранению и разрешению случаев несоблюдения;

d) оценка требуемых согласований и разрешений для обеспечения подотчётности на соответствующем уровне управления;

e) отслеживание отчётности по утверждённым исключениям из порогов или лимитов, управленческим переопределениям и иным отклонениям от политик, нормативных требований и законов.

49. Контрольные процессы и процедуры должны определять, как банк обеспечивает поддержание операционной устойчивости как в обычных условиях, так и при нарушении деятельности, с учётом должной осмотрительности соответствующих функций и в соответствии с подходом банка к операционной устойчивости.

50. Эффективная контрольная среда требует также надлежащего разделения обязанностей. Распределение функций, создающее конфликтующие обязанности у одного человека или команды без двойного контроля - например, процесса, в котором две или более независимые стороны действуют совместно для защиты чувствительных функций или информации - либо иных компенсирующих мер может привести к сокрытию убытков, ошибок или иных ненадлежащих действий. Поэтому области потенциального конфликта интересов должны выявляться, минимизироваться и подвергаться тщательному независимому мониторингу и проверке.

51. Помимо разделения обязанностей и двойного контроля, банки должны при необходимости применять и другие традиционные внутренние контроли для управления операционным риском. К ним относятся:

a) чётко установленные полномочия и/или процессы утверждения;

b) тщательный мониторинг соблюдения установленных порогов или лимитов риска;

c) меры защиты доступа к активам и записям банка и их использования;

d) достаточность численности и обучения персонала для поддержания технической компетентности;

e) постоянные процессы выявления бизнес-подразделений или продуктов, доходность которых выглядит несоответствующей разумным ожиданиям;[23]

f) регулярная проверка и сверка операций и счетов;

g) политика отпусков, предусматривающая отсутствие должностных лиц и сотрудников на рабочем месте не менее двух последовательных недель.

52. Эффективное и надлежащее применение технологий может усиливать контрольную среду. Например, автоматизированные процессы менее подвержены ошибкам, чем ручные. Однако автоматизация создаёт новые риски, которыми необходимо управлять посредством надлежащего технологического управления и программ управления инфраструктурными рисками.

53. Использование технологических продуктов, видов деятельности, процессов и каналов предоставления услуг подвергает банк операционному риску и возможности существенных финансовых потерь. Поэтому банк должен применять интегрированный подход к выявлению, измерению, мониторингу и управлению технологическими

рисками на тех же принципах, что и управление операционным риском.

54. Обращение к внешним организациям, включая поставщиков услуг третьих сторон, может помогать снижать затраты, получать экспертизу, расширять продуктовые предложения и улучшать сервис, но одновременно создаёт риски, которыми руководство должно управлять. Совет директоров и высшее руководство отвечают за понимание операционных рисков, связанных с аутсорсингом, и наличие эффективных политик и практик управления такими рисками. Среди прочего следует учитывать концентрацию риска и сложность аутсорсинга. Политики управления рисками третьих сторон как часть ORMF и соответствующая деятельность по управлению рисками[24] должны охватывать:

a) процедуры определения того, может ли деятельность передаваться на аутсорсинг и каким образом;

b) процессы должной проверки потенциальных поставщиков услуг;

c) надлежащее структурирование аутсорсинговой схемы, включая вопросы права собственности и конфиденциальности данных, а также права на прекращение отношений;

d) программы управления и мониторинга рисков аутсорсинга, включая финансовое состояние поставщика услуг;

e) создание эффективной контрольной среды как в банке, так и у поставщика услуг, включая реестр переданных на аутсорсинг видов деятельности, метрики и отчётность для обеспечения надзора за поставщиком;

f) разработку жизнеспособных планов действий в чрезвычайных ситуациях;

g) заключение всеобъемлющих договоров и/или соглашений об уровне услуг с чётким распределением обязанностей между поставщиком аутсорсинга и банком;

h) доступ надзорных органов банков и органов по урегулированию к третьим сторонам.

55. В случаях, когда внутренние контроли не позволяют адекватно управлять риском, а выход из риска не является разумным вариантом, руководство может дополнить контроли передачей риска другой стороне, например посредством страхования. Совет директоров должен определить максимальный размер убытка, который банк готов и финансово способен принять, и ежегодно пересматривать программу управления рисками и страхованием. Конкретная потребность банка в страховании или иных способах передачи риска определяется индивидуально, при этом необходимо учитывать регуляторные требования соответствующих юрисдикций.

56. Поскольку передача риска является несовершенной заменой надлежащих контролей и программ управления рисками, банки должны рассматривать инструменты передачи риска как дополнение, а не замену полноценному внутреннему контролю операционного риска. Механизмы быстрого выявления, признания и исправления отдельных ошибок операционного риска или конкретной подверженности юридическому риску способны значительно снизить риск. Также необходимо тщательно оценивать, действительно ли такие инструменты снижения риска, как страхование, уменьшают риск, лишь передают его в другой сектор или область либо создают новый риск, например риск контрагента.

57. Банки должны иметь единую классификацию, методологию и процедуры управления операционным риском, установленные CORF.

[22] Документ Комитета Framework for Internal Control Systems in Banking Organisations, сентябрь 1998 г., более подробно рассматривает внутренний контроль.

[23] Например, если якобы низкорисковая низкомаржинальная торговая деятельность приносит высокую доходность, это может поставить вопрос, не достигнута ли такая доходность вследствие нарушения внутреннего контроля.

[24] Эти политики и мероприятия по управлению рисками должны быть согласованы с управлением критически важными операциями и зависимостями для целей операционной устойчивости и выполняться параллельно с ними. См. Basel Committee on Banking Supervision, Principles for operational resilience, март 2021 г.

Информационно-коммуникационные технологии

Принцип 10. Банки должны внедрить надёжную программу управления ИКТ-риском[25], согласованную с рамочной системой управления операционным риском.

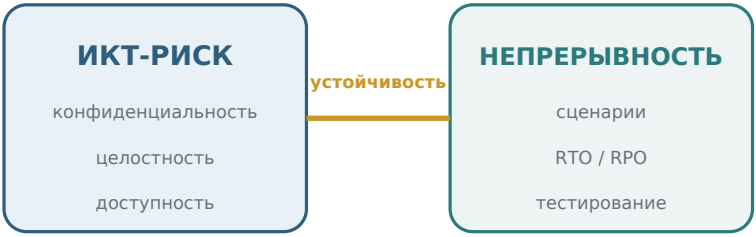


Иллюстрация: управление ИКТ-риском и непрерывностью деятельности совместно поддерживают операционную устойчивость.

58. Эффективность и безопасность ИКТ имеют первостепенное значение для надлежащего ведения банковской деятельности. Правильное использование и

реализация надлежащего управления ИКТ-риском повышают эффективность контрольной среды и являются фундаментальными для достижения стратегических целей банка. Оценка ИКТ-риска должна обеспечивать полноценную поддержку и облегчение банковских операций средствами ИКТ. Управление ИКТ-риском должно снижать подверженность операционному риску прямых убытков, юридических требований, репутационного ущерба, нарушений ИКТ и ненадлежащего использования технологий в соответствии с заявлением банка о риск-аппетите и толерантности.

59. Управление ИКТ-риском включает:

a) выявление и оценку ИКТ-риска;

b) меры снижения ИКТ-риска, соответствующие оценённому уровню риска, например кибербезопасность, программы реагирования и восстановления, процессы управления изменениями ИКТ, процессы управления ИКТ-инцидентами, включая своевременную передачу релевантной информации пользователям;

c) мониторинг этих мер снижения риска, включая регулярное тестирование.

60. Для обеспечения конфиденциальности, целостности и доступности данных и систем совет директоров должен регулярно осуществлять надзор за эффективностью управления ИКТ-риском банка, а высшее руководство - систематически оценивать проектирование, внедрение и эффективность такого управления. Это требует регулярного согласования бизнес-стратегии, стратегии управления рисками и ИКТ-стратегии с риск-аппетитом и толерантностью банка, требованиями конфиденциальности и другими применимыми законами. Банк должен постоянно мониторить ИКТ и регулярно отчитываться высшему руководству об ИКТ-рисках, контролях и событиях.

61. Управление ИКТ-риском вместе с дополняющими процессами банка должно:

a) регулярно проверяться на полноту относительно соответствующих отраслевых стандартов и лучших практик, а также развивающихся угроз, например киберугроз, и новых или меняющихся технологий;

b) регулярно тестироваться в рамках программы выявления разрывов относительно заявленных целей по толерантности к риску и совершенствования выявления ИКТ-риска, защиты, обнаружения и управления событиями;

c) использовать практически применимую аналитическую информацию для постоянного повышения ситуационной осведомлённости об уязвимостях ИКТ-систем, сетей и приложений и поддержки эффективных решений в управлении рисками или изменениями.

62. Банки должны развивать готовность ИКТ к стрессовым сценариям, вызванным нарушающими внешними событиями, например к необходимости быстро развернуть широкомасштабный удалённый доступ, оперативно разместить физические активы и/или значительно увеличить пропускную способность для удалённых подключений пользователей и защиты данных клиентов. Банки должны обеспечивать:

a) разработку надлежащих стратегий снижения потенциальных рисков, связанных с нарушением или компрометацией ИКТ-систем, сетей и приложений, и оценку того, находятся ли совокупные риски с учётом этих стратегий в пределах риск-аппетита и толерантности банка;

b) наличие чётко определённых процессов управления привилегированными пользователями и разработкой приложений;

c) регулярное обновление ИКТ, включая меры кибербезопасности, для поддержания надлежащего уровня защищённости.

[25] «Информационно-коммуникационные технологии» охватывают физическую и логическую архитектуру информационных технологий и коммуникационных систем, отдельные аппаратные и программные компоненты, данные и операционные среды.

Планирование непрерывности деятельности

Принцип 11. Банки должны иметь планы непрерывности деятельности, обеспечивающие способность продолжать работу и ограничивать убытки в случае серьёзного нарушения деятельности.[26] Планы непрерывности должны быть связаны с рамочной системой управления операционным риском.

63. Надлежащее и эффективное корпоративное управление политикой непрерывности деятельности банка[27] требует:

a) регулярного пересмотра и утверждения советом директоров;

b) активного участия высшего руководства и руководителей бизнес-подразделений во внедрении;

c) вовлечения первой и второй линий защиты в её разработку;

d) регулярной проверки третьей линией защиты.

64. Банки должны разрабатывать ориентированные на будущее планы непрерывности деятельности (BCP), содержащие сценарный анализ с соответствующей оценкой воздействия и процедурами восстановления:

a) политика непрерывности должна основываться на сценарном анализе потенциальных нарушений, который

выявляет и классифицирует критически важные бизнес-операции и ключевые внутренние или внешние зависимости. При этом банк должен охватывать все свои бизнес-подразделения, а также критически важных поставщиков и крупных третьих лиц, например центральные банки и клиринговые организации;

b) каждый сценарий должен подвергаться количественной и качественной оценке воздействия либо анализу влияния на бизнес (business impact analysis, BIA) в части финансовых, операционных, юридических и репутационных последствий;

c) для сценариев нарушения должны быть установлены пороги или лимиты, например максимально допустимая продолжительность простоя, при достижении которых активируется процедура непрерывности. Процедура должна охватывать возобновление деятельности, устанавливать целевое время восстановления (RTO) и целевую точку восстановления данных (RPO), а также правила коммуникации для информирования руководства, сотрудников, надзорных органов, клиентов, поставщиков и, где уместно, органов гражданской власти.

65. Банк должен периодически пересматривать планы и политики непрерывности, чтобы стратегии реагирования оставались согласованными с текущей деятельностью, рисками и угрозами. Программы обучения и повышения осведомлённости должны быть адаптированы к конкретным ролям, чтобы сотрудники могли эффективно выполнять планы действий. Процедуры непрерывности должны периодически тестироваться для подтверждения возможности достижения целей и сроков восстановления и возобновления. По возможности банк должен участвовать в совместном тестировании непрерывности с ключевыми поставщиками услуг. Результаты формального тестирования

и проверок должны докладываться высшему руководству и совету директоров.

[26] Документ Комитета High-level principles for business continuity, август 2006 г., подробнее рассматривает принципы непрерывности деятельности.

[27] Планирование непрерывности должно быть согласовано с планированием и тестированием непрерывности критически важных операций, предусмотренным Принципами операционной устойчивости, и проводиться параллельно с ним. BCBS, Principles for operational resilience, март 2021 г.

Роль раскрытия информации

Принцип 12. Публичное раскрытие информации банком должно позволять заинтересованным сторонам оценивать его подход к управлению операционным риском и подверженность операционному риску.

66. Публичное раскрытие релевантной информации об управлении операционным риском может повышать прозрачность и способствовать развитию лучших отраслевых практик посредством рыночной дисциплины. Объём и тип раскрываемой информации должны соответствовать размеру банка, его профилю риска, сложности операций и развивающейся отраслевой практике.

67. Банки должны раскрывать заинтересованным сторонам релевантную информацию о подверженности операционному риску, включая существенные события операционных убытков, не создавая при этом новый операционный риск самим раскрытием, например описанием ещё не устранённых уязвимостей контроля.[28,29] ORMF должна раскрываться в форме, позволяющей заинтересованным сторонам оценить, насколько эффективно банк выявляет, оценивает, мониторит, контролирует и снижает операционный риск.

68. Банк должен иметь формальную политику раскрытия информации, которая подлежит регулярной независимой проверке и утверждению высшим руководством и советом директоров. Политика должна описывать подход банка к определению того, какую информацию об операционном риске раскрывать, а также внутренние контроли процесса раскрытия. Кроме того, банк должен внедрить процесс оценки надлежащего характера своего раскрытия и соответствующей политики.

[28] Международно активные банки обязаны соблюдать требования компонента 3 Базель III к раскрытию информации об операционном риске.

[29] Рекомендация раскрывать существенные события операционных убытков не предусматривает раскрытие конфиденциальной и закрытой информации, включая сведения о юридических резервах.

Роль надзорных органов

69. Надзорные органы должны регулярно оценивать ORMF банков, анализируя их политики, процессы и системы, связанные с операционным риском. Они должны обеспечивать наличие надлежащих механизмов, позволяющих оставаться в курсе развития операционного риска в банках.

70. Надзорная оценка операционного риска должна охватывать все области, описанные в Принципах надлежащего управления операционным риском. Если банки входят в финансовую группу, надзорные органы должны убедиться, что действуют процессы надлежащего и интегрированного управления операционным риском по всей группе. При оценке ORMF банка может потребоваться сотрудничество и обмен информацией с другими надзорными органами в соответствии с установленными процедурами.[30] В отдельных обстоятельствах надзорные

органы могут привлекать к таким оценкам внешних аудиторов.[31]

71. Надзорные органы должны принимать меры, обеспечивающие устранение банками недостатков, выявленных в ходе надзорной проверки ORMF. Следует использовать инструменты, наиболее соответствующие конкретным обстоятельствам банка и его операционной среде. Для получения актуальной информации об операционном риске надзорный орган может установить механизмы прямой отчётности с банками и внешними аудиторами; например, внутренние управленческие отчёты банка по операционному риску могут регулярно предоставляться надзорному органу.

72. Надзорные органы должны поощрять постоянное внутреннее развитие банков, отслеживая, сопоставляя и оценивая их недавние улучшения и планы дальнейшего развития.

[30] См. документы Комитета High-level principles for the cross-border implementation of the New Accord, август 2003 г., и Principles for home-host supervisory cooperation and allocation mechanisms in the context of Advanced Measurement Approaches (AMA), ноябрь 2007 г.

[31] Подробнее см. документ Комитета The relationship between banking supervisors and bank’s external auditors, январь 2002 г.

Краткий словарь терминов

Термин	Перевод / смысл в этой версии
Operational risk	Операционный риск - риск убытков из-за недостаточных/сбойных процессов, людей, систем или внешних событий.
ORMF	Рамочная система управления операционным риском.
CORF	Независимая корпоративная функция управления операционным риском; обычно вторая линия защиты.
Risk appetite	Риск-аппетит - совокупный уровень и виды риска, которые банк готов принять ради стратегических целей.
Risk tolerance	Толерантность к риску - допустимое отклонение от установленного риск-аппетита.
Inherent / residual risk	Присущий риск - до учёта контролей; остаточный риск - после учёта контролей.
Operational resilience	Операционная устойчивость - способность продолжать критически важные операции в условиях нарушений.
ICT	ИКТ - информационно-коммуникационные технологии.
BCP / BIA	План непрерывности деятельности / анализ влияния на бизнес.
RTO / RPO	Целевое время восстановления / целевая точка восстановления данных.

Перевод подготовлен как удобная для чтения PDF-версия. Иллюстрации и словарь добавлены редакционно; нормативным источником остаётся англоязычная публикация BIS.