**УТВЕРЖДЕНО**

Приказом Генерального директора
АО МГКЛ «Мосгорломбард»
№ 24 от 27.01. 2020 года

# Регламент по управлению операционными рисками и выявлению мошенничества

2020 г.

**1. Общие положения.**

1.1. Настоящий Регламент устанавливает правила и порядок действий при управлении операционными рисками АО МГКЛ «Мосгорломбард» (далее – Общество). Регламент разработан на основе законодательных актов Российской Федерации, нормативных и иных актов Банка России, рекомендаций Банка России по управлению операционным риском, а также с учетом внутренних документов Общества и сложившейся отечественной и международной практики ломбардной деятельности.

1.2. Действие настоящего регламента распространяется на всех штатных сотрудников Общества, включая сотрудников региональных и обособленных подразделений.

1.3. Целью настоящего Регламента является обеспечение непрерывности работы Общества, а также снижение рисков, возникающих в результате неправильных действий персонала, мошенничества, сбоя в информационных системах. Для достижения указанной цели необходимо:

- Установление методов выявления и измерения операционных рисков;
- Установление стандартов и требований к управлению операционными рисками;
- Описание процессов взаимодействия структурных подразделений Общества в части проведения идентификации и оценки операционных рисков;
- Обеспечение постоянного и эффективного мониторинга операционных рисков на всех основных направлениях деятельности Общества.

1.4. Для управления операционными рисками необходимо решить следующие задачи:

- Обеспечить получение оперативных и объективных данных об объекте операционного риска;
- Произвести комплексную оценку операционного риска;
- Произвести оценку влияния операционного риска на другие типы рисков;
- Обеспечить мониторинг объектов операционного риска;
- Создать систему быстрого реагирования для принятия решения на начальной стадии реализации операционного риска.

1.5. Органы управления Общества (в частности, Совет директоров) получают информацию о состоянии операционного риска регулярно, а при необходимости – незамедлительно.

**2. Основные определения.**

2.1. **Операционный риск** – риск возникновения убытков в результате неправильно выстроенных бизнес-процессов, информационных систем, человеческого фактора либо внешних событий (не относящихся к рыночным рискам).
**Контроль операционного риска** - процесс оценки результатов управления операционным риском.
**Мониторинг операционного риска -** процесс систематического и непрерывного сбора и анализа информации об уровне операционного риска.
**Минимизация операционного риска** - комплекс мероприятий по поддержанию операционного риска на уровне, не угрожающем интересам кредиторов и акционеров, устойчивости Общества.
**Объекты риска** - процессы, системы, ресурсы, активы Общества, утрата, повреждение или нарушение работы которых под действием факторов риска могут привести к финансовым убыткам, упущенной финансовой выгоде или прекращению деятельности Общества.

**Операционное событие** - любое неблагоприятное событие, воздействующее на объекты риска под влиянием факторов риска, следствием которого являются финансовые убытки, упущенная финансовая выгода или прекращение деятельности Общества.
**Оценка операционного риска** - комплекс мероприятий, направленных на выявление и анализ внутренних и внешних факторов, оказывающих воздействие на деятельность Общества и способствующих возникновению операционного риска.
**Управление операционным риском** - комплекс мероприятий и процедур по выявлению (идентификации), оценке (измерению), мониторингу, контролю и (или) минимизации операционного риска.
**Факторы (источники) риска** - это причины возникновения случайных неблагоприятных событий, приводящих к финансовым убыткам, упущенной финансовой выгоде или прекращению деятельности Общества.

2.2. В зависимости от причин возникновения выделяются следующие риски:
**Риски действующих бизнес-процессов –** риски потерь, связанных с несовершенством применяемых бизнес-процессов (наличием в них дефектов, которые могут привести к ресурсным потерям – средств, времени), ошибками в процессах проведения операций, расчетов по ним и их учета, отсутствием или несовершенством внутренних процедур, слабой организацией и эффективностью процессных потоков и регламентов проведения операций и систем контроля, неадекватной реакцией на жалобы, а также потерь из-за прерывания критических бизнес-процессов:

- в сфере продаж и привлечения клиентов;
- в сфере взыскания задолженности и реализации залогов;
- в финансово-инвестиционной сфере;
- в исковой работе (как в качестве истца, так и в качестве ответчика);
- прочие (административно-хозяйственная деятельность и т.д.).

**Риски управления проектами по совершенствованию бизнес-процессов –** риски потерь при срывах и задержках проектов по причине плохого управления проектами или отсутствия поддержки в результате неверной расстановки приоритетов, ведущих к недостаточной скоординированности или нехватке ресурсов.
**Риски действий персонала – риски потерь, связанных с:**

- недостаточной компетенцией (квалификацией) сотрудников при выполнении бизнес-процессов или недостатком квалифицированных сотрудников;
- низким уровнем исполнительской дисциплины (нарушение установленных процедур и регламентов);
- возможными ошибками сотрудников при выполнении производственных операций;
- действиями сверх предоставленных полномочий;
- мошенничеством, при котором информация намеренно сфальсифицирована, одним или несколькими сотрудниками с целью вывести активы компании незаконным путем и другими противоправными действиями, в том числе:
  - кражей имущества, денежных средств или интеллектуальной собственности;
  - приемом поддельных /несанкционированно измененных документов;
  - завышением оценочной стоимости залога;
  - использования служебного положения в личных целях (взятки, «откаты»).

**Риск внешнего мошенничества –** риски потерь, связанных с обманом или несоблюдением закона клиентами и третьими лицами. К данным рискам относятся, в том числе:

- Риск получения ворованного предмета. В ломбард обращаются не только люди, относящиеся к среднему классу, но и лица, имеющие сомнительную репутацию. Из этого следует, что многие предметы, которые они приносят

под залог, могут быть ворованными. В тех случаях, когда прокуратура доказывает их криминальное происхождение, происходит их изъятие у ломбарда без последующей компенсации. Когда предмет имеет очень высокую цену, ломбард может от этого пострадать.

- Риск получения поддельного предмета. Мошенники научились делать искусные подделки практически всего: от небольших аксессуаров известных брендов до китайского фарфора, которые с трудом отличит от оригинала даже опытный эксперт.
- Высокий риск ограблений. Многим, особенно, в кризис необходимы средства. Многие люди обращаются в ломбард, сдавая ценные ювелирные украшения и прочее имущество. Мошенники пользуются моментом, стараясь произвести ограбление именно тогда, когда витрины и сейфы ломбарда и комиссионного магазина полны изделий. Случается также, что наводчиками выступают сами работники учреждения, которым захотелось легких денег и знающие как обойти систему безопасности.

**Риски информационных технологий, технологические риски –** риски потерь, обусловленных:

- несовершенством используемых технологий, т.е. соотношение цена/качество не соответствует рыночным стандартам;
- недостаточной емкостью систем, каналов связи, при которых пользователи могут не получить доступ к информации, либо получить его не вовремя;
- несоответствием возможностей систем проводимым операциям;
- грубостью методов обработки данных;
- неадекватностью используемой информации или ее потерей;
- недостаточной гибкостью, надежностью или устойчивостью к чрезвычайным ситуациям;
- возможностями персонала, не имеющего прав доступа, получить доступ к конфиденциальной информации.

**Риски чрезвычайных ситуаций –** риски потерь по причинам природного и техногенного характера, а также связанные с непосредственным физическим вмешательством в деятельность Общества и его контрагентов (стихийные бедствия, пожары, ограбления, терроризм, влияние криминальной среды).

**Регулятивные риски –** риски применения финансовых, административных санкций со стороны государственных и квазигосударственных органов (ФНС, Росфинмониторинг, Гострудинспекция, ФАС, Центральный Банк и тд.) в связи с несоответствием деятельности Общества требованиям регуляторов (часть юридических рисков).

**Юридические риски –** риски возникновения убытков вследствие допускаемых правовых ошибок при осуществлении деятельности, в том числе при неадекватном мониторинге изменений действующего законодательства, отсутствия осведомленности, например, отсутствии или некорректной экспертизе полномочий контрагента при совершении сделки, несоблюдения требований нормативных правовых актов и заключенных договоров, несовершенства правовой системы (противоречивость законодательства, а также отсутствие правовых норм по регулированию отдельных вопросов).

**Риски, связанные с внутренней обеспеченностью информацией –** риски потерь в связи с тем, что были приняты неверные решения или не были приняты необходимые решения из-за того, что внутренняя информация представлена некорректно, поздно или рано или вообще не отражает суть произошедших процессов.

**Риски, связанные с безопасностью персонала –** риски, угрожающие здоровью и безопасности сотрудников.

**Риски, связанные с безопасностью имущества или информации –** риски того, что «физическое окружение» угрожает имуществу или информации (цифровой или бумажной).

**Риски, связанные с недостатками инфраструктуры –** риски потерь, связанных с неадекватным обеспечением производственной деятельности всеми инфраструктурными ресурсами – производственными площадями, транспортом, бесперебойным обеспечением энергопитанием, теплом, водоснабжением, и т.п., а также со сбоями в производственной деятельности вследствие нарушения поставщиком обязательств по срокам /качеству предоставляемых услуг.

**Риски внешнего окружения** включают в себя:

a. Риски воздействия преступности
b. Риски воздействия социальной, политической, экономической среды
c. Конкуренцию
d. Рынок труда
e. Специфический региональный риск

**Риски внутренней среды** включают в себя:

a. Корпоративную культуру
b. Риск-менеджмент
c. Риски организационной структуры
d. Персонал

2.3. Убытки в результате реализации операционных рисков могут быть следующими:

- *Снижение стоимости активов* – прямое уменьшение стоимости активов Общества вследствие кражи, мошенничества, противоправной деятельности работников Общества или третьих лиц, а также рыночные и кредитные потери Компании, произошедшие в результате таких рисковых событий.
- *Досрочное списание (выбытие) материальных активов* – уничтожение или прямое уменьшение стоимости материальных ценностей и активов Общества вследствие событий случайного характера (в т.ч. халатности, неосторожности, стихийных бедствий).
- *Денежные выплаты в судебном порядке* – штрафы, неустойки и издержки Общества в результате проведения судебного урегулирования разногласий с клиентом / контрагентом или работником Общества.
- *Денежные выплаты на основании решений органов, уполномоченных в соответствии с законодательством РФ* – штрафы, пени или любые другие санкции в денежном выражении, наложенные на Общество органами надзора вследствие нарушения Обществом действующего законодательства.
- *Денежные выплаты во внесудебном порядке* – денежные выплаты и компенсации, осуществленные Обществом своим клиентам и контрагентам, а также работникам Общества в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине Общества.
- *Повторные затраты* – затраты на восстановление хозяйственной деятельности Общества и устранение последствий ошибок, аварий, стихийных бедствий и других аналогичных обстоятельств.

**3. Оценка операционных рисков.**

3.1. Оценка операционных рисков строится на основе анализа следующей информации:

- Ведения базы данных по операционным рискам.
- Мониторинга индикаторов риска, которые указывают на общий уровень операционных рисков. Примеры индикаторов: количество дополнительных

рабочих часов у персонала, степень укомплектованности штата, ежедневные объемы операций, уровень текучести кадров, время простоя систем.

- Матричного моделирования операционных рисков (три параметра – событие, причина, последствие).
- Экспертного анализа рисков Общества – анкетирование сотрудников Общества с целью получить оценку вероятности наступления риска и размера потенциального ущерба. Разработка политики управления операционными рисками должна строиться на основе анализа рисков в координатах вероятность реализации – размер ущерба.

**4. Методы управления операционными рисками.**

4.1. Основными методами управления операционными рисками Общества являются:

- Использование процессно-ориентированного метода управления рисками, который предполагает выявление наиболее значимых процессов в Обществе и призван обеспечивать их непрерывность и жизнеспособность. Основные принципы этого метода должны заключаться во внедрении многоуровневой системы принятия решений в зависимости от значимости вопроса, утверждении наиболее значимых операций высшими органами управления, а также документированном описании основных элементов бизнес-процессов.
- Разработка организационной структуры Общества.
- Описание бизнес-процессов, продуктов и услуг Общества.
- Соблюдение принципов разделения полномочий и подотчетности по проводимым операциям.
- Информирование работников Общества об изменениях в законодательной и нормативной базе РФ.
- Разработка внутренних документов Общества, регламентирующих совершение ломбардных операций, в соответствии с законодательной и нормативной базой РФ.
- Поддержание в актуальном состоянии внутренней нормативной базы Общества.
- Проверка на соответствие бизнес-процессов законодательству РФ, при условии оперативного мониторинга законодательных изменений.
- Стандартизация бизнес-процессов (прежде всего в ключевых сферах и имеющих массовый характер – прием имущества в залог и на хранение), их документирование и актуализация описаний при изменениях.
- Ведение специальной базы данных с фиксацией дефектов бизнес-процессов по трем параметрам (событие/дефект, причина, последствие), накоплением и обработкой соответствующей статистики.
- Систематические плановые и внеплановые ревизии финансово–хозяйственной деятельности подразделений Общества, а также ключевых бизнес-процессов (в т.ч. применение метода «тайный покупатель»).
- Сплошная проверка при приеме на работу и, при необходимости, периодическая проверка сотрудников, работающих на должностях с повышенным риском участия во внутрифирменном мошенничестве, на «полиграфе».
- Специальная система противодействия мошенничеству, включающая актуализируемые «черные списки» неблагонадежных клиентов, специальные регламенты действий экспертов при возникновении подозрений на мошенничество при оценке имущества.
- Страхование имущества Общества, снижение размера потенциального ущерба (противопожарная сигнализация, охрана, видеонаблюдение).

- Детальная система управленческого учета доходов и расходов Общества, позволяющая оперативно анализировать причины повышения и снижения рентабельности операций по подразделениям компании.
- Совокупность мер по эффективному функционированию автоматизированной информационной системы, в т.ч. разграничение прав доступа, защита от несанкционированного доступа во внутреннюю сеть Общества, единая централизованная система антивирусной защиты, регламентное резервное копирование, наличие резервных источников питания и каналов связи, наличие автоматической идентификации пользователя при осуществлении важных операций, периодическая смена паролей доступа, ограничение физического доступа к серверам Общества:
  - Обновление основного сервера и сетевого оборудования Общества не реже чем раз в 5 лет.
  - Организация оперативного восстановления информации на основе системы резервного копирования и архивирования информации.
  - Установка резервного сервера, расположенного в другом здании или в другом крыле здания.
  - Наличие резервных источников питания.
  - Наличие резервных каналов связи.
  - Резервное копирование информации на ежедневной основе.
  - Наличие плана действий на случай выхода из строя и/или сбоя сервера, потери основного питания, связи и т.д.
  - Синхронизация обновлений IT-процессов в головном офисе и филиалах Общества.
  - Организация текущего обучения и повышения квалификации работников.
  - Ограничение доступа к критической информации в Обществе в соответствии с полномочиями и обязанностями сотрудников, использующих систему.
  - Наличие автоматической идентификации пользователя при осуществлении важных операций в системе.
  - Смена паролей доступа не реже чем раз в полгода.
- Нейтральное отношение ко всем политическим партиям и организациям.
- Участие в профессиональных союзах и объединениях, способствующих защите интересов и развитию Общества.
- Выдвижение законодательных инициатив (через союзы и общественные организации), а также предложений в нормативные ведомственные Акты, Правила профессиональной деятельности и т.п., снижающих риски неблагоприятных последствий для деятельности Общества.
- Развитие собственной инфраструктуры и/или партнерских отношений с контрагентами, обеспечивающее высокий уровень сервиса клиентам.
- Постоянная работа по разработке и реализации конкурентных преимуществ при оптимальном соотношении «цена – качество» с активным воздействием на целевые сегменты рынка, мониторинг деятельности конкурентов (прежде всего изменения условий кредитования и дисконтов) и своевременная реакция на их действия.
- Активное взаимодействие с правоохранительными органами (прежде всего, в сфере противодействия мошенничеству) и судебными органами (прежде всего, относительно правоприменительной практики по специфике ломбардной деятельности).
- Социально активная позиция (благотворительность, участие в общественной жизни и т.п.) на территориях деятельности Общества.

- Привлечение широкого круга сотрудников к совместной с собственниками и топ-менеджерами разработке и актуализации Миссии, Видения, Ценностей, Правил корпоративного поведения.
- Неукоснительное соблюдение руководством Общества принятых обязательств перед персоналом.
- Регулярные встречи руководства Общества с сотрудниками для разъяснения выбранной стратегии, тактических целей и задач и выбранных методов их реализации.
- Обеспечение безопасных и комфортных условий труда, а также развитие инфраструктуры бизнеса для высокопроизводительной работы (информационное обслуживание, связь, транспорт и т.д.).
- Реализация регулярного процесса повышения квалификации сотрудников.
- Реализация принципа не «кто виноват», а «что виновато» при сбоях в бизнес-процессах и анализе возникающих дефектов – т.е. отсутствие наказаний «за ошибки» (в отличие от наказаний за «злоупотребления»).
- Периодическое анкетирование сотрудников по степени удовлетворенности работой и анализ динамики изменения оценок.
- Формирование 3-5 летней стратегии (в т.ч. стратегических целей) в отношении ключевых аспектов деятельности Общества (в финансово-экономической сфере, клиентской сфере, в области бизнес-процессов, в сфере персонала и корпоративных отношений) с участием топ-менеджмента Общества и руководителей основных производственных подразделений на основании нескольких сценариев развития рынка и с учетом наличия необходимых ресурсов (финансовых, материальных, кадровых), а также актуализация этой стратегии в случае существенных изменений во внешней среде.
- Формирование планов бизнес-единицам и системы мотивации персонала за достижение стратегических целей.
- Обеспечение действенного контроля и анализа выполнения стратегических целей и планов.

**5. Организация процесса управления операционными рисками в Обществе.**

5.1. В процессе управления операционным риском Общество руководствуется следующими принципами:

5.1.1. Ключевая роль Совета директоров в части формирования культуры управления рисками. Совет директоров и Генеральный директор формируют корпоративную культуру, которая основана на надежном управлении рисками, а также поддерживают и создают надлежащие стандарты и стимулы ответственного профессионального поведения. Четкое определение ожиданий и подотчетности обеспечивает понимание сотрудниками Общества своих ролей и ответственности, а также компетенции. Политика в области выплаты вознаграждений согласована с установленными Обществом допустимым уровнем риска, его долгосрочной стратегией, плановыми финансовыми показателями и общими стандартами безопасности и надежности, необходимостью обеспечивать надлежащий баланс принятых рисков и выплачиваемых вознаграждений. Советом директоров обеспечивается надлежащий уровень профессиональной подготовки служащих в области операционного риска.

5.1.2. Комплексность и системность управления операционным риском. Система управления операционным риском интегрирована в общую систему управления рисками Общества. Управление операционными рисками проводится на постоянной основе во всех

структурных подразделениях Общества (осведомленность руководителей структурных подразделений Общества об основных операционных рисках своих подразделений и понимание ими своей ответственности за управление этими рисками).

5.1.3. Утверждение и периодический анализ Советом директоров системы управления операционным риском и контроль обеспечения эффективного применения принципов и процессов на всех уровнях принятия решений. Совет директоров анализирует структуру управления операционным риском с целью обеспечения выявления и управления Обществом операционным риском, вызванным изменениями рыночной ситуации и другими внешними факторами, а также операционными рисками, связанными с новыми продуктами, видами деятельности, процессами или системами, включая изменения уровня и видов риска и приоритетов.

5.1.4. Установление и анализ (пересмотр) Советом директоров риск-аппетита, а также определение особенностей, природы и уровня операционного риска, который готово нести Общество. В процессе анализа (пересмотра) учитываются изменения внешних факторов, существенное увеличение объема операций, в том числе по отдельным видам деятельности, качество системы контроля, эффективность стратегий управления риском или снижения риска, объем понесенных убытков, а также частота, масштабы и характер нарушений установленных лимитов. Совет директоров контролирует соблюдение установленного уровня риск-аппетита и обеспечивает своевременное выявление и устранение нарушений.

5.1.5. Ответственность Генерального директора за последовательное внедрение и применение на всех уровнях организации принципов, процессов и систем управления операционным риском, присущим всем существенным продуктам, направлениям деятельности, процессам и системам Общества, в соответствии с риск-аппетитом. Генеральный директор определяет полномочия, обязанности и порядок отчетности для поддержания и сохранения надлежащей структуры подотчетности, а также для обеспечения наличия необходимых ресурсов для управления операционным риском в соответствии с риск-аппетитом.

5.1.6. Обеспечение Генеральным директором выявления и оценки операционного риска, присущего всем существенным продуктам, направлениям деятельности, процессам и системам, с целью четкого понимания природы рисков и стимулов, создающих предпосылки для возникновения рисков.

5.1.7. Обеспечение Генеральным директором наличия процесса одобрения всех новых продуктов, направлений деятельности, процедур и систем с целью учета подверженности операционному риску.

5.1.8. Организация Генеральным директором процесса регулярного мониторинга уровня и природы операционного риска и вероятности возникновения существенных убытков. На уровне Совета директоров и на уровне осуществления различных направлений деятельности применяются механизмы представления отчетности, позволяющие осуществлять упреждающее управление операционным риском.

5.1.9. Наличие надежных систем контроля применения принципов, процессов и систем, надлежащего внутреннего контроля, а также надлежащих стратегий снижения риска. Средства внутреннего контроля обеспечивают обоснованную уверенность в том, что Общество осуществляет эффективные операции, защищает свои активы, представляет

достоверную финансовую отчетность и соблюдает действующие законодательные и нормативные акты.

5.1.10. Наличие планов обеспечения непрерывности и восстановления деятельности для сохранения возможности непрерывной работы и ограничения убытков в случае возникновения неблагоприятных обстоятельств, способных отрицательно повлиять на деятельность Общества.

5.2. Оценкой и мониторингом операционных рисков Общества занимаются отделы – владельцы риска совместно с Подразделением по управлению рисками, а также при необходимости другие отделы - в частности, Юридический департамент.

5.3. Методика и процедура оценки операционных рисков утверждаются протоколом заседания Комитета по управлению рисками.

5.4. Внеплановая процедура идентификации и оценки операционных рисков Общества проводится в следующих случаях:

- При формировании предложений по изменению бизнес-процессов;
- При изменении организационной структуры подразделений и их функций;
- При появлении внешних по отношению к Обществу факторов, действие которых носит долго- и среднесрочный характер и влияет на деятельность подразделений (изменения в законодательстве, природные катаклизмы, техногенные факторы, социальные изменения и т.п.);
- При реализации событий операционного риска.

5.5. Доклад об итогах внеплановой процедуры идентификации и оценки операционных рисков Общества рассматривается на ближайшем Комитете по управлению рисками, который принимает решения по корректировке соответствующих методик и регламентов.

**6. Мониторинг и оценка эффективности управления операционными рисками.**

6.1. Контроль за соблюдением регламента по управлению операционными рисками в Компании осуществляет Департамент по реализации правил внутреннего контроля.

6.2. Мониторинг операционных рисков происходит на ежеквартальной основе.

6.3. Отчет об управлении операционными рисками Общества составляется на ежеквартальной основе Подразделением по управлению рисками и представляется на Комитете по управлению рисками.

6.4. За неисполнение (ненадлежащее исполнение) настоящего регламента работник несет ответственность в пределах, определенных законодательством РФ.

Прошито, пронумеровано
и скреплено печатью 10
(десять)страниц
**Генеральный директор**
**АО МГКЛ «Мосгорломбард»**