Выписка из решения заочного заседания Совета директоров акционерного общества «Казахстанский фонд устойчивости»

№ 17

г. Алматы 23 октября 2020 года

Повестка дня:

2. Об утверждении Политики управления рисками акционерного общества «Казахстанский фонд устойчивости».

По вопросу 2 повестки дня «Об утверждении Политики управления рисками акционерного общества «Казахстанский фонд устойчивости»

По итогам голосования Совет директоров решил:

1. Утвердить Политику управления рисками акционерного общества «Казахстанский фонд устойчивости» согласно приложению № 4 к настоящему решению.

2. Признать утратившими силу:

2.1. Политику управления рисками акционерного общества «Казахстанский фонд устойчивости», утвержденную решением заочного заседания Совета директоров от 5 декабря 2018 года №14;

2.2. Правила управления операционными рисками акционерного общества «Казахстанский фонд устойчивости», утвержденные решением заочного заседания Совета директоров от 23 декабря 2019 года №17;

2.3. Правила управления финансовыми рисками акционерного общества «Казахстанский фонд устойчивости», утвержденные решением заочного заседания Совета директоров от 27 декабря 2019 года №19.

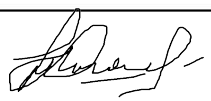
3. Настоящее решение вступает в силу с даты принятия.

Выписка верна.
Секретарь Совета директоров **Идилова А.А.**

Информационный лист к проекту
Политики управления рисками акционерного общества
«Казахстанский фонд устойчивости»

Разработчик	Управления рисков и анализа
Основание/ цель разработки	В целях выработки единого подхода к управлению рисками Общества, описания основных видов рисков и системы управления ими
Предмет регулирования	Регулирование порядка формирования единого понимания рисков Общества, обеспечение непрерывного согласованного процесса управления рисками, основанного на своевременной идентификации, измерении, оценке, проведении мероприятий по минимизации, контроле, мониторинге, а также последующем их предупреждении, для обеспечения достижения поставленных целей, минимизация финансовых потерь вследствие реализации финансовых, операционных и прочих рисков для обеспечения принципа непрерывности деятельности Общества, включая сохранность собственного капитала Общества, формирование риск-культуры у работников Общества.

Согласующие

Подразделение/должностное лицо	**ФИО**	**Виза о согласовании**
Юридическое управление	Югай Инна Владимировна	
Служба внутреннего аудита	Бейкутова Гульнур Мейрамбековна	
Кибер безопасность	И Константин Олегович	
Управление программ финансовой устойчивости	Тажибекова Карлыгаш Мусирбековна	

Приложение №4
к протоколу/решению заочного заседания
Совета директоров акционерного общества
«Казахстанский фонд устойчивости»
№17 от «23» октября 2020 года

Политика управления рисками акционерного общества «Казахстанский фонд устойчивости»

г. Алматы, 2020 год

Содержание документа:

Глава 1. Определение терминов, обозначения и сокращения

1. Сокращения, используемые в настоящей Политике:
   1) *УРиА* – Управление рисков и анализа;
   2) *ЮУ* – Юридическое управление;
   3) *ОС* – Основные средства;
   4) *НМА* – Нематериальные Активы;
   5) *ТМЗ* – Товарно-материальные запасы;
   6) *КСУР* – Корпоративная система управления рисками;
   7) *СВА* – Служба внутреннего аудита*;*
   8) *СД* – Совет директоров;
   9) *ВРД* – Внутренний регламентирующий документ;
2. Термины и определения, используемые в настоящей Политике:
   1) *Общество* – акционерное общество «Казахстанский фонд устойчивости»;
   2) *Уполномоченный (коллегиальный) орган (далее – УО)* – Правление и комитеты при Правлении (в зависимости от рассматриваемого вопроса).
   3) *Провизии (резервы)* – оценочный резерв под ожидаемые и имеющиеся кредитные убытки по займам и оценочное обязательство в отношении ожидаемых кредитных убытков по условным обязательствам;
   4) *Активы* – требования ко всем физическим и юридическим лицам, в том числе к банкам второго уровня;
   5) *Кредитный портфель* -портфель займов, выданных в рамках Программ повышения доступности ипотечных займов и выкупленных у банков второго уровня;
   6) *Инвестиционный портфель* - портфель активов, приобретенных в рамках реализации Программ по оздоровлению и развитию банковского сектора, кредитованию покупателей автотранспорта отечественного производства, рефинансированию ипотечных и ипотечных жилищных займов, кредитованию субъектов малого и среднего предпринимательства;
   7) *Пассивы* – совокупность обязательств и собственного капитала Общества;
   8) *Стресс-тестирование* – методы измерения потенциального влияния на финансовое положение Общества исключительных, но возможных событий, которые могут оказать влияние на деятельность Общества;
   9) *ГЭП* – методы измерения процентного риска Общества и риска потери ликвидности на основе сравнения объема активов и обязательств Компании, подверженных изменениям ставок вознаграждения или подлежащих погашению в течение определенных сроков;
   10) *Конфликт интересов* – ситуация, при которой возникает противоречие между личной заинтересованностью должностных лиц Общества и (или) его работников и надлежащим исполнением ими своих должностных полномочий или имущественными и иными интересами Общества и (или) его работников и (или) контрагентов, которое может повлечь за собой неблагоприятные последствия для Общества и (или) его контрагентов;
   11) *Корпоративная система управления рисками* (далее – КСУР) – набор взаимосвязанных компонентов, объединенных в единый процесс, в рамках которого СД, УО, подразделения и работники, каждый на своем уровне, участвуют в выявлении потенциальных негативных событий и реализованных инцидентов, которые могут повлиять на деятельность Общества, а также в управлении этими событиями, их минимизации в рамках приемлемого для акционера уровня риска.
   12) *Лимит* – инструмент управления определенными видами риска, который представляет собой количественное ограничение, накладываемое на определенные показатели;
   13) *Риск-аппетит* – способность и желание Общества принимать на себя риски определенного размера для достижения своих целей;
   14) *Риск концентрации* – риск возникновения потерь вследствие сосредоточения значительного размера риска (относительно размера собственного капитала, актива Общества или иного финансового показателя) на определенном контрагенте, секторе экономики, стране и прочих объектах;

15) *Риск-культура* - ценности, убеждения, понимание и знания в сфере управления рисками, разделяемые и применяемые работниками Общества на всех уровнях;

16) *Информационный актив* - совокупность информации и объекта информационно-коммуникационной инфраструктуры Общества, используемого для ее хранения и (или) обработки;

17) *Инциденты информационной безопасности* - отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов Компании;

18) *Информационная безопасность* - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Общества от внешних и внутренних угроз.

Глава 2. Общие положения

3. Настоящая Политика управления рисками акционерного общества «Казахстанский фонд устойчивости» (далее - Политика) разработана с целью выработки единого подхода к управлению рисками Общества, описания основных видов рисков и системы управления ими.

4. Политика разработана в соответствии с законодательством Республики Казахстан, Уставом и ВРД Общества.

Действие Политики распространяется на все виды деятельности Общества. Политика является обязательной для ознакомления, изучения и применения всеми подразделениями и работниками Общества.

5. Политика является документом верхнего уровня в КСУР, которая определяет:

1) основы построения КСУР;
2) цели и задачи КСУР;
3) организационную структуру КСУР Общества;
4) классификацию рисков Общества;
5) общие подходы к управлению рисками Общества.

6. Описание методов и процедур процесса управления рисками, включая порядок предоставления, сроки, формы и виды отчетности по управлению рисками, задачи, функции и ответственность участников процесса управления отдельными видами рисков, мероприятия по управлению рисками и другие составляющие процесса управления рисками, не указанные в Политике, регламентируются иными ВРД Общества.

7. Управление рисками в Обществе является постоянным, непрерывным процессом и осуществляется на всех уровнях с вовлечением УО, структурных подразделений и работников Общества.

8. Общество придерживается консервативного подхода к оценке риска, который подразумевает, что при наличии данных для оценки рисков из различных источников в расчет принимается наихудшая объективно обоснованная оценка, рейтинг, и/или прогноз.

9. Основными целями Политики являются:

1) построение эффективной КСУР в Обществе, а также постоянное совершенствование деятельности на основе единого стандартизированного подхода к методам и процедурам управления рисками;

2) обеспечение достижения стратегических целей Общества в рамках одобренного Риск-аппетита;

3) обеспечение финансовой устойчивости Общества в процессе ее развития;
4) обеспечение устойчивого развития КСУР Общества;
5) обеспечение защиты интересов акционера и партнеров Общества.

10. Основными задачами Политики являются:

1) формирование единого понимания рисков Общества участниками КСУР;
2) обеспечение стратегического планирования с учетом уровня принимаемого риска;
3) обеспечение непрерывного согласованного процесса управления рисками, основанного на своевременной идентификации, измерении, оценке, проведении мероприятий по

минимизации, контроле, мониторинге, а также последующем их предупреждении, для обеспечения достижения поставленных целей;

4) обеспечение эффективности бизнес-процессов, достоверности внутренней и внешней отчетности и содействие соблюдению требований законодательства;

5) создание полноценной базы для процесса принятия решений и планирования;

6) повышение эффективности управления активами Общества;

7) минимизация финансовых потерь вследствие реализации финансовых, операционных и прочих рисков для обеспечения принципа непрерывности деятельности Общества, включая сохранность собственного капитала Общества;

8) формирование риск-культуры у работников Общества.

11. В целях совершенствования процессов управления рисками в Обществе определяется долгосрочная стратегия развития КСУР, которая должна являться частью общей стратегии Общества.

12. На основе Плана развития/стратегии Общества разрабатываются планы работ УРиА, ответственного за управление рисками, в которых определены мероприятия на предстоящий период, сроки осуществления, а также ответственные работники УРиА.

13. Отчеты по рискам выносятся на рассмотрение СД не реже одного раза в квартал. Отчетность по событиям и инцидентам, также по принятым мерам непрерывности деятельности предоставляется раз в год для ознакомления членам Совета директоров в рамках общей управленческой отчетности по рискам Общества.

Глава 3. Корпоративная система управления рисками

14. При построении КСУР Общество предусматривает 3 линии защиты:

1) 1-я линия - все работники и подразделениями Общества в ответственность которых входит своевременное выявление и доведение до второй линии защиты информации о нарушениях (недостатках, событиях, сделках), которые могут привести к возникновению и реализации рисков Общества. Руководители структурных подразделений несут ответственность за организацию и осуществление управления рисками в подразделении в рамках компетенций, в том числе за осуществление мероприятий по устранению выявленных нарушений и недостатков;

2) 2-я линия – УРиА ответственно за оценку, мониторинг, минимизацию рисков как свершившихся, так и потенциальных в рамках функциональной ответственности. ЮУ несет ответственность за управление правовыми рисками Общества;

3) 3-я линия - СВА, оценивающий эффективность системы управления рисками и внутреннего контроля.

15. Механизм организации и внедрения КСУР в Обществе подразумевает:

1) разработку структуры системы управления рисками;

2) определение среды функционирования системы управления рисками, развитие необходимой инфраструктуры и культуры;

3) внедрение и интеграцию КСУР в общую систему управления Обществом;

4) разработку методов и инструментов управления рисками;

5) совершенствование КСУР на постоянной основе с учетом стратегических целей Общества.

16. Процесс управления рисками в Обществе состоит из десяти взаимосвязанных компонентов:

1) внутренняя и внешняя среда;
2) постановка целей;
3) идентификация рисков;
4) измерение и оценка рисков;
5) реагирование на риск;
6) проведение мероприятий по минимизации рисков;
7) контрольные действия;
8) информация и коммуникация;
9) мониторинг;

10) последующее предупреждение рисков.

17. Организационная структура КСУР. Участниками КСУР являются:

1) Совет директоров, Комитеты при СД;
2) Правление, коллегиальные органы при Правлении;
3) СВА;
4) УРиА, ЮУ (в части правовых рисков Общества);
5) Структурные подразделения и работники Общества.

18. Структура управления рисками в Обществе обеспечивает адекватный поток информации – по вертикали и по горизонтали:

1) информация, поступающая снизу-вверх, обеспечивает Совет директоров и Правление Общества сведениями относительно:

− текущей деятельности;

− принятых в ходе деятельности рисках, их оценке, проведении мероприятий по минимизации, контроле, мониторинге, методах реагирования, предупреждения и управления ими;

2) информация, направляемая сверху вниз, обеспечивает:

− доведение целей, стратегий и поставленных задач путем утверждения ВРД, издания приказов, поручений и прочих актов Общества;

3) передача информации по горизонтали подразумевает взаимодействие структурных подразделений/работников внутри Общества.

19. Первый уровень управления в КСУР представлен СД Общества. СД играет ключевую роль в создании и осуществлении контроля за КСУР. Комитет по рассмотрению вопросов стратегического планирования, кадров и вознаграждений, социальных вопросов при СД рассматривает вопросы и готовит СД рекомендации по вопросам управления рисками.

20. СД Общества осуществляет следующие функции в области управления рисками:

1) постановка краткосрочных и долгосрочных целей Общества;
2) утверждение политики управления рисками Общества;
3) рассмотрение отчетов по управлению рисками, в том числе карты рисков;
4) прочие функции согласно Кодексу корпоративного управления, Положению о СД Общества и другим ВРД.

21. Комитет/ы при СД выполняет следующие функции (не ограничиваясь):

1) рассматривает и предоставляет рекомендации СД по формированию плана работ по совершенствованию КСУР Общества;
2) согласовывает расчет приемлемого уровня Риск-аппетита для рекомендации СД;
3) предоставляет рекомендации СД по оптимизации бизнес-процессов Общества по вопросам управления рисками.

22. Второй уровень управления в КСУР представлен Правлением Общества. Правление Общества обеспечивает условия для эффективной реализации системы управления рисками, организует процесс управления рисками в Обществе, определяет подразделения, ответственные за управление рисками.

23. Правление ответственно за формирование в Обществе риск-культуры, которая является необходимым элементом для построения эффективной КСУР.

24. Правление в рамках КСУР вправе образовывать коллегиальные рабочие органы.

25. Правление в рамках КСУР утверждает ВРД Общества.

26. Правление обеспечивает целостность и функциональность КСУР путем осуществления следующих функций:

1) реализация Политики;
2) организация эффективной системы управления рисками, позволяющей идентифицировать и оценить потенциальные риски;
3) обеспечение соблюдения положений Политики работниками и подразделениями Общества;
4) рассмотрение отчетов по управлению рисками и принятие соответствующих мер в рамках своей компетенции;
5) утверждение мероприятий по реагированию и методик по управлению рисками в Обществе;

6) обеспечение совершенствования внутренних процедур и регламентов в области управления рисками.

27. В целях идентификации, независимой оценки и анализа основных рисков, связанных с проводимыми Обществом операциями, а также выработки методов управления рисками в Обществе функционирует подразделение – УРиА.

28. Полномочия и функциональные обязанности УРиА:

1) идентификация, измерение, оценка, проведение мероприятий по минимизации, контроль, мониторинг, последующее предупреждение рисков на постоянной основе;

2) разработка и актуализация ВРД по вопросам управления рисками;

3) обеспечение утверждения и реализация утвержденных мероприятий по реагированию на риски;

4) содействие процессу обмена информацией и коммуникацией между подразделениями Общества в процессе управления рисками;

5) прочие функции в рамках утвержденной компетенции.

29. С целью реализации поставленных целей и задач, работникам УРиА необходимо эффективно взаимодействовать с другими подразделениями Общества, в том числе с представителями внутреннего и внешнего аудита.

30. СВА Общества в процессе управления рисками осуществляет следующие основные функции:

1) аудит процедур управления рисками и методологии по оценке рисков, а также выработка предложений по повышению эффективности процедур управления рисками;

2) предоставление отчета по оценке эффективности КСУР для Совета директоров Общества, в том числе отчета о независимой оценке эффективности системы управления рисками;

3) проведение оценки состояния КСУР Общества;

4) иные функции в соответствии с утвержденными ВРД.

31. Структурные подразделения и работники Общества в процессе управления рисками осуществляют следующие функции:

1) своевременно выявляют и информируют УРиА о рисках в сфере своих функциональных обязанностей, в том числе предоставляют предложения по управлению рисками для включения их в план мероприятий;

2) несут персональную ответственность за обеспечение информационной безопасности.

32. Система внутреннего контроля (далее - СВК) - процесс, встроенный в повседневную деятельность, осуществляемую Советом директоров, коллегиальными органами, структурными подразделениями и всеми работниками Общества при исполнении своих обязанностей.

33. Основные компоненты СВК:

1)Контрольная среда – это комплекс процессов, обеспечивающих базу для осуществления внутренних контролей по всему Обществу;

2)Оценка рисков – это динамичный, непрерывный процесс выявления, идентификации и оценки рисков, препятствующих достижению целей Общества;

3)Контрольные действия – это комплекс мероприятий, встроенные в процессы, направленные на снижение рисков до допустимого уровня, обеспечивающего достижение целей Общества;

4)Информация и коммуникации – это непрерывный процесс сбора, обмена, предоставления необходимой информации для достижения целей Общества;

5)Мониторинг – это непрерывная, встроенная в процессы или отдельная оценка наличия или функционирования компонентов СВК.

34. Эффективный внутренний контроль обеспечивается путем формирования надлежащей контрольной среды, СВК является эффективной, когда все пять компонентов присутствуют и функционируют.

35. Несмотря на наличие основных компонентов эффективности СВК, Общество признает, что существует ряд ограничений СВК, таких как, ошибочное профессиональное суждение, ошибочное принятие решения, внешние негативные факторы, не подконтрольные Обществу, установление изначально недостижимых целей, человеческий фактор и т.д.

36. Эффективное функционирования СВК обеспечивается участниками всех трех линий защиты согласно п.14 настоящей Политики.

37. В первой линии защиты руководитель каждого подразделения осуществляет функции внутреннего контроля в подотчетном структурном подразделении.

38. Вторая линия защиты обеспечивает функционирование второго компонента СВК, УРиА разрабатывает единую методологию оценки всех видов рисков, осуществляет их оценку, ЮУ осуществляет оценку юридических (правовых) рисков.

39. Третья линия защиты, СВА осуществляет оценку эффективности системы управления рисками и внутреннего контроля по всем аспектам деятельности Общества.

40. Мониторинг СВК осуществляется работниками и руководителями структурных подразделений на постоянной основе, а также СВА посредством проверок.

41. Недостатки внутреннего контроля, выявленные на всех уровнях линий защиты, должны своевременно доводиться до руководителей структурных подразделений и оперативно устраняться.

Глава 4. Система управления рисками

42. Система управления рисками включает определение, идентификацию, измерение и оценку, проведение мероприятий по минимизации рисков, контроль, мониторинг, а также последующее предупреждение рисков, которые осуществляются Обществом на постоянной основе.

43. Риск аппетит нацелен на интегрирование факторов риска в процесс управления Обществом, отражает допустимые уровни риска. Допустимый уровень риска должен быть отражен в структуре риск аппетита, которая включает, но не ограничивается такими компонентами как достаточность капитала, уровень просроченных займов, ликвидность и другие компоненты, характерные деятельности Общества.

44. Определение и идентификация рисков - признание и понимание имеющихся и возможных рисков, а также характер их влияния на деятельность Общества.

45. Измерение и оценка рисков - использование системы и инструментов, позволяющих объективно определить размер и степень влияния рисков на деятельность Общества.

46. Проведение мероприятий по минимизации - создание резервов, установление Лимитов на различные операции, проводимые Обществом, отслеживание признаков наступления рисковых событий, формирование плана мероприятий по минимизации реализованных рисков;

47. Контроль за рисками - установление максимально допустимых ограничений на риски в отношении отдельных операций, их групп и совокупности, исходя из уровня собственного капитала и других показателей Общества.

48. Мониторинг рисков - осуществление оценки уровня подверженности Общества основным рискам, в том числе контроля за соблюдением максимально допустимых Лимитов рисков.

49. Предупреждение рисков - стратегическое планирование развития Общества, прогнозирование развития внешней среды, повышение квалификации работников Общества.

50. Классификация рисков, связанных с деятельностью Общества (не ограничиваясь), включает следующие виды рисков:

1) Кредитный риск;
2) Процентный риск;
3) Риск ликвидности;
4) Операционный риск;
5) Риск информационных технологий;
6) Риск информационной безопасности;
7) Риски непрерывности деятельности.

Глава 5. Управление кредитным риском

51. Кредитный риск представляет собой максимально ожидаемый убыток, который может иметь место с определенной вероятностью в течение некоторого периода времени в результате уменьшения стоимости актива, в том числе с учетом оценки денежных потоков от реализации обеспечения по кредиту.

52. Принципы управления кредитным риском:

Принцип 1: Правление Общества разрабатывает и периодически пересматривает План развития Общества и основные процедуры по управлению рисками, определяющие максимальный размер риска, принимаемого Обществом, и соответствующий ему уровень ожидаемой Обществом прибыли.

Принцип 2: разрабатываются процедуры по определению, измерению, контролю и мониторингу кредитного риска на уровне, как отдельных кредитов, так и всех подверженных кредитному риску активов;

Принцип 3: Общество реализует систему мониторинга состояния как отдельных кредитов, включая оценку адекватности созданных резервов, так и качества всех активов в целом;

Принцип 4: Общество принимает во внимание будущие изменения экономической ситуации при оценке отдельных кредитов и портфеля в целом, а также моделирует «поведение» портфеля в экстремальных ситуациях.

53. Определение риска производится путем проведения анализа следующей информации:

1) Прогноз движения денежных потоков;
2) Обеспечение кредитов;
3) Другие параметры доступные для анализа.

54. Мониторинг и контроль риска:

1) Важным элементом управления кредитным риском является система установления кредитных Лимитов и коэффициентных норм.

2) Важным элементом контроля и мониторинга кредитного риска является кредитное администрирование, включающее обновление текущей информации по заемщикам Общества, переписку с Банками партнерами и другие документы, отражающие актуальные данные.

3) Общество осуществляет постоянный мониторинг кредитного портфеля. Система кредитного мониторинга позволяет:

- адекватно оценивать текущее состояние портфеля Общества;
- контролировать соблюдение условий договоров в части своевременности и полноты погашения задолженности по займам;
- контролировать соответствие кредитов Общества программам повышения доступности ипотечных жилищных займов для населения;
- контролировать исполнение контрольных дат по кредитам;
- своевременно ранжировать кредиты Общества с учетом стадий изменения кредитного риска с момента первоначального признания.

4) Постоянным предметом мониторинга кредитного портфеля является его Риск концентрации в части:

- Банка - партнера, в том числе его филиальной сети;
- Географического региона;
- Сектора занятости заемщиков;
- Кредитной дисциплины заемщика и прочее.

5) С целью эффективного управления кредитными рисками отчетность в отношении подверженности Общества кредитному риску имеет постоянный характер и определяет текущую позицию в сравнении с установленными Лимитами и прогнозными данными. В выходные формы по мониторингу кредитного риска входит информация следующего характера:

- Анализ качества кредитного портфеля;
- Анализ по досрочно погашенным кредитам;
- Анализ концентрации кредитов как по Банкам партнерам, так и по филиалам и т. п.

6) Система внутреннего ранжирования является важным инструментом измерения кредитного риска и мониторинга качества кредитов, что позволяет более точно определять характеристики кредитного портфеля, концентрацию, проблемные кредиты и адекватность формирования Провизий. Данная система классифицирует кредиты по степени подверженности риску.

7) Общество производит стресс-тестирование кредитного риска. Сценарии стресс-тестирования разрабатываются с учетом специфики деятельности Общества, основываясь на оценке влияния локальных стрессовых факторов, в том числе связанных с особенностями деятельности Общества и структурой кредитного портфеля. Стресс-тестирование является ключевым инструментом для составления плана мероприятий в условиях кризиса. При стресс-тестировании Обществом используются, но не ограничиваются следующие факторы:

- ухудшение ситуации в экономике;
- случаи возникновения рыночного риска.

Глава 6. Управление процентным риском

55. Процентный риск — это риск возникновения расходов (убытков) вследствие неблагоприятного изменения ставок вознаграждения, включающий:

- риск возникновения расходов (убытков) из-за несоответствия сроков возврата и погашения размещенных активов и привлеченных обязательств Общества (при фиксированных ставках вознаграждения);

- риск возникновения расходов (убытков) вследствие применения Обществом разных видов ставок (плавающей либо фиксированной) по активам Общества, с одной стороны и обязательств, с другой;

- базисный риск, связанный с применением различных методов начисления и корректировки получаемого и уплачиваемого вознаграждения по ряду инструментов, которые при прочих условиях имеют сходные ценовые характеристики.

56. Принципы управления процентным риском:

Принцип 1: Общество определяет ответственных лиц и /или УО, ответственные за управление процентным риском, а также обеспечивает разделение должностных обязанностей по ключевым моментам управления риска с целью избежания потенциальных Конфликтов интересов.

Принцип 2: Политика и процедуры по управлению процентным риском должны быть четко определены и соответствовать видам и сложности проводимых Обществом операций.

Принцип 3: В процессе создания новых продуктов и операций, Компания определяет уровень процентного риска, связанного с ними, и разрабатывает необходимые процедуры управления данным риском.

Принцип 4: Система измерения процентного риска должна охватывать все существенные источники данного риска и оценивать эффект изменения процентных ставок в соответствии с объемом операций, осуществляемых Обществом, и их сроками.

Принцип 5: Общество разрабатывает и устанавливает операционные Лимиты, ограничивающие воздействие процентного риска в рамках, соответствующих внутренней политике Общества.

Принцип 6: Общество имеет достаточную информационную систему для измерения, мониторинга, контроля и отчетности о подверженности процентному риску.

57. Определение и измерение риска. Определение риска производится путем проведения следующих мероприятий:

1) система измерения процентного риска позволит осуществлять измерения текущего уровня процентного риска Общества, а также определить возможное увеличение подверженности Общества данному риску. Система измерения призвана рассматривать подверженность Общества процентному риску, связанную с Активами, Пассивами;

2) использовать общепринятые финансовые концепции и технологии риск-менеджмента;

3) иметь задокументированные предположения и параметры.

58. Мониторинг и контроль риска. В целях мониторинга и контроля процентного риска УРиА составляет отчетность в отношении подверженности Общества процентному риску, который имеет постоянный характер и определяет текущую позицию в сравнении с установленными Лимитами и прогнозными данными. В выходные формы по мониторингу процентного риска входит информация следующего характера:

1) Анализ текущего уровня процентных ставок, в разрезе кредитного портфеля Общества;

2) Анализ разрыва (Гэп - анализ) процентных ставок;

3) Анализ соблюдения установленных внутренних ограничений по процентным ставкам.

Глава 7. Риск ликвидности

59. Правление отслеживает ситуацию с риском управления структурой Активов и Пассивов, с полной детализацией, позволяющей понять и оценить степень подверженности Общества данному риску. Руководство также оценивает способность Общества принимать оперативные меры по выходу из кризиса при управлении Активами и Пассивами, а также фондировать часть или все операции в определенные сроки и при определенных затратах.

60. Принципы:

Принцип 1: Общество согласовано осуществляет управление Активами и Пассивами.

Принцип 2: Общество имеет подразделения, обеспечивающие эффективное управление Активами и Пассивами, контролирующие исполнение соответствующих политик и процедур с целью мониторинга и ограничения риска неправильного управления Активами и Пассивами.

Принцип 3: Общество имеет достаточную информационную систему, позволяющую проводить оценку, мониторинг, контроль и формировать управленческую отчетность по риску управления структурой Активами и Пассивами. Руководство Общества обеспечивается отчетами о финансовых рисках, в котором отражается состояние риска управления структурой Активами и Пассивами Общества на постоянной основе.

Принцип 4: Общество разрабатывает процесс оперативной оценки и мониторинга необходимых объемов фондирования.

Принцип 5: Общество постоянно пересматривает предположения, использованные при управлении структурой Активов и Пассивов с целью определения их состоятельности.

Принцип 6: Общество периодически пересматривает свою стратегию установления и развития отношений с кредиторами с целью диверсификации обязательств и обеспечения возможности продажи активов в случае необходимости.

Принцип 7: Общество разрабатывает и утверждает долгосрочный План развития, раскрывающий структуру Активов и Пассивов.

Принцип 8: Для оценки адекватности процесса управления риском структуры Активов и Пассивов Общество формирует систему внутреннего контроля, включающую регулярный независимый анализ и оценку эффективности управления данным риском.

Принцип 9: Общество разрабатывает механизм адекватного публичного раскрытия информации о себе с целью формирования общественного мнения.

61. В рамках процесса управления Активами и Пассивами между подразделениями Общества распределены функции и ответственность, закрепленные в ВРД Общества. Важным элементом в процессе управления риском ликвидности в части несбалансированности Активов и Пассивов, является достаточная информационная система, обеспечивающая все ответственные подразделения необходимой информацией о состоянии структуры Активов и Пассивов Общества.

62. Определение и измерение риска. Процесс оперативной оценки и мониторинга является основой для эффективного управления риском нарушения структуры Активов и Пассивов. Основой данного процесса является учет всех планируемых оттоков и притоков денежных средств с целью определения состояния Активов и Пассивов, как на текущий момент, так и в определенный момент времени в будущем. Результаты данной оценки позволяют Обществу планировать будущую потребность в краткосрочном и долгосрочном фондировании.

63. Мониторинг и контроль риска

1) ГЭП - анализ Активов и Пассивов Общества;

2) Анализ структуры баланса - собственных средств (уставного капитала, фондов), активов (доходности активов производительных (кредитный портфель) и непроизводительных (ОС, НМА, ТМЗ и т.д.) активов) и обязательств (привлеченных, заемных);

3) Анализ доходов, расходов, прибыли и рентабельности;

4) Анализ доходов, расходов и прибыли на 1 работника (1 раз в год);

5) Стресс-тестирование, разрабатывается с учетом специфики деятельности Общества, основываясь на оценке влияния локальных стрессовых факторов, в том числе связанных с особенностями деятельности Общества. При разработке сценариев стресс-тестирования Обществом используются, но не ограничиваются факторы, связанные с ухудшением ситуации на рынке недвижимости и в экономике в целом, а также недостаточный спрос на жилье либо его отсутствие.

64. Общество формирует четкое представление о наступлении кризиса позиции актива и пассива, определение которого устанавливается с учетом специфики финансового состояния Общества, стратегии его развития и особенностей, проводимых им операций путем установления предельных значений показателей, характеризующих позиции Актива и Пассива. В случае наступления кризиса, Обществом проводятся комплексные мероприятия по восстановлению позиции Актива и Пассива.

65. Для оценки адекватности процесса управления риском структуры Активов и Пассивов Общество формирует систему внутреннего контроля, включающую регулярный независимый анализ и оценку эффективности управления данным риском.

Глава 8. Управление операционными рисками

66. Операционный риск (далее – ОР) определяется как риск прямых или косвенных потерь, от неадекватных или ошибочных внутренних процессов, действий работников и подразделений Общества или от внешних событий.

67. ОР связан с нарушениями процессов осуществления видов деятельности Общества, отсутствием надлежащего внутреннего контроля, управления или неэффективности (методической ошибочности) какой-либо технологии осуществления вида деятельности.

68. Система управления операционными рисками (далее – СУОР) - совокупность основных процессов, включающих в себя различные функции и виды деятельности, позволяющие Обществу эффективно управлять ОР, присущему Обществу;

69. В процессе построения СУОР Общество руководствуется следующими принципами:

1) Принцип вовлеченности - вовлечение всех работников/подразделений Общества в процесс управления ОР;

2) Принцип своевременности - своевременное доведение до сведения работников, подразделений и руководства Общества о выявленных ОР;

3) Принцип разделения полномочий - четкое разделение полномочий работников и исключение ситуаций, когда сфера ответственности работника допускает конфликт интересов;

4) Принцип независимости - самостоятельное выявление подразделениями Общества ОР;

5) Принцип экономической целесообразности - стоимость мер контроля ОР должна быть меньше величины возможных потерь Общества от этого риска, при этом, принятие дополнительного ОР напрямую не должно повлечь за собой возникновения каких-либо дополнительных расходов. Определение приоритетных мер по контролю ОР должно быть реализовано экономически эффективно при оценке соотношения расходов на внедрение контрольных процедур с размером возможных потерь.

70. Классификация ОР Общества:

1) **Риск персонала** - риск потерь, связанный с ошибками и противоправными действиями работников Общества, их недостаточной квалификацией, излишней загруженностью, нерациональной организацией труда в Обществе;

2) **Риск процесса** - риск потерь, связанный с ошибками в процессах проведения операций и расчётов по ним, их учёта, отчётности, ценообразования;

3) **Риск систем** - риск потерь, обусловленных несовершенством используемых в Обществе

технологий - недостаточной ёмкостью систем, их неадекватностью по отношению к проводимым операциям, грубости методов обработки данных, или низкого качества, или неадекватности используемых данных;

4) **Риски внешней среды** - риски потерь, связанные с изменениями в среде, в которой функционирует Общество - изменения в законодательстве, политике, экономике, а также риски внешнего физического вмешательства в деятельность организации.

71. Процесс управления ОР подразделяется на следующие этапы:

1) Определение и идентификация реализованных ОР (инцидентов), а также ОР, присущих осуществляемым Обществом бизнес-процессам, путем проведения, включая, но не ограничиваясь, следующих мероприятий:

- анализ изменений во внешней среде в целом, которые могут оказать влияние на эффективность деятельности Общества;
- анализ организационной структуры Общества с целью выявления неэффективного распределения ответственности, структуры подотчетности и управления;
- анализ всех новых продуктов, видов деятельности, процессов и систем;
- анализ внутренних процедур, включая систему отчетности и обмена информацией;
- обнаружение реализованного ОР подразделениями Общества, информирование УРиА;
- регистрация факта реализации ОР;
- анализ вероятности реализации схожего ОР в других бизнес-процессах и/или подразделениях Общества;

2) Измерение и оценка реализованных ОР (инцидентов), а также ОР, присущих осуществляемым Обществом бизнес-процессам, осуществляется путем проведения, включая, но не ограничиваясь, следующих мероприятий:

- определение уровня ущерба, вероятного в случае реализации ОР, при не покрытии его соответствующими мерами минимизации;
- оценка влияния реализованного риска на бизнес-процессы Общества;
- анализ действующих бизнес-процессов, в том числе процедур управления ОР;
- оценка вероятности реализации схожего риска в других бизнес-процессах и/или подразделениях Общества.

Для оценки вероятности возникновения ОР используется система оценки качественных показателей, подготовленных на основе:

- ретроспективного анализа заключений по результатам внешних и внутренних проверок, информации по операционным событиям и убыткам;
- анализа эффективности мероприятий по снижению ОР.

Для оценки вероятности возникновения ОР используется система оценки количественных показателей, отражающих объем потерь за период, количество ошибок, сбоев, нарушений процедур и т.д. и периодичность их возникновения.

3) Минимизация реализованных ОР (инцидентов), а также ОР, присущих осуществляемым Обществом бизнес-процессам, осуществляется путем проведения, включая, но не ограничиваясь, следующих мероприятий:

- принятие срочных мер для минимизации ущерба в результате реализованного риска либо ликвидации причин реализованного риска. Указанные действия могут предприниматься до нанесения ущерба, вовремя и после реализации риска;
- автоматизация операций и элементов контроля в бизнес-процессах;
- разработка организационной структуры, внутренних правил и процедур совершения операций и других сделок таким образом, чтобы исключить/минимизировать возможность возникновения факторов ОР;
- отказа от наиболее рискованных, с точки зрения ОР, продуктов и услуги на основе детального их анализа;
- исправление выявленных недостатков в работе Общества;
- подготовка и реализация планов мероприятий по минимизации ОР.

4) Контроль реализованных ОР (инцидентов), а также ОР, присущих осуществляемым Обществом бизнес-процессам, осуществляется путем проведения выборочного контроля за

соблюдением установленных правил и процедур.

5) Мониторинг ОР осуществляется путем проведения, включая, но не ограничиваясь, следующие мероприятий:

- изучение ВРД Общества, анализ бизнес-процессов;
- практическое изучение осуществляемых подразделениями бизнес-процессов;
- изучение результатов аудиторских проверок соответствующих областей аудита;
- проведения рабочих встреч с владельцами и участниками бизнес-процесса;
- анализа реализованных рисков и их последствий, убытков Общества (при наличии).

6) Предупреждение ОР. С целью предупреждения (предотвращения) всех типов ОР и снижения возможных финансовых потерь, Общество принимает корректирующие меры, в том числе путем внесения изменений в действующие бизнес-процессы, процедуры, ВРД Общества.

Глава 9. Управление рисками информационных технологий

72. Риски, связанные с информационными системами Общества, включают в себя риски отказа или сбоя элементов инфраструктуры информационных систем, программного обеспечения, технологий и оборудования, используемых в деятельности Общества.

73. Объем и качество информационных систем Общества и связанных с ними процессов, включая процессов разработки (доработки), администрирования и эксплуатации информационных систем, должны соответствовать операционным потребностям и деятельности Общества, а также рискам, присущим данным процессам. Информационные системы Общества и связанные с ними процессы должны обеспечивать целостность, доступность, достоверность и конфиденциальность данных Общества, ее клиентов и контрагентов.

74. Для управления рисками, связанными с информационными системами Общество, применяет следующие меры, но, не ограничиваясь только ими:

1) регламентация порядка и процедур разработки (доработки) информационных систем Общества с учетом необходимости тестирования таких систем перед вводом в эксплуатацию;
2) разработка и реализация принципов и методов обеспечения информационной безопасности, включающих выявление, оценку и управление угрозами и уязвимостями информационной безопасности Общества;
3) осуществление анализа инцидентов, возникающих в работе информационных систем Общества, направленного на выявление причин возникновения инцидентов и своевременное определение необходимых мер по недопущению таких инцидентов в будущем.
4) внутренний аудит информационных систем Общества.

75. В целях мониторинга и контроля рисков Общества в части функционирования информационных технологий, а также для оценки потерь от наступления события риска информационных технологий Общество аккумулирует и анализирует следующую информацию о параметрах реализованного риска:

1) Дата и время события;
2) Описание события;
3) Причина события;
4) Общее время сбоя;
5) Место события.

76. В целях управления и оценки рисков информационных технологий Общество устанавливает следующие основные параметры: частота (вероятность) наступления риска и размер риска с дальнейшим отражением их в управленческой отчетности для Руководства.

Глава 10. Управление рисками информационной безопасности

77. Система управления Информационной безопасностью обеспечивает защиту Информационных активов Общества, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Общества.

78. Основными рисками Инцидентами (рисками) информационной безопасности являются:

1) сбои в информационных системах, создающие угрозу их надлежащему функционированию;

2) незаконное получение, копирование, распространение, модификация, уничтожение или блокирование электронных информационных ресурсов Общества;

3) несанкционированный доступ в информационную систему Общества;

4) заражение сервера Общества вредоносной программой или кодом;

5) иные инциденты информационной безопасности, несущие угрозу стабильности деятельности Общества.

79. Принципы:

Принцип 1: законность - соблюдение законодательства Республики Казахстан по защите информации и законных интересов всех участников информационного обмена;

Принцип 2: приоритетность – предварительное категорирование (ранжирование) информационных ресурсов Общества по степени важности в виде перечней сведений, подлежащих защите, и оценка реальных угроз информационной безопасности;

Принцип 3: комплексный подход - согласование мероприятий, проводимых в области информационной безопасности Общества, со всем комплексом мероприятий по физической и технической безопасности Общества, а также противодействие всем возможным угрозам информационной безопасности Общества;

Принцип 4: целесообразность - затраты на обеспечение защиты информации не должны превышать потери, которые может понести Общество при реализации угроз.

80. Основными объектами обеспечения информационной безопасности в Обществе являются:

1) Информационные ресурсы, содержащие сведения, отнесенные в соответствии с законодательством Республики Казахстан к конфиденциальной информации, банковской, коммерческой или иной охраняемой законом тайне (далее по тексту – защищаемая информация);

2) Средства и системы информатизации: средства вычислительной техники, информационно - вычислительные комплексы, сети, системы, на которых производится обработка, передача и хранение защищаемой информации;

3) Программные средства: операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение, автоматизированной системы Общества, с помощью которых производится обработка защищаемой информации;

81. Подлежащая защите информация Общества находится как бумажных носителях, так и в электронном виде.

82. Идентификация риска заключается в составлении перечня и описании элементов риска: объектов защиты, угроз, уязвимостей. При идентификации угроз и уязвимостей в качестве исходных данных Общество использует результаты аудитов (при наличии), данные об инцидентах информационной безопасности, экспертные оценки пользователей, специалистов по информационной безопасности, ИТ-специалистов и внешних консультантов.

83. Оценка и мониторинг. Информация, полученная на этапе идентификации рисков, используется в процессе анализа рисков для определения:

1) возможного ущерба, наносимого Обществу в результате нарушений безопасности Информационных активов;

2) вероятности наступления такого нарушения;

3) величины риска.

84. Контроль и минимизация достигается следующими процедурами:

- Резервное хранение данных критичных информационных систем, их файлов и настроек, которое обеспечивает восстановление работоспособной копии информационной системы;
- Персонализация доступа к информационным активам для работников Общества;
- Внутренний аудит состояния информационной безопасности.

85. Методы оценки, мониторинга и контроля регулируются во ВРД Общества по управлению рисками информационной безопасности.

Глава 11. Управление непрерывностью деятельности

86. Основная цель управления непрерывностью деятельности заключается в минимизации негативных операционных, финансовых, правовых, репутационных и других последствий, вытекающих из инцидентов.

87. При регламентации процессов обеспечения непрерывности деятельности Общества необходимо учитывать:

1) организационную деятельность, включая установление требований и полного цикла непрерывности деятельности от разработки, внедрения и до первоначальной проверки способности Общества к непрерывности деятельности;

2) поддержку способности к обеспечению непрерывности деятельности, которые включают в себя:

а) управление непрерывностью деятельности;

б) проведение регулярных учений по применению Планов мероприятий по обеспечению непрерывности деятельности (далее – План);

в) актуализацию Плана, особенно в случаях возникновения существенных изменений в производственных и технологических процессах, рыночных\внешних условиях.

88. Общество идентифицирует критичные виды деятельности. Идентификация критичных видов деятельности в рамках системы управления непрерывностью деятельности идентификация потенциальных угроз деятельности Общества, оценка возможных воздействии на бизнес-операции в случае осуществления угроз, а также создание основ для обеспечения способности Общества восстанавливать свою деятельность и эффективно реагировать на инциденты.

89. Руководители подразделений, являющиеся владельцами критичных процессов, несут ответственность за проведение анализа процессов, в рамках которого идентифицируются критичные функции, продукты Общества, приостановление которых может принести существенный ущерб, и беспрерывная реализация которых является наиболее важной для Общества, требуемые ресурсы для восстановления, определение сроков и уровней их восстановления и внесение соответствующих изменений в Планы.

90. После идентификации основных рисков и угроз деятельности Общества, выполненной в рамках анализа факторов влияния возникших непредвиденных обстоятельств на деятельность Общества, необходимо определить и внедрить меры по минимизации и предотвращению данных рисков, минимизировать последствия нарушений путем внедрения предотвращающих мер в ежедневную деятельность Общества.

91. Общество определяет ресурсы, необходимые для поддержания критичных видов деятельности, которые включают, но не ограничиваются следующим:

1) Персонал - Общество определяет необходимое для поддержания критичных видов деятельности количество работников, необходимые навыки и компетенции данных работников для работы в аварийном режиме;
2) Помещения - при определении помещений, как ресурса, необходимого для поддержания критичных видов деятельности Общества определяет:
   - основные и альтернативные площадки;
   - помещения, требующие повышенной защиты;
3) Технологии - При определении технологий, как ресурса, необходимого для поддержания критичных видов деятельности Общества определяет:
   - информационно-технологические услуги, поддерживающие критичные виды деятельности;
   - телекоммуникационные услуги, поддерживающие критичные виды деятельности;
   - прочие технологии, поддерживающие критичные виды деятельности, в том числе охрана периметра;
4) Информация - при определении информации, как ресурса, необходимого для поддержания критичных видов деятельности соответствующими подразделениями Общества определяется:
   - информация, необходимая для выполнения критичных видов деятельности, включая внутренние документы Общества;

- объем информации, требующей восстановления (целевая точка восстановления);
- методы хранения, защиты и восстановления этой информации.

5) Поставщики, внешние услуги и снабжение - при определении поставщиков, внешних услуг и снабжения, как ресурса, необходимого для поддержания критичных видов деятельности соответствующими подразделениями Общества определяются поставщики, внешние услуги и снабжение, от которых зависит выполнение критичных видов деятельности.
6) Финансовые ресурсы - при определении финансовых ресурсов, необходимых для поддержания критичных видов деятельности соответствующими подразделениями Общества определяется объем финансовых ресурсов, потенциально доступный для исполнения Плана в случае возникновения непредвиденных обстоятельств.

92. Анализ рисков непрерывности деятельности Общества позволяет оценить угрозы и уязвимость в критичных видах деятельности и используемых ими ресурсах. В качестве угроз, которые могут оказать негативное воздействие на деятельность и ресурсы, Общество рассматривает, но не ограничивается следующим:

1) недоступность работников;
2) недоступность технологий, в том числе информационных и коммуникационных технологий (компьютерные вирусы, отказ компьютерных аппаратных средств, потеря связи);
3) недоступность снабжения (воды, электричества);
4) отсутствие доступа к зданиям (помещениям);
5) недоступность ключевых поставщиков, контрагентов;
6) недоступность ключевой информации;
7) недоступность финансовых ресурсов.

93. Общество определяет меры управления рисками непредвиденных обстоятельств, которые охватывают (но, не ограничивает) следующие ключевые ресурсы:

1) персонал;
2) помещения;
3) технологии;
4) информацию;
5) поставщиков, контрагентов и каналы снабжения.

94. При выборе мер управления рисками непрерывности деятельности Общество учитывает результаты анализа влияния инцидентов на деятельность Общества и определяет, в том числе порядок взаимодействия с внешними поставщиками, участвующими в восстановительных работах, с внешними контрагентами, с уполномоченным органом и иными органами власти, а также со средствами массовой информации и другими заинтересованными сторонами.

95. При выборе мер управления рисками непрерывности деятельности Общество учитывает, но не ограничивается следующими факторами:

1) максимально приемлемый период простоя критичного вида деятельности;
2) затраты на реализацию Плана;
3) последствия бездействия;
4) реалистичность рисков и величину потерь от их реализации;
5) согласованность с установленными целями системы управления непрерывностью деятельности;
6) согласованность с политиками и процедурами по управлению рисками Общества.

96. Общество определяет меры по поддержанию работоспособности в информационно-технологических и коммуникационных услугах, необходимых для обеспечения непрерывности деятельности, которые включают, но не ограничиваются следующим:

1) предоставление информационно-технологических и коммуникационных услуг внутри Общества;
2) предоставление информационно-технологических и коммуникационных услуг из альтернативного помещения;
3) предоставление информационно-технологических и коммуникационных услуг сторонней организацией.

97. Общество обеспечивает целостность, доступность и конфиденциальность информации, необходимой для обеспечения непрерывности деятельности, в случае критичного события. Способ

хранения и восстановления информации согласовывается с результатами анализа влияния на деятельность и учитывает:

1) требования к объему восстанавливаемой информации, целевые точки и сроки восстановления информации;
2) защищенность хранения и передачи информации;
3) способы и надежность механизма восстановления;
4) частоту и объем резервируемой информации;

98. Общество определяет перечень используемых ресурсов (включая материальное снабжение, финансовые ресурсы) и мероприятия по обеспечению их наличия, в том числе от внешних поставщиков и контрагентов и иных заинтересованных лиц в случае критичного события, которые могут включать:

1) хранение дополнительных ресурсов, в том числе технологического и телекоммуникационного оборудования, в складских помещениях;
2) соглашения с поставщиком о срочной доставке (замене) ресурсов на складе;
3) наличие альтернативных поставщиков ресурсов.

99. Для проверки эффективности Планов, работниками Управления рисков и анализа совместно с владельцами критичных бизнес-процессов, раз в год проводится тестирование планов.

Глава 12. Заключительные положения

100. Вопросы, не урегулированные Политикой, решаются в соответствии с законодательством Республики Казахстан и ВРД;

101. Обществом могут быть разработаны и приняты дополнительные ВРД, направленные на адаптацию и применение положений настоящей Политики;

102. Актуализация Политики осуществляется УРиА.