

«УТВЕРЖДАЮ»

И.о. Заместителя председателя правления

АКБ «Банк развития бизнеса»

Вохидов О.

«25» 12. 2024 г.



АКБ «Банк развития бизнеса»

Техническая документация

Автоматизированная система управления операционными рисками (АСУОР)

«СОГЛАСОВАНО»

Главный директор по рискам

АКБ «Банк развития бизнеса»

Хакимов Д.

«25» 12. 2024г

«СОГЛАСОВАНО»

Директор департамента Риск менеджмента

АКБ «Банк развития бизнеса»

Каримов К.

«25» 12. 2024 г.

«СОГЛАСОВАНО»

Директор департамента ИТ

АКБ «Банк развития бизнеса»

Орифхужаев З.

«25» 12. 2024 г.

Ташкент - 2024

Оглавление

Оглавление	2
1. Общие положения.....	4
1.1 Сокращения и определения	4
1.2 Полное наименование Системы:	4
1.3 Предмет	5
1.4 Порядок оформления и предъявления Заказчику результатов работ	5
2. Цели и назначение Работ	5
2.1 Цели и задачи выполнения Работ	5
2.2 Основными задачами создания Системы является автоматизация процедур	5
3. Требования к системе	5
3.1 Общие требования	5
3.1.1 Преднастроенная маршрутизация.....	7
3.1.2 Преднастроенный перечень КПУРов	17
3.1.3 Преднастроенный перечень КИРов	20
3.1.4 Преднастроенный реестр операционных рисков.....	20
3.2 Требования к архитектуре решения.....	22
3.2.1 Требования к архитектуре Системы	22
3.2.2 Требование к взаимодействию с внешними источниками	24
3.2.3 Требования к составу и объему лицензии	24
3.2.4 Требования к функциональным возможностям.....	27
3.2.5 Требования к возможностям расширения функциональности	41
3.2.6 Требования к информационной безопасности Системы	42
3.2.7 Требования к журналированию и логированию.....	43
3.3 Требования к структуре Системы в целом.....	46
3.3.1 Требования к информационному обмену и информационной совместимости	46
3.3.2 Требования к взаимосвязи Системы со смежными системами, обеспечение совместимости..	46
4. Требования к выполняемым Работам	46
4.1 Общие принципы выполнения Работ	46
4.2 Общие технические требования к Работам.....	47
4.2.1 Требования к составу Работ.....	47
4.2.2 Требования к применению систем управления базами данных.....	48
4.2.3 Требования к эргономике и технической эстетике Системы	48
4.2.4 Требования к защите информации от несанкционированного доступа к Системе.....	49
4.2.5 Технические требования к защите информации	49

4.2.6	Требования по стандартизации и унификации	49
5.	Требования к составу и срокам выполнения работ.	49
6.	Порядок контроля и приемки Системы	52
7.	Требования к документированию	53
7.1	Требования к содержанию отчетных документов	53
7.1.1	Документ «Руководство пользователя»	53
7.1.2	Документ «Руководство администратора».	53
7.1.3	Руководство по установке и настройке решения	54
7.1.4	Руководство по обновлению системы	54
7.2	Требования к разработке внутренних нормативных документов (ВНД) по управлению операционным риском и операционной надежности.	54
7.2.1	Политика управления операционным риском:	54
7.2.2	Порядок взаимодействия при выявлении событий операционного риска:	54
7.2.3	Порядок определения потерь и возмещений:	54
7.2.4	Методика качественной оценки операционного риска:	54
7.2.5	Порядок мониторинга операционного риска:	55
7.2.6	Политика информационной безопасности по управлению рисками ИБ:	55
7.2.7	Политика информационных систем (управление рисками информационных систем):	55
7.2.8	Методика обеспечения качества данных в информационных системах:	55
7.2.9	Порядок обеспечения качества данных в информационных системах:	55
7.2.10	Политика обеспечения операционной надежности:	56
7.2.11	Порядок обеспечения операционной надежности:	56
8.	Техническое сопровождение Системы	57

1. Общие положения

1.1 Сокращения и определения

Сокращение	Определение
Заказчик	Банк Развития Бизнеса
Исполнитель	Правообладатель и производитель Системы, выполняющий работы по ее внедрению и передачи лицензий Заказчику
Система, АСУОР	Автоматизированная система управления операционным риском в кредитной организации
ГППО, «Из коробки»	Готовое прикладное программное обеспечение категории АСУОР, неисключительные права на которое передаются Исполнителем Заказчику для создания, внедрения и эксплуатации Системы. Программное обеспечения должно быть готово к полноценному использованию в базовом режиме после установки и минимальной настройки, которая предполагает добавление пользователей, назначение преднастроенных ролей и подразделений.
Договор	Договор на выполнение работ по внедрению «Автоматизированной системы управления операционным риском АКБ «Банк развития бизнеса»
Работы	Комплекс работ, предусматривающий внедрение Системы
Администратор безопасности	Специалист Заказчика, выполняющий функции по защите информации, обрабатываемой в Системе
Администратор системы	Специалист Заказчика, отвечающий за эксплуатацию Системы
ИБ	Информационная безопасность
ИТ	Информационные технологии
ИС	Информационная система
КПУР	Контрольный показатель уровня операционного риска
КИР	Ключевой индикатор риска
Пользователь Системы	Работник Заказчика
ОР	Операционный риск
Замечание	Любое событие, не являющееся частью нормального функционирования Системы, описанного в руководствах пользователей и технологической документации, которое может вызвать прерывание или изменение качества работы Системы
Запрос	Обращение Заказчика к Исполнителю в случае обнаружения Замечания или для получения консультации
ЮЛ	Юридические лица
ФЛ	Физические лица
ОПЭ	Опытно-промышленная эксплуатация
ПСИ	Приемо-сдаточные испытания
СУБД	Система управления базой данных
ТЗ	Настоящее техническое задание
АБС	Автоматизированная банковская система

1.2 Полное наименование Системы:

Автоматизированная система управления операционным риском (далее – Система, ПО, Продукт).

1.3 Предмет

Выполнение работ по созданию Автоматизированной системы управления операционным риском на базе готового прикладного программного обеспечения (далее – Работы).

1.4 Порядок оформления и предъявления Заказчику результатов работ

Результаты Работ передаются Заказчику в порядке, определенном Договором.

2. Цели и назначение Работ

2.1 Цели и задачи выполнения Работ

Основным назначением Системы является автоматизация процесса управления операционным риском в кредитных организациях в соответствии с методическими рекомендациями, приведенными в Базель III.

Основными целями создания Системы являются:

- Создание и обеспечение соблюдения требований по управлению операционным риском в БРБ.
- Повышение эффективности и прозрачности процедур управления операционным риском, повышение риск-культуры подразделений банка;
- Снижение операционных затрат на ведение базы событий операционных рисков, аналитику и формирование отчетности;
- Снижение уровня операционных рисков в виду более качественного управления ими - т.е. снижение величины потерь и количества риск-событий;
- Накопление качественной исторической базы СОР;
- Внедрение подходов, базирующихся на требованиях Базель III - превентивное их внедрение позволит быстро и безболезненно адаптироваться к новым более продвинутым требованиям регулятора в случае их внедрения;
- Оперативная аналитика по историческим данным для предоставления руководству, внешним аудиторам либо регулятору.

2.2 Основными задачами создания Системы является автоматизация процедур

- Ведение базы событий операционного риска (далее – СОР);
- Ведение реестра операционных рисков (Далее ОР);
- Проведение процедур качественной оценки ОР для идентификации и оценки СОР;
- Мониторинг уровня операционного риска по прямым и косвенным признакам;
- Повышение степени автоматизации процедуры выявления СОР;
- Повышение культуры управления операционным риском.

3. Требования к системе

3.1 Общие требования

ГППО, поставляемое Исполнителем, должно представлять с собой готовое решение:

- с предзаполненным набором справочников и классификаторов, с возможностью дальнейшей адаптации под требования Заказчика.
- с преднастроенной ролевой моделью «из коробки» достаточной для управления операционным риском в БРБ с вовлечением всех подразделений и пользователей банка, учитывая минимально необходимую степень вовлеченности в процедуры управления операционным риском.

Права использования ГППО предоставляется Заказчику после заключения договора на выполнение Работ в целях внедрения Системы с учетом требований технического задания; Работы должны проводиться с учетом специфики деятельности Заказчика, и в соответствии с методическими рекомендациями «Базель III».

Основные критерии:

- Программное обеспечение готово к установке и использованию в рамках преднастроенной базовой функциональности для управления операционным риском в банке с минимальным конфигурированием (добавление пользователей, организационной структуры, ввод реквизитов почтового сервера, ввод реквизитов AD) и возможностью вовлечением всех подразделений и пользователей банка, учитывая минимально необходимую степень вовлеченности в процедуры

управления операционным риском течение 60 рабочих дней после заключения договора. Базовый состав:

- с предзаполненным набором справочников и классификаторов для ведения базы событий операционного риска, реестра операционных рисков, инцидентов операционной надежности
- с преднастроенным процессом обработки событий операционного риска с вовлечением всех подразделений и сотрудников по усмотрению банка в соответствии с преднастроенно ролевой моделью
- с преднастроенной ролевой моделью «из коробки» для регистраторов событий, для руководителей и центров компетенций по бизнес-подразделениям, для риск-менеджеров, для аудиторов, для подразделений, выделенных для управления отдельными видами операционного риска
- с преднастроенным перечнем рекомендуемых мероприятий
- с преднастроенным перечнем операционных рисков для банка
- с преднастроенным процессом проведения процедуры самооценки с вовлечением бизнес-подразделений с возможностью выявления и регистрации новых рисков и проведением процедуры оценки эффективности ранее проведенных мероприятий
- с преднастроенным перечнем контрольных показателей уровня операционного риска по базе событий операционного риска
- Готовое программное обеспечение поставляется с технической документацией:
 - Инструкции пользователей (для каждой роли)
 - Инструкция администратора
 - Инструкция по установке и настройке решения
 - Описание формата взаимодействия с базовым сервисом ПО для записи из внешней системы любых данных, для которых предусмотрена структура данных в ПО
- На первом этапе, готовность установить и настроить базовую версию системы с ранее упомянутым набором в течение 60 рабочих дней после заключения договора
- Программное обеспечение поддерживает адаптацию функциональности под специфику Банка без использования программного кода и в дальнейшем позволяет расширять функциональность силами Банка
- На втором этапе внедрения, доработать базовый состав и установить следующие компоненты в течении 40 рабочих дней:
 - Поддержка многоязычности на уровне пользовательского интерфейса (узбекский и русский язык)
 - Преднастроенный перечень ключевых индикаторов риска для автоматического мониторинга
 - Преднастроенный процесс проведения процедуры сценарного анализа на базе результатов проведенной самооценки по операционному риску для выявления максимально возможных потерь в денежном эквиваленте
 - Преднастроенный процесс расчета размера операционного риска и капитала на покрытие операционного риска
- Вендор является правообладателем решения АСУОР и имеет права на его модификацию, доработку

Ведущий менеджер
Управления операционного рисков

Р.Фазилов

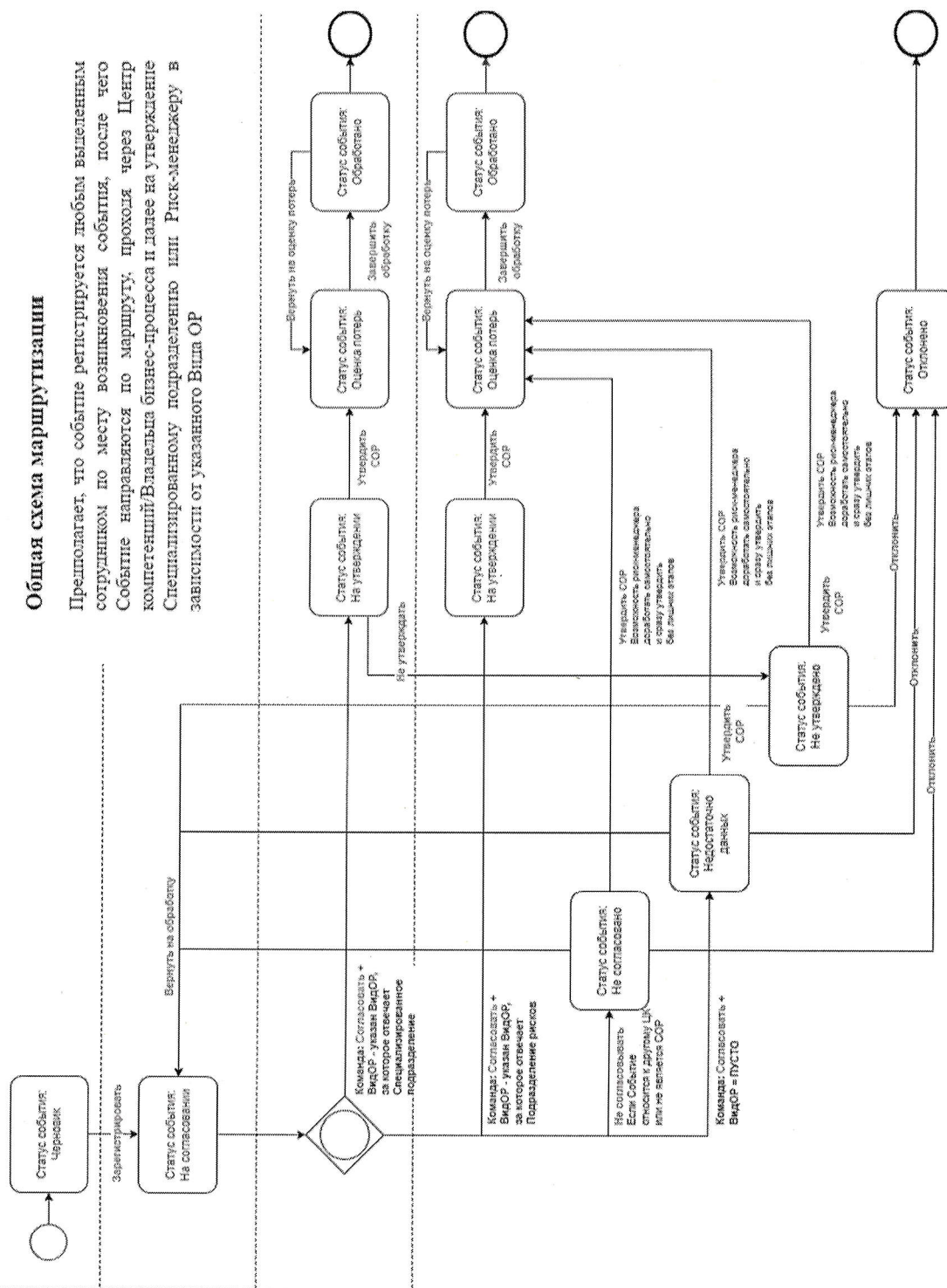
Платой сотрудник Банка подключенный к системе, в том числе Фиск-менеджер, Фиск-координатор ОП, Фиск-координатор ЦК.

Сотрудник структурного подразделения
Владимир Юзвист-процесс, упомянутый
на верификацию и согласование зарплатных
данных

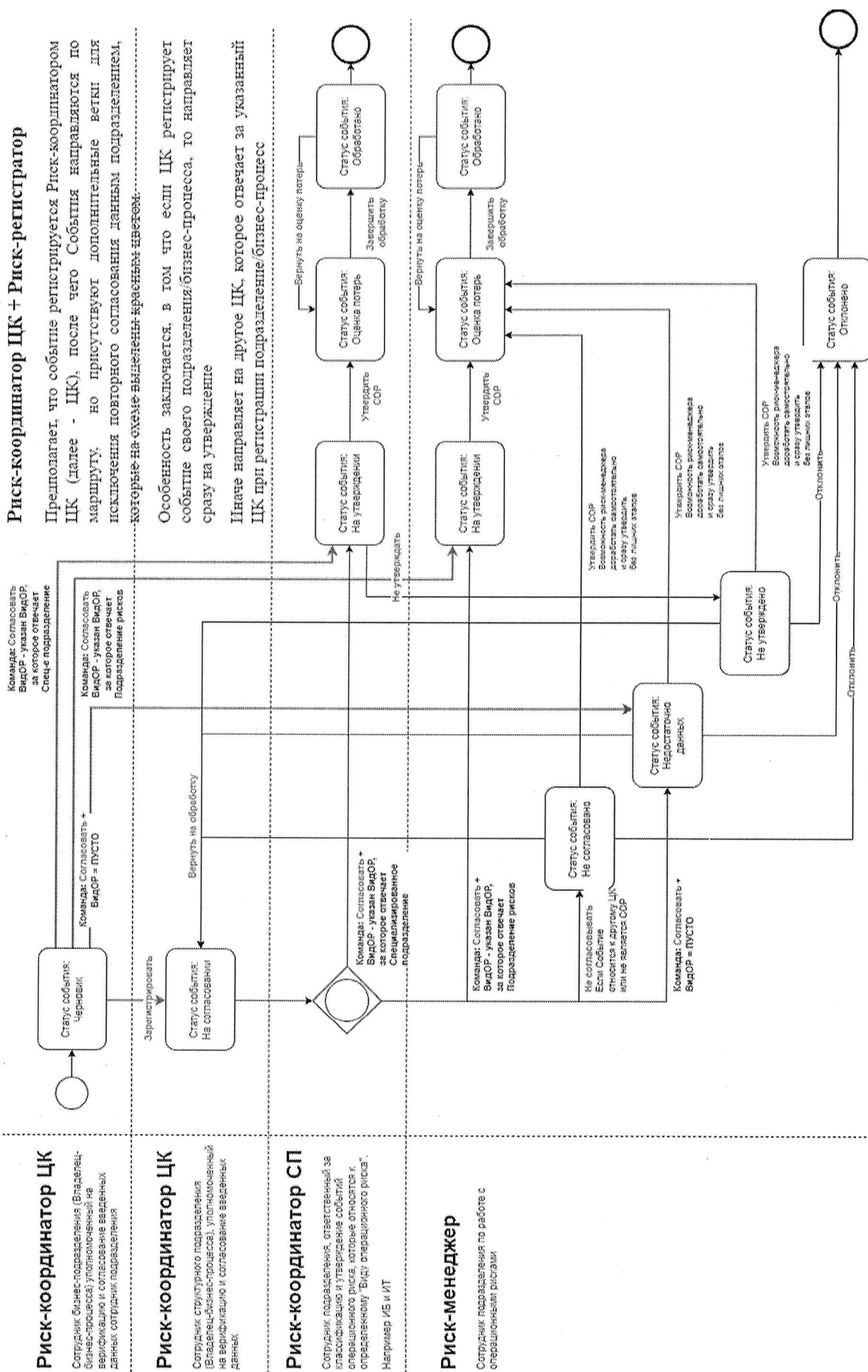
Сопоставив подразделение, ответственный за классификацию и утверждение событий операционного риска, которые относятся к определенному "Виду операционного риска". Например ИБ и ИТ

Сотрудники подразделения по борьбе с
оперативным розыском

Предполагает, что событие регистрируется любым выделенным сотрудником по месту возникновения события, после чего Событие направляется по маршруту, проходя через Центр компетенций Владельца бизнес-процесса и далее на утверждение Специализированному подразделению или Риск-менеджеру в зависимости от указанного Вида ОР.



3.1.1.1.2 Схема маршрутизации: Риск-координатор ЦК + Риск-регистратор

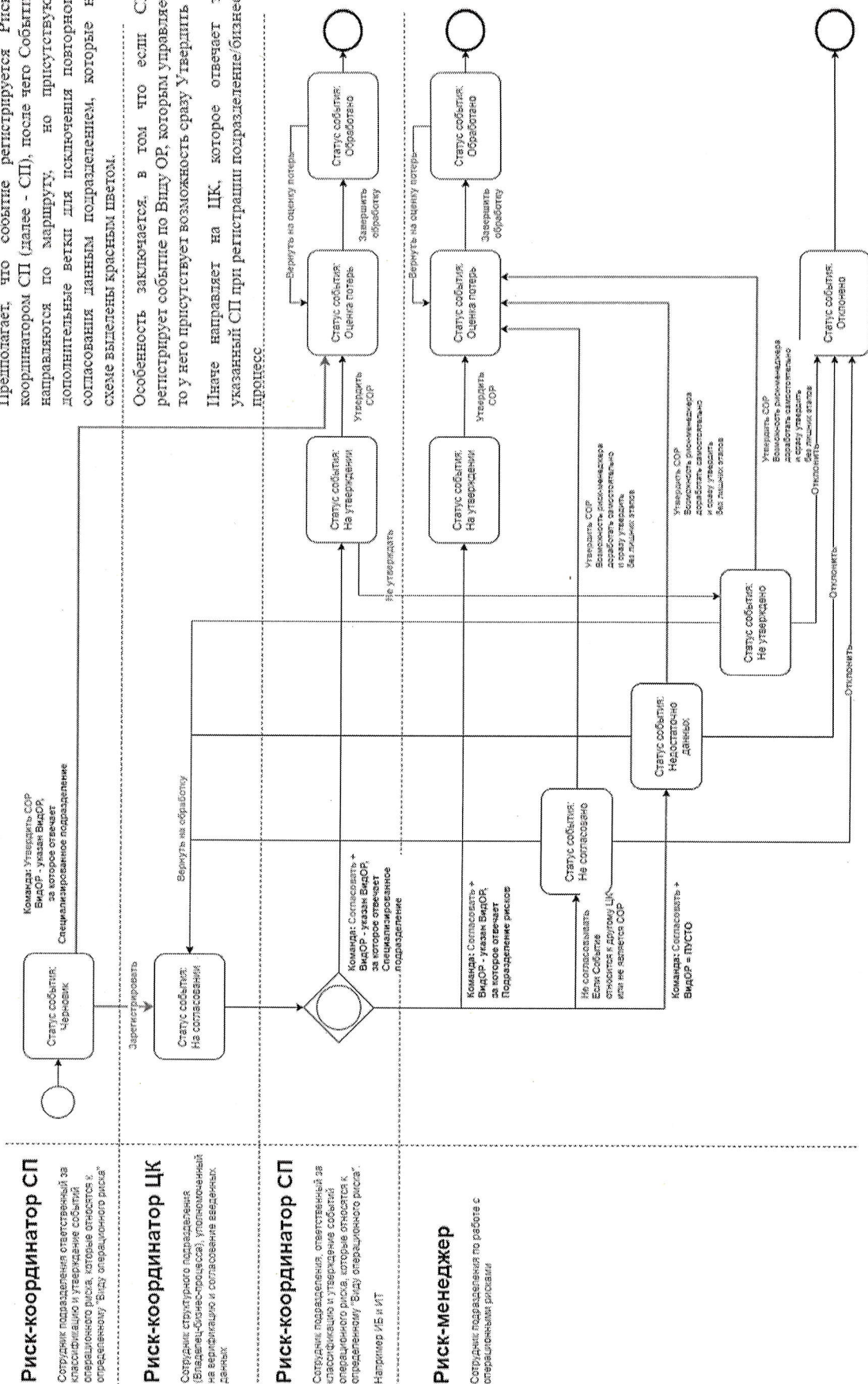


3.1.1.1.3 Схема маршрутизации: Риск-координатор СП + Риск-регистратор

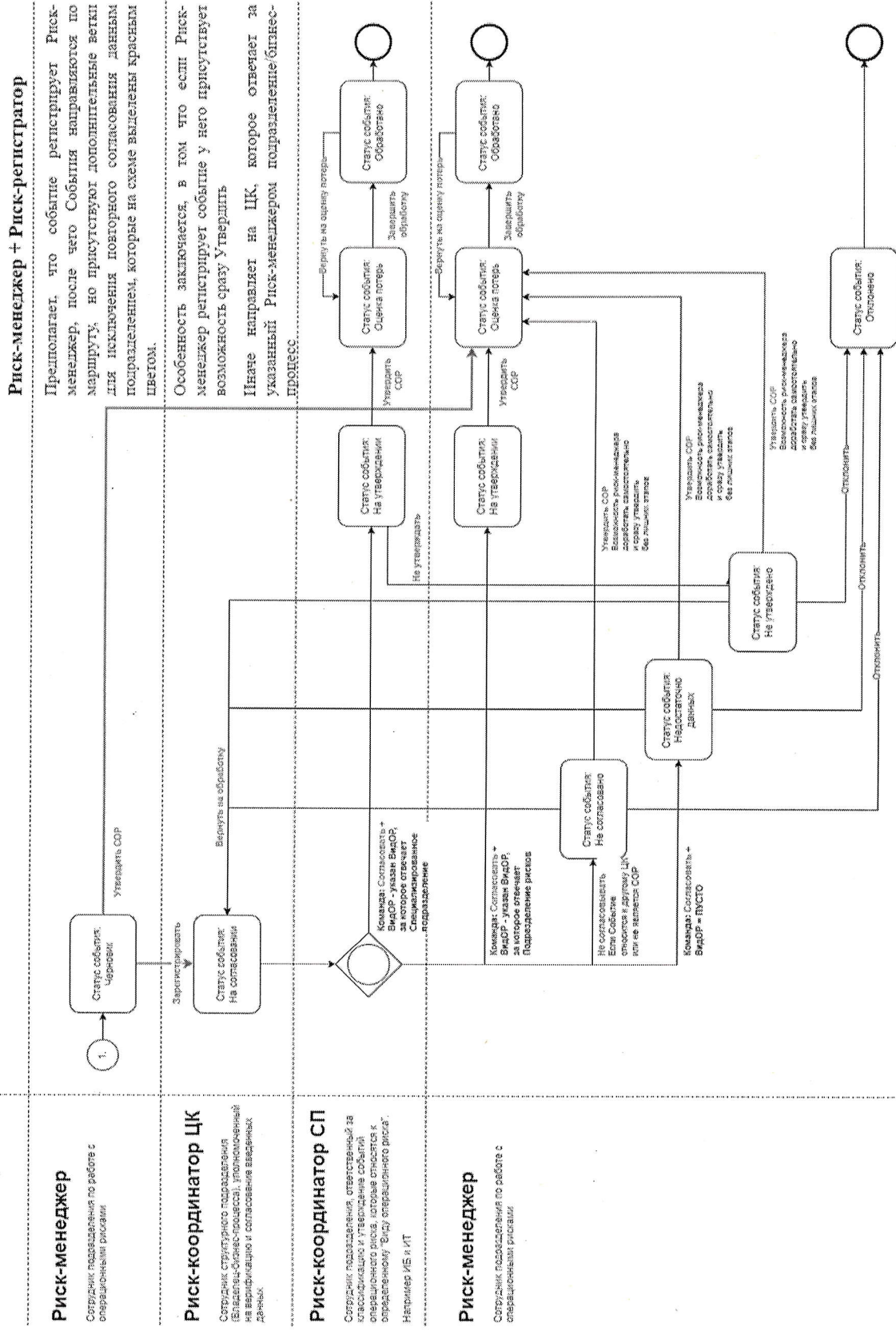
Риск-координатор СП + Риск-регистратор

Предполагает, что событие регистрируется Риск-координатором СП (далее - СП), после чего События направляются по маршруту, но присутствующим дополнительные ветки для исключения повторного согласования данным подразделением, которые на схеме выделены красным цветом.

Особенность заключается в том, что если СП регистрирует событие по Виду ОР, которым управляет, то у него присутствует возможность сразу Утвердить. Иначе направляет на ЦК, которое отвечает за указанный СП при регистрации подразделения/бизнес-процесс.



3.1.1.1.4 Схема маршрутизации: Риск-менеджер + Риск-регистратор



3.1.1.2 Описание ролей

Общее описание функциональных возможностей ролей по ведению базы Событий ОР

Роль	Исполнитель (Пользователь)	Описание
Риск-регистратор	Сотрудник бизнес-подразделения	Доступные функции: - Создание и наполнение события: - Описание мероприятия; - Ответственное подразделение; - Ответственный сотрудник (контакт); - Дата выявления; - Дата реализации; - Дата окончание инцидента; - Выбор бизнес-процесса; - Выбор вида ОР; - Добавление документов; - Добавление выполненного мероприятия; «Зарегистрировать» - регистрация события – отправка на согласование Риск-координатору ЦК по выбранному бизнес-процессу; «Заполнить по шаблону» – заполнения события по шаблону существующего события ОР.
Риск-координатор ЦК	Уполномоченный сотрудник или Руководитель бизнес-подразделения	Доступные функции: «Согласовать» - возможность согласовывания события в части корректности введенных данных. Отправка на этап «На утверждении» на «Риск-менеджера» или «Риск-координатора СП» в зависимости от Вида ОР. «Не согласовать» - возможность не согласовывания события и отправка на этап «Не

		согласовано» на «Риск-менеджера» • «Заполнить по шаблону» – заполнения события по шаблону существующего события ОР • Добавление выполненного мероприятия/меры реагирования (при необходимости, на всех этапах, кроме «Обработано»); • Запрос на обработку в подразделение(я) с плановой датой выполнения (в том числе назначение мер реагирования); • Отражение прямых, косвенных, качественных и потенциальных потерь; • Отражение возмещений; • Отражение связей с другими рисками и событиями ОР; • Добавление документов.
Риск-регистратор + Риск-координатор ЦК		При дополнении ролью «Риск-регистратор» у пользователя появляется возможность регистрировать события, но в отличии от простого сотрудника открывается форма События НЕ минимальная, а со всем объемом информации доступной роли «Риск-координатор ЦК».
Риск-координатор СП	Уполномоченный сотрудник или Руководитель подразделения, назначенный в качестве Специализированного подразделения для управления отдельным Видом операционного риска	Доступные функции: • «Утвердить СОР» - возможность утвердить Событие как Событие ОР – перевод на этап «Оценка потерь»; • «Не утверждать» - возможность не утверждать Событие и перевод на этап «Не утверждено» на Риск;

	• «Найти связанные риски» - Связь События ОР с перечнем ОР банка; • «Завершить обработку» - возможность завершить обработку События ОР и перевод на этап «Обработано»; • «Вернуть на оценку потерь» - возможность вернуть Событие ОР на этап «Оценка потерь» на этапе «Обработано»; • «Заполнить по шаблону» – заполнения события по шаблону существующего события ОР; • Добавление выполненного мероприятия/меры реагирования; • Запрос на обработку в подразделение(я) с плановой датой выполнения (в том числе назначение мер реагирования) (при необходимости, на всех этапах, кроме «Обработано»); • Отражение и подтверждение прямых, косвенных, качественных и потенциальных потерь; • Отражение и подтверждение возмещений; • Отражение связей с другими рисками и событиями ОР; • Добавление документов.
Риск-регистратор + Риск-координатор СП	При дополнении ролью «Риск-регистратор» у пользователя появляется возможность регистрировать события, но в отличии от простого сотрудника открывается форма События НЕ минимальная, а со всем объемом информации

		доступной роли «Риск-координатор СП»
Риск-менеджер	Сотрудник подразделения по работе с операционными рисками	Доступные функции: • Видят все СОР по Банку • «Утвердить СОР» - возможность утвердить Событие как Событие ОР – перевод на этап «Оценка потерь»; • «Не утверждать» - возможность не утверждать Событие и перевод на этап «Не утверждено»; • «Найти связанные риски» - Связь События ОР с перечнем ОР банка; • «Вернуть в обработку» - возможность вернуть в обработку на этапах «Не согласовано», «Не утверждено» и «Недостаточно данных» на риск-координатора ЦК; • «Завершить обработку» - возможность завершить обработку События ОР и перевод на этап «Обработано»; • «Вернуть на оценку потерь» - возможность вернуть Событие ОР на этап «Оценка потерь» на этапе «Обработано» (как СП); • Связь События ОР с ОР. • «Заполнить по шаблону» – заполнения события по шаблону существующего события ОР; • Добавление выполненного мероприятия/меры реагирования (при необходимости, на всех этапах); • Запрос на обработку в подразделение(я) с плановой датой выполнения (в том числе

		назначение мер реагирования); • Отражение и подтверждение прямых, косвенных, качественных и потенциальных потерь; • Отражение и подтверждение возмещений; • Отражение связей с другими рисками и событиями ОР • Добавление документов.
Риск-регистратор+ Риск-менеджер		При дополнении ролью «Риск-регистратор» у пользователя появляется возможность регистрировать события, но в отличие от простого сотрудника открывается форма События НЕ минимальная, а со всем объемом информации доступной роли «Риск-менеджер».

3.1.1.3 Матрица маршрутизации

Начальный статус события ОР			Конечный статус события ОР	
Роль / подразделение	Статус СОР	Команда	Статус СОР	Роль / подразделение
Риск-регистратор		Регистрация события	Черновик	Риск-регистратор
	Черновик	Зарегистрировать	На согласовании	Риск-координатор ЦК
Риск-координатор ЦК	Черновик	Согласовать	На утверждении	Риск-координатор СП/Риск-менеджер * В зависимости от Вида операционного риска (поле «Вид операционного риска»)
	На согласовании	Согласовать	На утверждении	
		Не согласовывать	Не согласовано	Риск-менеджер
Риск-координатор СП	Черновик	Зарегистрировать	На согласовании	Риск-координатор ЦК
		Утвердить СОР	Оценка потерь	Риск-координатор СП
	На утверждении	Утвердить СОР	Оценка потерь	Риск-координатор СП
	Оценка потерь	Завершить обработку	Обработано	Риск-координатор СП
	Обработано	Вернуть на оценку потерь	Оценка потерь	Риск-координатор СП
	На утверждении	Не утверждать	Не утверждено	Риск-менеджер
Риск-менеджер	Черновик	Зарегистрировать	На согласовании	Риск-координатор ЦК
		Утвердить СОР	Оценка потерь	Риск-координатор СП/Риск-менеджер * В зависимости от Вида операционного риска (поле «Вид операционного риска»)
	Недостаточно данных	Вернуть в обработку	На согласовании	Риск-координатор ЦК
	Не согласовано	Вернуть в обработку	На согласовании	Риск-координатор ЦК
		Отклонить	Отклонено	Риск-менеджер
		Утвердить СОР	Оценка потерь	Риск-координатор СП/Риск-менеджер * В зависимости от Вида операционного риска (поле «Вид операционного риска»)

	Не утверждено	Вернуть в обработку	На согласовании	Риск-координатор ЦК
		Отклонить	Отклонено	Риск-менеджер
		Утвердить СОР	Оценка потерь	Риск-координатор СП/Риск-менеджер
	Обработано	Вернуть на оценку потерь	Оценка потерь	* В зависимости от Вида операционного риска (поле «Вид операционного риска»)
	*Для экстренных случаев			
	Любой	Направить на подразделение	Выбранный	Выбранное подразделение
	Черновик, На согласовании, на утверждении	Взять в обработку	На утверждении	Риск-менеджер
	Оценка потерь	Взять в обработку	Оценка потерь	Риск-менеджер

3.1.1.4 Особенности

3.1.1.4.1 Запросы на обработку

Для гибкости и привлечения параллельно других подразделений к работе с Событием основная маршрутизация дополнена функциональностью для назначения задач (запросов на обработку):

- Для назначения мероприятий
- Для назначения мер реагирования
- Для назначения прочих задач (предоставить заключение, дать пояснение и т.д.)

Команда для назначения запроса доступна для пользователей со следующими ролями:

- Риск-координатор СП
- Риск-менеджер

Команда: Отправка запросов на обработку

Алгоритм:

1. Выбирается одно или несколько подразделений, после выбирается мероприятие.
2. Для каждого типа мероприятия можно установить нормативный срок исполнения, в соответствии с ним будет устанавливаться плановая дата обработки, в случае превышения, которой будет индикация подобных запросов в системе и уведомление на почту.
3. Наличие открытого запроса на обработку на подразделении, дает возможность дополнения События.

3.1.2 Преднастроенный перечень КПУРОВ

№	Контрольный показатель уровня операционного риска
1	Общая сумма чистых прямых потерь, понесенных кредитной организацией от реализации событий операционного риска за вычетом чистых прямых потерь от реализации событий риска информационной безопасности за определенный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года
2	Отношение общей суммы валовых прямых потерь от реализации событий операционного риска за вычетом валовых прямых потерь от реализации событий риска информационной безопасности, понесенных кредитной организацией за годовой период, к базовому капиталу кредитной организации на последнюю отчетную дату года

№	Контрольный показатель уровня операционного риска
3	Отношение общей суммы чистых прямых потерь (включая чистые прямые потери от реализации событий риска информационной безопасности), понесенных кредитной организацией за год, к показателю объема операционного риска
4	Отношение общей суммы валовых прямых потерь от реализации событий операционного риска за вычетом валовых прямых потерь от реализации событий риска информационной безопасности, понесенных кредитной организацией за год, к показателю объема операционного риска
5	Отношение суммы чистых прямых потерь от реализации событий операционного риска, понесенных кредитной организацией за год, за вычетом чистых прямых потерь от реализации событий риска информационной безопасности к показателю объема операционного риска
6	Доля выявленных (по количеству) в ходе оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением, внешним экспертом или Регулятором, событий операционного риска с валовыми прямыми потерями, превышающими порог регистрации, которые кредитная организация не отразила в базе событий, по отношению ко всем зарегистрированным в базе событий событиям операционного риска с валовыми прямыми потерями, превышающими порог регистрации, за годовой период, к которому относится проверяемый период
7	Отношение сумм валовых прямых потерь от реализации выявленных в ходе оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением, внешним экспертом или Регулятором, событий операционного риска с прямыми потерями, превышающими порог регистрации, которые кредитная организация не отразила в базе событий, к общей сумме валовых прямых потерь от реализации всех событий операционного риска, зарегистрированных в базе событий с прямыми потерями, превышающими порог регистрации, за годовой период, к которому относится проверяемый период
8	Общая сумма чистых прямых потерь от реализации событий риска информационной безопасности за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года
9	Общая сумма валовых прямых потерь от реализации событий риска информационной безопасности, связанных с переводами денежных средств и платежами в платежных системах за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года
10	Отношение общей суммы чистых прямых потерь от реализации событий риска информационной безопасности, понесенных кредитной организацией за отчетный период (первый квартал, полугодие, девять месяцев, год), к базовому капиталу кредитной организации на последнюю отчетную дату года
11	Отношение суммы валовых прямых потерь от реализации событий риска информационной безопасности, понесенных кредитной организацией при выполнении кредитной организацией функций участника платежной системы Центрального Банка Узбекистана, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме осуществленных кредитной организацией операций по переводу денежных средств через платежную за этот же период
12	Отношение суммы валовых прямых потерь от реализации событий риска информационной безопасности, связанных с переводами денежных средств и платежами в платежных системах, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме переводов денежных средств и платежей в платежных системах за этот же период
13	Отношение суммы денежных средств, по которой получены уведомления, связанные с осуществлением перевода денежных средств без согласия клиента, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме переводов денежных средств за этот же период

№	Контрольный показатель уровня операционного риска
14	Доля реализованных (по количеству), то есть не предотвращенных системой информационной безопасности кредитной организации, событий риска информационной безопасности с ненулевой величиной валовых прямых потерь, которые кредитная организация не отразила в базе событий, по отношению ко всем событиям риска информационной безопасности, зарегистрированным в базе событий, с ненулевой величиной валовых прямых потерь в течение отчетного периода (первого квартала, полугодия, девяти месяцев, года)
16	Общая сумма валовых прямых и сумм величин косвенных потерь от реализации событий операционного риска, определяемых расчетным образом, за вычетом суммы валовых прямых и сумм величин косвенных потерь от реализации событий риска информационной безопасности, за определенный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года
17	Отношение суммы чистых прямых и сумм величин косвенных потерь от реализации событий операционного риска, определяемых расчетным образом, за вычетом суммы чистых прямых и сумм величин косвенных потерь от реализации событий риска информационной безопасности, к общему капиталу (собственным средствам) кредитной организации на последнюю отчетную дату года
18	Оценка эффективности функционирования системы управления операционным риском, проведенная уполномоченным подразделением
19	Оценка эффективности функционирования системы управления риском информационной безопасности, проведенная уполномоченным подразделением и (или) внешним экспертом (специализированной организацией или квалифицированным внешним экспертом) по решению совета директоров (наблюдательного совета) кредитной организации
20	Отношение количества операций по переводу денежных средств, соответствующих признакам осуществления перевода денежных средств без согласия клиента - физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общему количеству операций по переводу денежных средств за этот же период
21	Отношение суммы денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента - физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме денежных средств по операциям по переводу денежных средств за этот же период
22	Отношение количества операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента - физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств и по которым получены подтверждения клиентов - физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены от клиентов - физических лиц подтверждения возобновления исполнения распоряжений, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к количеству операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента - физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за этот же период
24	Отношение суммы денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента - физического лица, в отношении которых кредитная организация не приняла к исполнению и (или)

№	Контрольный показатель уровня операционного риска
	приостановила исполнение распоряжений о совершении операций по переводу денежных средств и по которым получены подтверждения клиентов - физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены от клиентов - физических лиц подтверждения возобновления исполнения распоряжений, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента - физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за этот же период
25	Отношение количества операций по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств и по которым получены уведомления от клиентов - физических лиц об использовании электронного средства платежа без их согласия, в том числе, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к количеству операций по переводу денежных средств без согласия клиента - физического лица за этот же период
26	Отношение суммы денежных средств по операциям по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств и по которым получены уведомления от клиентов - физических лиц об использовании электронного средства платежа без их согласия, в том числе, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств по операциям по переводу денежных средств без согласия клиента - физического лица за этот же период
27	Отношение суммы денежных средств, возмещенной (возвращенной) клиентам, по которой получены уведомления от клиентов об использовании электронного средства платежа без их согласия, в том числе, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств, в отношении которой получены такие уведомления, за этот же период
28	Оценка соответствия уровню защиты информации в отношении процесса 1 «Обеспечение защиты информации при управлении доступом»
29	Оценка соответствия уровню защиты информации в отношении процесса 5 "Предотвращение утечек информации"
30	Оценка выполнения требований к обеспечению защиты информации, применяемых в отношении объектов информационной инфраструктуры

3.1.3 Преднастроенный перечень КИРов

КИРы для экспертного мониторинга:

№	Ключевой индикатор риска
1	Составлять не менее 50 процентов коэффициента прогулов сотрудников (руководители, то есть директор департамента и вышестоящие сотрудники, руководители филиалов);
2	Повторение более 60 процентов системных недостатков, выявленных службой внутреннего аудита;
3	Повторение более 60 процентов системных недостатков, выявленных Службой комплаенс-контроля;
4	Кибератаки на банковские информационные системы;
5	Внеплановый простой программного обеспечения IABS более 2 часов;
6	Нанесение ущерба репутации Банка вследствие распространения негативной информации о Банке в официальных средствах массовой информации.

3.1.4 Преднастроенный реестр операционных рисков

№	Реестр операционных рисков
1	Умышленное сокрытие информации о совершенных сделках
2	Подписание несанкционированных сделок с финансовыми потерями
3	Мошенничество в кредитование, сбережения и кассира в розничной торговле

№	Реестр операционных рисков
4	Мошенничество при обслуживании счетов клиентов
5	Кража или мошенничество
6	Незаконная смена активов
7	Умышленное уничтожение, повреждение или незаконное присвоение активов банка
8	Подделка, кража или уничтожение банковских документов
9	Использование банковской тайны или информации, составляющей коммерческую тайну, в личных целях.
10	Присвоение чужих денег, хранящихся в банке
11	Управление счетами клиентов от своего имени
12	Осуществление деятельности, не предусмотренной лицензией или внутренними документами банка.
13	Взяточничество или злоупотребление служебным положением
14	Мошенничество с использованием инсайдерской информации
15	Предоставление неверной или неполной информации
16	Участие в легализации доходов, полученных преступным путем
17	Осуществление банковских операций без надлежащих документов или с поддельными документами
18	Не заключение договоров залогов или незаконное выселение залогового имущества.
19	Ограбление банка, грабеж и мошенничество
20	Незаконное присвоение денежных средств с использованием поддельных документов
21	Другие подделки
22	Некорректное начисление процентов по депозитам ФЛ вследствие сбоя ПО
23	Некорректное начисление процентов по депозитам ФЛ вследствие ошибки бэк-офиса
24	Ошибочный платеж ФЛ вследствие сбоя систем
25	Нарушение безопасности банковских информационных систем, кибератаки
26	Кража информации (с финансовыми потерями)
27	Расчет сверхурочной работы и премий
28	Занижение заработной платы и премий
29	Подача исков о выплате работникам компенсаций (компенсаций).
30	Телесные повреждения сотрудникам банка и третьим лицам;
31	Нарушение трудового законодательства, правил охраны труда и гигиены.
32	Дискриминация работников в трудовых отношениях
33	Раскрытие личной информации и конфиденциальной информации сотрудников
34	Недостатки банковских услуг и продуктов
35	Принудительная передача банковских услуг и продуктов клиентам или неправильные рекомендации клиентам
36	Завышение цен с клиентов
37	Нарушение требований раскрытия информации
38	Незаконная загрузка продуктов или услуг
39	Искусственное увеличение банковских комиссий
40	Неправомерное использование конфиденциальной информации
41	Действия по установлению монополии
42	Правила торговли, нарушение рыночной деятельности
43	Манипулирование рынком
44	Осуществление финансовых операций, не указанных в лицензии и истечение срока действия лицензии
45	Ошибки в модели
46	Невыполнение требований по идентификации и проверке клиентов.
47	Ущерб, причиненный стихийными бедствиями

№	Реестр операционных рисков
48	Человеческие потери от внешних источников (терроризм, вандализм)
49	Кредитные коллекции и другие юридические документы не хранятся в железных сейфах.
50	Перебои и сбои в работе программного обеспечения (iABS и т.п.).
51	Выход из строя телекоммуникационного оборудования и оборудования
52	Отключения в инженерных сетях.
53	Недостатки хранения баз данных (серверов).
54	Недостатки в состоянии и оперативности антикибер и антивирусного ПО.
55	Ошибки и упущения при расчете доходов банка (процентов и комиссий) и невзысканных штрафов.
56	Ошибки и упущения при расчете и оплате банковских расходов (недостаток и переплат)
57	Нарушение процедуры банковской гарантии
58	Нарушение кредитных требований и ошибки
59	Недостатки в кредитном мониторинге
60	Слабые стороны в процессе работы с проблемными активами
61	Выявленные недостатки и излишки (касса, депозит, ПК, банкомат, инфактос и т.д.)
62	Недостатки в техническом оснащении кассовой сети и кассового склада
63	Ошибки и упущения в розничном бизнесе (депозит, ПК, МДП, ОП, Терминал, Банкомат и т.д.)
64	Неисполнение заявок (в т. ч. нарушение сроков) в рамках брокерского обслуживания клиентов вследствие нарушения внутренних процессов
65	Ошибки на практике, связанные с внешнеэкономической деятельностью
66	Недостатки в мониторинге платежных операций и подготовке отчетов;
67	Ошибки в привлечении клиентов и ведении документов;
68	Ненадлежащее управление счетами клиентов, проблемы с торговыми партнерами и поставщиками;
69	Ошибки при вводе и хранении данных, учете;
70	Недостатки, связанные с определением принадлежности заемщика к группе взаимосвязанных заемщиков;
71	Проблемы с отправкой платежных документов;
72	Неполнота документов клиента;
73	Ошибки и штрафы при предоставлении отчетности в Центральный банк и другие органы в соответствии с законодательством;
74	Нарушения при исполнении договоров и штрафы, взимаемые по решению суда;
75	Несанкционированное использование расчетных счетов клиентов;

3.2 Требования к архитектуре решения

В рамках настоящего Технического задания под внедрением понимается установка, настройка и адаптация ГППО в информационно-технической инфраструктуре Заказчика, а также формирование перечня типовых объектов Системы, в том числе иные работы по доработке Системы по требованию Заказчика.

3.2.1 Требования к архитектуре Системы

Программные компоненты, необходимые для работы Системы, должны предоставляться Исполнителем, кроме операционной системы и СУБД.

Общая архитектура создаваемой Системы должна соответствовать предлагаемому Исполнителем ГППО.

Система должна работать в закрытом сегменте Заказчика без доступа в сеть Интернет, в том числе без доступа для получения обновлений.

Система должна состоять из СУБД, серверного и клиентского приложения.

Серверная часть Системы:

- серверная часть должна быть конфигурируема;
- должно допускаться использование операционных систем Linux (CentOS, Ubuntu, Debian), Windows Server 2016 и новее;

- должна поддерживаться работа серверной части на виртуальной машине (VmWare) и/или в среде контейнеризации (Docker).

Аппаратное обеспечение предоставляется Заказчиком по требованию Исполнителя. Предварительные требования к серверным ресурсам согласно документации прикладного программного обеспечения использованной в системе АСУОР:

Ограничения сайзинга:				
• До 50 одновременно активных пользователей процессов обработки СОР/Рисков; • До 100 одновременно активных пользователей RCSA; • До 5 000 загружаемых объектов в буфер в сутки; • Сайзинг учитывает только high availability, для обеспечения disaster recovery необходима копия промышленной среды; • В ходе проектирования и реализации системы может понадобиться изменение конфигурации серверов (их количества и распределения между ними ресурсов) при сохранении общих мощностей; • Расчёт дискового пространства на сервере СУБД предварительный. В дальнейшем необходим мониторинг свободного пространства и расширение по мере необходимости.				
Тип среды	Конфигурация	CPU (кол-во ядер) Intel® Xeon™ 2.40GHz+	RAM (Gb)	HDD (Gb)
• Продуктивная;	Сервер СУБД (PostgreSQL 11+)	4	24	250 Gb
• Предпродуктивная;	Сервер приложений (WildFly 14.0.1.Final)	6	32	250 Gb
	Резервный сервер СУБД (PostgreSQL 11+)	4	24	250 Gb
	Резервный сервер приложений (WildFly 14.0.1.Final)	6	32	250 Gb
Бинарные файлы предполагается хранить на сервере, размер файлового хранилища: 600 событий в месяц*40 Mb = 23,5 Gb в месяц*12 = ~282 Gb в год. Необходим дополнительный мониторинг свободного места и расширение по мере необходимости				
• Тестовая	Сервер СУБД (PostgreSQL 11+)	4	16	120 Gb
• обезличенная;	Сервер приложений (WildFly 14.0.1.Final)	4	16	120 Gb
*Опционально:				
• Тестовая;	Файловое хранилище: 100 Gb в год. Необходим дополнительный мониторинг свободного места и расширение/освобождения по мере необходимости.			
• Разработческая				

3.3 Рабочая станция

4. Рабочее место	5. Минимальный требования
6. АРМ Пользователя	7. Двух-ядерный процессор 2.5GHz, 4Gb ОЗУ*
	8. * В условиях работы с большими, сложными формами системные требования для АРМ Пользователя рекомендуется пересматривать в большую сторону, до уровня требований АРМ Конфигуратора.
9. АРМ Конфигуратора	10. Двух-ядерный процессор 3.0GHz, 8Gb ОЗУ*

Для обеспечения требований к времени обработки экранных форм (АРМ Пользователя) с прикрепленными вложениями (файлы, сканированные документы) в суммарном размере не более 10 мегабайт, должно быть подключено к сети интернет со следующими характеристиками¹:

- Минимальная гарантированная пропускная ширина канала с рабочего места оператора до сервера Platform - не менее 10 Mbit/s;

¹ в случае если характеристики подключения к сети интернет не соответствуют указанным требованиям, то возможна деградация качества сервиса пропорционально снижению характеристик.

- Латентность канала с рабочего места оператора до сервера Platform не более 100ms.

Клиентская часть Системы:

- клиентская часть должна быть реализована в виде веб-приложения;
- допускается реализация клиентской части для администрирования в виде толстого (декстопного) приложения;
- web-приложение должно поддерживать браузер Chrome и функционировать на персональных компьютерах под управлением операционных система семейства Windows и Linux
- взаимодействие с серверной частью должно осуществляться по протоколу HTTP(S).

База данных Системы:

- Для эксплуатации Системы должно быть допустимо использование только промышленных версий СУБД PostgreSQL или MS SQL;

10.1.1 Требование к взаимодействию с внешними источниками

Система «из коробки» должна обладать универсальным шлюзом для взаимодействия с ней с использованием протокола взаимодействия RestAPI:

- Шлюз «из коробки» должен предоставлять метод для аутентификации внешней системы для последующей процедуры взаимодействия.
- Шлюз «из коробки» должен предоставлять возможность запись внешней системой данных (одного или нескольких связанных между собой объектов) в структуру данных любого объекта Системы по его метаописанию
- Шлюз «из коробки» должен обладать возможностью предоставления по запросу внешней системы, которая прошла аутентификацию на шлюзе, получение данных одного или нескольких объектов.

Система «из коробки» должна взаимодействовать с Active Directory с целью аутентификации пользователей, почтовой системой MS Exchange с целью рассылки уведомлений путем минимальных настроек, а именно ввода значений почтового и доменного серверов.

Система «из коробки» должна позволять синхронизацию пользователей с Active Directory по сопоставлению предустановленной роли в системе и доменной группе. Система должна позволять «из коробки» аутентификацию с использованием OpenIDConnectio

Перечень смежных систем и форматов взаимодействия может быть пересмотрен в процессе создания Системы, в связи с вводом в промышленную эксплуатацию Заказчиком новых систем. При этом, Система должна поддерживать способ взаимодействия приложения с сервером через RestAPI, dblink (интеграция на уровне баз данных) и SOAP.

10.1.2 Требования к составу и объему лицензии

Состав и объем передаваемой лицензии должен обеспечивать следующими функциональными возможностями:

10.1.2.1 Срок действия лицензий, патентов и корреспондентских платежей, если они предусмотрены и требуется для работы системы АСУОР, должны быть бессрочными с момента сдачи-приёмки системы АСУОР.

10.1.2.2 Ведение базы событий операционного риска (COP) и реестра операционных рисков (OP)

1.1. Возможность автоматизированного выявления информации из Информационной Системы (ИС) Банка о реализовавшихся или возможных в будущем Событиях операционного риска (далее - COP);

1.2. Возможность неавтоматизированного выявления и сбора информации о COP, предусматривающие выявление информации и проведение анализа обстоятельств и причин, произошедших COP, с использованием экспертного мнения, в случае если автоматизированное выявление и сбор информации о COP невозможны;

1.3. Возможность регистрации выявленных COP в базе, в том числе ввод информации по алгоритмизированным правилам их классификацию, определение потерь от реализации, определение стоимости возмещений потерь от реализации COP в базе событий, также обновление информации о COP в базе событий при выяснении новых обстоятельств их реализации и в зависимости от вида OP;

- 1.4. Возможность оставить на контроле события, не проходящие по порогу регистрации, не включая в базу СОР, но с возможностью просмотра с помощью расширенной выгрузки;
- 1.5. Возможность актуализации источников информации о СОР и сведений о Центрах компетенций, ответственных за их сбор;
- 1.6. Возможность настройки правил верификации собираемых данных;
- 1.7. Возможность сбора внешних СОР;
- 1.8. Возможность идентификации, сбора, обработки и дальнейшее ведение реестра операционных рисков (далее – ОР), в том числе в зависимости от вида ОР;
- 1.9. Возможность настройки управления планами по проведению мероприятий с целью минимизации рисков;
- 1.10. Возможность мониторинга и отслеживания ОР с применением Ключевых индикаторов риска (далее – КИР), а именно создание индикаторов, сбор фактических значений, в том числе возможность сбора данных в автоматическом режиме из ИТ-систем Банка;
- 1.11. Возможность проведения во внутреннем структурном подразделении Банка процедур самооценки рисков и контролей (создание анкет и анкетирование);
- 1.12. Возможность настройки автоматического формирования отчетности по заданным параметрам;
- 1.13. Возможность настройки оповещения участников процессов при возникновении важных событий при обработке СОР, ОР, в рамках мониторинга КИР, КПУР и иных событий;
- 1.14. Возможность ведение реестра бизнес-процессов с возможностью оценки критичности бизнес-процесса (BIA);
- 1.15. Возможность настройки процесса обработки СОР и ОР в рамках их видов;
- 1.16. Возможность ведения базы СОР по отдельным видам ОР;
- 1.17. Возможность выгрузки информации по СОР и ОР для проведения последующей обработки вне системы;
- 1.18. Возможность настройки автоматической загрузки из ИС Банка в АСУОР (пример: Антифрод система, Service Desk, OTRS);
- 1.19. Возможность разграничения функциональности в соответствии с бизнес-ролью пользователя (Владельцы риска, Центры компетенции, виды ОР);
- 1.20. Связь между модулями системы и возможность быстрого перехода по всем введенным ссылкам (сквозной переход между объектами) и обратно;
- 1.21. Возможность настройки автоматического обновления справочников и классификаторов в результате их изменения;
- 1.22. Возможность настройки автоматического отслеживания хода обработки соответствующих сущностей с возможностью настройки предусмотренных параметров отслеживания;
- 1.23. Возможность формирования выборки из соответствующих объектов с настройкой: поиск, сортировка по полям, формирование выборки по критериям (фильтрация);
- 1.24. Возможность импорта и экспорта информации в формате xlsx и других форматов;
- 1.25. Возможность автоматического заполнения полей по определенным правилам, при работе с различными объектами системы;
- 1.26. Возможность автоматического заполнения полей, определенных по Оператору ввода (организация, подразделение, ФИО и т.д.);
- 1.27. Возможность формирования шаблонов и типовой информации, которая бы использовалась для ввода или обработки различных сущностей АСУОР;
- 1.28. Возможность разграничения прав доступа к объектам АСУОР на основании ролевой модели доступа АСУОР;
- 1.29. Возможность ведения справочников с иерархической структурой и возможность редактирования через пользовательский интерфейс;
- 1.30. Возможность сохранности данных и защиту от искажений с помощью внешних средств для управления разными компонентами Программы;
- 1.31. Возможность загрузки и хранения различных сопроводительных файлов, для каждого объекта и просмотр файлов внутри АСУОР;

- 1.32. Возможность настройки внесения сопроводительных комментариев, в различных объектах, для внутреннего использования, а также переписки;
 - 1.33. Возможность настройки управленческих отчетов для получения информации, запускаемых по расписанию и/или событию;
 - 1.34. Возможность автоматизации и настройки бизнес-процессов для управления операционным риском, включая, но не ограничиваясь:
 - 1.34.1. Ведение События ИТ/ИБ,
 - 1.34.2. Инциденты ИТ/ИБ,
 - 1.34.3. Самооценка;
 - 1.34.4. Сценарный анализ;
 - 1.34.5. Преднастроенный алгоритм расчет Капитала на покрытие операционного риска;
 - 1.34.6. Расчет рисков информационной безопасности;
 - 1.34.7. Визуализация отчетности;
 - 1.34.8. Планы мероприятий.
 - 1.35. возможность хранения и просмотра информации об изменениях с указанием даты, автора изменений, а также предыдущих и текущего значениях атрибутов;
 - 1.36. Контроль сроков работы с контрольными мероприятиями.
 - 1.37. Автоматизация и настройки бизнес-процессов для управления операционным риском, в части инцидентов ИТ/ИБ должна осуществляться с учётом Регламента банка по управлению Инцидентами ИТ/ИБ. Ведение инцидентов операционной надежности (ИОН)
 - 1.38. Возможность ведения справочников для классификации событий, которые являются инцидентами операционной надежности
 - 1.38.1. технологические процессы кредитной организации;
 - 1.38.2. технологические участки;
 - 1.38.3. объекты информационной инфраструктуры;
 - 1.38.4. автоматизированные системы;
 - 1.38.5. программное обеспечение;
 - 1.38.6. телекоммуникационное оборудование;
 - 1.38.7. средства вычислительной техники.
 - 1.38.8. типы инцидентов операционной надежности;
 - 1.38.9. участники технологических процессов;
 - 1.38.10. поставщики услуг в сфере информационных технологий;
 - 1.38.11. субъекты доступа технологических процессов;
 - 1.38.12. каналы передачи защищаемой информации.
 - 1.39. Импорт/Наполнение справочников по пункту 2.1;
 - 1.40. Установление целевых показателей операционной надежности (КПУР) с учетом установленных контрольных значений и возможность их отслеживания в соответствии с экспертной оценкой подразделений:
 - 1.40.1. допустимая доля деградации технологического процесса;
 - 1.40.2. допустимое время простоя и (или) деградации технологического процесса;
 - 1.40.3. допустимое суммарное время простоя и (или) деградации технологического процесса в течение очередного календарного года;
 - 1.40.4. показатели соблюдения режима работы (функционирования) технологического процесса.
 - 1.41. Возможность проведения процедуры самооценки и сценарного анализа для рисков по инцидентам операционной надежности;
 - 1.42. Отчет по целевым показателям операционной надёжности в разрезе технологических процессов кредитной организации.
- ГППО по результатам внедрения должно быть доработано и настроено под индивидуальные особенности системы управления операционным риском в соответствии с объемом работ, отраженным в Договоре.
- В случае использования при создании Системы программ (программных комплексов или компонентов), разработанных третьими лицами, условия, на которых передается право на

использование (исполнение) этих программ, не должны накладывать ограничений, препятствующих использованию Системы по ее прямому назначению.

10.1.3 Требования к функциональным возможностям

1. Платформа ГППО должна содержать инструменты настройки бизнес-процессов со стороны бизнес-администратора Системы;
2. Платформа ГППО должна позволять дальнейшее расширение функциональности за счет внедрения новых модулей и функциональных подсистем;
3. Система должна иметь:
 - 3.1. возможность настройки под индивидуальные особенности управления операционным риском Заказчика;
 - 3.2. возможность автоматического расчета полей на основе связанных объектов (Например, расчет агрегированных сумм потерь события на основе связанных последствий и возмещений);
 - 3.3. преднастроенную, изменяемую под требования Заказчика ролевую модель;
 - 3.4. Автоматическое сохранение в риске текущего уровня риска на основе последней проведенной оценки риска и сохранение в карточке предыдущих оценок по риску;
 - 3.5. модульную архитектуру, в том числе с обеспечением связи между объектами модулей, с возможностью перехода из одного объекта модуля в объект другого модуля по клику мыши;
 - 3.6. интуитивно-понятный пользовательский интерфейс, включая отчетность, реализованный на русском и узбекском языках;
 - 3.7. настраиваемые ограничения по количеству символов при заполнении полей;
 - 3.8. возможность контроля исполнения мероприятий;
 - 3.9. инструментарий для агрегации результатов самооценки;
 - 3.10. возможность и инструментарий для построения тепловой карты рисков по результатам самооценки рисков;
 - 3.11. руководство пользователя в разбивке по ролям.
4. Взаимодействие бизнес-пользователей с Системой должно осуществляться через web-интерфейс;
5. В Системе должна быть реализована функция уведомления по электронной почте о любых пользовательских событиях в Системе;
6. В Системе должен быть реализован механизм подсвечивания задач в работе у пользователя Системы, управление задачами в одном месте. Уведомление о задаче в интерфейсе Системы;
7. В Системе должны быть реализованы преднастроенные экранные web-формы (карточки) по объектам (события, риски, анкеты самооценки, контроли, мероприятия, планы, процессы, отчеты);
8. В системе должен использоваться многоуровневый принцип построения данных в Системе (использование витрины данных);
9. Система должна обеспечивать работу с данными:
 - 9.1. поиск по атрибутам карточек документов Системы;
 - 9.2. возможность вложения документов (без ограничения объема) и просмотр загруженного в Систему документа;
 - 9.3. возможность создания быстрых фильтров с возможностью их сохранения при работе с объектами;
 - 9.4. сортировку результатов поиска по релевантности / дате изменения объекта;
 - 9.5. наличие механизма импорта исторических данных Заказчика;
10. Система должна обеспечивать хранение данных и документов в Системе, защиту от искажений, логирование изменений (любых действий, выполняемых бизнес-пользователями);
11. Система должна обеспечивать контроль работы пользователя с данными в интерфейсе Системы:
 - 11.1. Автоматический контроль заполнения полей с запретом сохранения без заполнения обязательных полей;
 - 11.2. Проверку корректности заполнения количественных полей, полей с датами;

- 11.3. Наличие этапов проверки в ходе заполнения полей на соответствие форматов вводимых данных, полноты заполнения обязательных полей, а также на корректное заполнение полей при их сочетании друг с другом;
- 11.4. Система должна обеспечивать работу со справочниками:
- 11.5. наличие преднастроенных иерархических справочников;
- 11.6. автоматическое обновление данных при актуализации справочников, классификаторов;
- 11.7. возможность редактирования и обновления справочников бизнес-пользователем, в том числе при помощи загрузчика;
- 11.8. заполнение полей из справочников.
- 11.9. Система должна обеспечивать работу с отчетами:
- 11.10. возможность создания дашбордов с использованием виджетов самостоятельно пользователем;
- 11.11. выгрузку отчетов в форматах docx, xlsx;
- 11.12. отчетность в табличном и графическом виде;
- 11.13. возможность разработки новых отчетов бизнес-пользователем посредством встроенных инструментов;
12. Система должна иметь инструменты интеграции ГППО с другими ИТ-системами Заказчика (включая iABS, KomplaensControl и электронная база Департамента Внутреннего Аудита).
13. Интеграционное взаимодействие с АБС Банка, а именно запрос данных от АБС, реализуется посредством готовых сервисов из централизованного Middleware (API Manager) платформы Заказчика. API сервисы предоставляются Заказчиком на основе следующий требований:

- сальдовая оборотная ведомость из iABS по счетам 11503, 90993, 15701, 15703, 15705, 15707, 16505, 16701, 16703, 16705, 16707, 16709, 17401, 17403, 17405, 17407, 17409, 19909, 19997, 23230, 29801, 19908, 56718, (ежемесячно);
- информационная базы HR из iABS включая ФИО, должность, организационная структура, номер телефона, электронная почта сотрудников банка (ежемесячно);
- информационная база AUDIT департамента Внутреннего аудита включая информацию о ошибках, выводах и рекомендаций по событиям операционного риска определенным в результате аудита (ежемесячно);
- информационная база COMPLAENS CONTROL включая информацию о фактах и событиях операционного риска определенным в результате мониторинга (ежемесячно);
- все события поступающие в информационную базу BRB-Risk_Bot (ежедневно);
- все события и IT инциденты, поступающие в систему HelpDesk (ежедневно).

10.1.3.1 Требования к ведению базы событий операционного риска

Событие операционного риска - реализация операционного риска, фактический инцидент, который произошел бизнес-процессах кредитной организации.

Структура данных, регистрируемых по событиям операционного риска.

В рамках регистрации события операционного риска должен фиксироваться минимально следующий набор данных:

- уникальный порядковый идентификационный номер события операционного риска (группы событий операционного риска);
- идентификатор группы событий операционного риска (в случае, если события операционного риска объединены в группу);
- дату, когда событие операционного риска было зарегистрировано в базе событий (дата регистрации);
- время регистрации события операционного риска в базе событий;
- дату, когда событие операционного риска произошло или впервые началось (дата реализации);
- время, когда событие операционного риска произошло или впервые началось;

- дату (и время в случае, если характер события операционного риска это предусматривает), когда стало известно о событии операционного риска (дата выявления);
- дату и время окончания события операционного риска (дата окончания события) в случае, если наличие такой информации определяется характером события операционного риска;
- статус события операционного риска;
- подразделение, в котором произошло событие операционного риска;
- подразделение, выявившее событие операционного риска;
- описание события операционного риска (детализированное описание события операционного риска, включающее ответы на вопросы: в чем заключается событие операционного риска, каким образом оно было обнаружено, что явилось его причиной (причинами));
- категорию источника операционного риска;
- значимые источники операционного риска, которые повлияли на реализацию события операционного риска, с указанием долей их влияния в отношении события операционного риска;
- тип события операционного риска;
- вид операционного риска;
- связь с другими видами операционного риска;
- идентификатор связанного события операционного риска (в случае, если такая связь установлена);
- дополнительную классификацию типа события операционного риска в зависимости от вида риска;
- направления деятельности;
- бизнес-процесс;
- меры, направленные на уменьшение негативного влияния операционного риска;

Группа полей базы событий, содержащая информацию о потерях от реализации события операционного риска по каждому виду потерь и возмещений, включающая:

- вид потери;
- признак связи потери с другим видом риска;
- величину потери от реализации события операционного риска в стоимостном выражении;
- дату учета потери;
- информацию о бухгалтерской записи (бухгалтерских записях) в бухгалтерском учете содержащей суммы прямой потери;
- экспертную оценку качественной потери;
- агрегированную сумму валовых прямых потерь и сумму косвенных потерь накопленным итогом с даты регистрации первой потери;
- агрегированную сумму валовых прямых потерь накопленным итогом с даты регистрации первой потери;
- сумму косвенных потерь накопленным итогом с даты регистрации первой потери;

Группа полей базы событий, содержащая информацию о полученном возмещении понесенных потерь, включая:

- мероприятия, осуществленные в целях получения возмещения по понесенным потерям от реализации события операционного риска;
- вид возмещения;
- сумму возмещения;
- дату отражения возмещения на счетах бухгалтерского учета;
- информацию о бухгалтерской записи суммы возмещения;
- источники получения возмещения;
- сумму чистых потерь, определяемых с учетом возмещения.

10.1.3.2 Требования к ведению реестра операционных рисков

Операционный риск – риск убытка в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или внешних событий. Потенциальная проблема, которые кредитная организация идентифицирует во внутренних бизнес-процессах, определяет уровень существенности и другие параметры риска для определения способа реагирования с учетом или без учета применения мероприятий для снижения негативного эффекта и дальнейшего возникновения.

Объект «операционный риск» из перечня операционных рисков должен включать следующие параметры:

- наименование
- ответственное подразделение
- оценка способа реагирования
- оценка вероятности реализации
- оценка существенности потерь при реализации риска
- уровень операционного риска
- остаточный уровень операционного риска
- классификация по основным классификаторам (вид операционного риска, направление деятельности, бизнес-процесс, источник риска, тип события)
- события операционного риска, реализовавшиеся по данному операционному риску (ссылки на объекты событий)
- перечень мероприятий для снижения операционного риска
- результаты самооценки
- результаты сценарного анализа

Доступ к ведению и актуализации перечня операционных рисков должен быть исключительно у пользователей подразделения риск-менеджмента.

В рамках минимизации уровня операционного риска должны фиксироваться мероприятия по минимизации риска – отдельный объект в перечне мероприятий.

Мероприятие по снижению риска должно содержать следующие параметры:

- дата начала
- плановая дата завершения
- ответственное подразделение-исполнитель
- наименование
- вид мероприятия
- статус исполнения мероприятия
- связь с объектами системы в рамках которых было разработано мероприятие (ссылки на объекты в разрезе видов – события, риски, КИРы, КПУРы, самооценка, сценарный анализ)
- реквизиты плана мероприятий, в рамках которого реализуется мероприятие)

10.1.3.3 Требования к процедуре качественной оценки

Качественная оценка – комплекс процедур для идентификации и регулярной оценки операционных рисков для определения способа реагирования и возможных мер с снижением негативного эффекта и вероятности возникновения.

Качественная оценка должна состоять из 2-х процедур: самооценка и сценарный анализ. Объектом качественной оценки выступает конкретный операционный риск из перечня рисков.

10.1.3.3.1 Самооценка проводится по следующей процедуре.

В рамках операционного риска оценивается существенность потерь от операционного риска по следующей шкале оценок с присвоением балльной (коэффициент) оценки:

Коэффициент существенности и потерь	Сумма потерь при однократной реализации операционного риска, сум.	Качественная оценка существенности потерь
1,0	> 2 000 000 000	Катастрофический
0,8	250 000 001 – 2 000 000 000	Критический
0,7	14 000 001 – 250 000 000	Очень высокий

0,4	7 000 001 – 14 000 000	Высокий
0,3	3 500 001 – 7 000 000	Средний
0,2	1 000 001 – 3 500 000	Ниже среднего
0,1	200 001 – 1 000 000	Низкий
0,05	0 – 200 000	Несущественный

Оценивается и ранжируется вероятность реализации оцениваемого операционного риска по следующей шкале оценок с присвоением бальной (коэффициент) оценки:

Коэффициент вероятности	Периодичность реализации аналогичных операционных рисков	Коэффициент ожидаемой частоты события	Качественная оценка вероятности
0,9	Ежедневно либо несколько раз в день	250	Очень высокая
0,8	Раз в неделю	52	Высокая
0,6	Раз в месяц	12	Выше средней
0,5	Раз в квартал	4	Средняя
0,4	Раз в год	1	Низкая
0,3	Раз в два года	0,5	Очень низкая
0,2	Раз в четыре года и реже	0,25	Маловероятная

Далее путем перемножения параметров (коэффициентов) существенности потерь и вероятности возникновения определяется Уровень операционного риска:

Вероятность возникновения	Существенность потерь							
	0,05	0,1	0,2	0,3	0,4	0,7	0,8	1
0,9	0,05	0,09	0,18	0,27	0,36	0,63	0,72	0,90
0,8	0,04	0,08	0,16	0,24	0,32	0,56	0,64	0,80
0,6	0,03	0,06	0,12	0,18	0,24	0,42	0,48	0,60
0,5	0,03	0,05	0,10	0,15	0,20	0,35	0,40	0,50
0,4	0,02	0,04	0,08	0,12	0,16	0,28	0,32	0,40
0,3	0,02	0,03	0,06	0,09	0,12	0,21	0,24	0,30
0,2	0,01	0,02	0,04	0,06	0,08	0,14	0,16	0,20

Характеристики уровней риска

Уровень риска	Оценка уровня существенности операционного риска	Описание
0,36-0,90	Очень высокий	Реализация риска может оказать критическое воздействие на деятельность Банка. Требуется принятия срочных мер по его минимизации, либо его избеганию. Риск может быть принят на Банк только решением органа управления Банка.
0,16-0,35	Высокий	Риск для Банка является высоким. Разработка мер по его снижению обязательна.
0,06-0,15	Средний	Риск является значительным для деятельности Банка. Рекомендуется разрабатывать меры по его снижению.
0,2 0-0,05	Низкий	Риск не является существенным для Банка. Разработка мер по его снижению не обязательна, но допустима.

Далее для определения остаточного риска оцениваются контрольные процедуры (эффективность контрольных процедур):

Итоговая оценка эффективности контрольной процедуры	Коэффициент эффективности контрольной процедуры
---	---

1	Неэффективная контрольная процедура (контрольная процедура отсутствует)	1
2	Неэффективная контрольная процедура (существенные недостатки)	0,7
3	Эффективная контрольная процедура (несущественные недостатки)	0,4
4	Эффективная контрольная процедура	0,1

Оценка итогового **Уровня статочного риска** определяется как произведение Уровня операционного риска на Коэффициент эффективности контрольной процедуры.

10.1.3.3.2 **Сценарный анализ** проводится по следующей процедуре.

На первом этапе проводится этап выявления угроз, на котором определяется перечень угроз, способных привести к реализации данного операционного риска.

На втором этапе происходит стоимостная оценка влияния реализации каждой угрозы и оценка общего уровня остаточного риска с учетом и без учета реализации мероприятий по снижению риска.

Оценка реализации выявленной угрозы определяется как произведение объема потерь по реализации операционного риска по верхней границе диапазона потерь из самооценки, вероятности реализации операционного риска из самооценки, а также вероятности реализации угрозы. Вероятность реализации угрозы определяется отдельным параметром в соответствии со следующей шкалой:

Коэффициент вероятности	Качественная оценка вероятности
0,9	Очень высокая
0,8	Высокая
0,6	Выше средней
0,5	Средняя
0,4	Низкая
0,2	Маловероятная

При разработке мероприятий по снижению риска оценивается их эффективность с использованием следующей шкалы оценок:

Коэффициент эффективности	Оценка эффективности	Описание
0,9	Высокая	Мероприятие практически полностью снизит негативное влияние операционного риска.
0,7	Выше средней	Мероприятие значительно ограничит негативное влияние операционного риска.
0,5	Средняя	Мероприятие частично ограничит негативное влияние операционного риска.
0,3	Ниже средней	Мероприятие несущественно ограничит негативное влияние операционного риска.
0	Низкая	Мероприятие либо не будет исполняться, либо не эффективно.

Итоговая оценка с учетом реализации мероприятий определяется путем взвешивания на величину (1-КЭм), где КЭм – коэффициент эффективности мероприятия.

Итоговая стоимостная оценка по сценарному анализу определяется по угрозе, несущей максимальный негативный эффект.

10.1.3.4 Требования к ведению инцидентов операционной надежности

Операционная надежность - способность организации обеспечить непрерывность функционирования критически важных процессов в случае возникновения отказов и (или) нарушений функционирования.

В рамках управления операционной надежностью по инцидентам операционной надежности и технологическим процессам (отдельный объект системы) должны рассчитываться следующие целевые показатели операционной надежности:

- Допустимая доля деградации технологического процесса (отношение фактического и планируемого количества операций, совершенных за время инцидента);
- Допустимое время простоя в рамках одного инцидента (время простоя или деградации в рамках одного инцидента определяется как разница между окончанием и началом инцидента операционной надежности, в минутах);
- Допустимое суммарное время простоя (время простоя или деградации в рамках технологического процесса по всем инцидентам за последние 12 календарных месяцев, в минутах);
- Показатель соблюдения режима работы (количество часов функционирования технологического процесса за отчетный квартал).

В рамках технологического процесса должны учитываться следующие параметры:

- наименование
- идентификатор
- ответственные подразделения
- вид операций, осуществляемых в рамках технологического процесса
- режим работы (периоды проведения операций в рамках технологического процесса)
- целевые показатели операционной надежности
- связанные бизнес-процессы
- связанные с технологическим процессом объекты информационной инфраструктуры (в разрезе видов: автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование) с указанием субъектов доступа к ним
- технологические участки

Целевые показатели операционной надежности в рамках инцидентов и технологических процессов должны рассчитываться автоматически на основе данных базы инцидентов операционной надежности.

10.1.3.5 Требования к аналитике и отчетности

В рамках аналитических возможностей обработки данных система должна позволять формировать выборку данных на основе объектной модели данных системы, в том числе с учетом выбора набора данных по объекту, а также с учетом установки фильтра на параметры объекта, на основе которых формируются данные.

В рамках формализованных отчетов необходимо формирование отчета с учетом следующей аналитики по следующим форматам данных:

- 10.1.3.5.1 Отчёт о сумме потерь / количестве СОР по Банку в целом, по подразделениям Банка, а также по типам событий операционного риска, направлениям деятельности, в том числе в разрезе составляющих их процессов, и видам операционного риска ;
- 10.1.3.5.2 Отчет о сумме потерь для расчета экономического капитала;
- 10.1.3.5.3 Отчет о СОР, зарегистрированных в Системе за предыдущий рабочий день;
- 10.1.3.5.4 Ежемесячный отчет по величине валовых потерь;
- 10.1.3.5.5 Ежеквартальный отчет о сумме потерь / количестве СОР в разрезе элементов классификации событий операционного риска;
- 10.1.3.5.6 Отчет, формируемый для расчета контрольных показателей уровня операционного риска (КПУОР);
- 10.1.3.5.7 Отчет по управлению операционным риском в кредитной организации:
- 13.1. Отчёт о прямых потерях/возмещениях от реализации событий операционного риска в разрезе типов событий операционного риска и источников операционного риска;
- 13.2. Отчёт о количестве событий операционного риска/прямых потерях в разрезе типов событий операционного риска и групп по диапазону потерь;
- 13.3. Отчёт о чистых (фактических) прямых потерях;
- 13.4. Отчёт о прямых потерях;

- 13.5. Отчёт о возмещениях по прямым потерям;
- 13.6. Отчёт о непрямых потерях;
- 13.7. Отчёт о прямых потерях от реализации риска информационной безопасности, связанных с нарушением защиты информации;
- 13.8. Отчёт о значениях контрольных показателей уровня операционного риска и риска информационной безопасности в разрезе направлений деятельности.
- 10.1.3.5.8 Отчеты в рамках количественной оценки уровня операционного риска:
- отчет о сумме потерь / количестве СОР по Банку в целом, по подразделениям Банка, а также по типам событий операционного риска, направлениям деятельности, в том числе в разрезе составляющих их процессов, и видам операционного риска;
 - Отчет о сумме потерь для расчета экономического капитала.
- 10.1.3.5.9 Отчет, формируемый на регулярной основе (ежедневно) – отчет о СОР, зарегистрированных в Системе за предыдущий рабочий день. Данный отчет в автоматическом режиме должен направляться на корпоративную электронную почту по рассылке.
- 10.1.3.5.10 Отчет, формируемый на регулярной основе (ежемесячно), включающий:
- величину валовых потерь от реализации СОР со статусом "оценка потерь от реализации события операционного риска не завершена" начиная от даты регистрации СОР в Системе и от начала календарного года (в случае, если событие операционного риска реализовалось ранее текущего календарного года) нарастающим итогом;
 - величину валовых потерь Банка, в которые включаются потери от реализации СОР, статус которых был переведен в статус "оценка потерь от реализации события операционного риска завершена", в течение отчетного месяца.
- 10.1.3.5.11 Отчет, формируемый на регулярной основе (ежеквартально) - отчет о сумме потерь / количестве СОР в разрезе элементов классификации событий операционного риска, предусмотренных АБД, в том числе следующие показатели:
- общее количество событий операционного риска - количество всех СОР, которые были зафиксированы в Системе с начала года до отчетной даты и в отчетном периоде;
 - количество СОР в разрезе прямых и косвенных потерь с начала года до отчетной даты и в отчетном периоде;
 - количество СОР в разрезе потерь с начала года до отчетной даты и в отчетном периоде;
 - сумма прямых и сумма косвенных потерь от реализации СОР в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска с начала года до отчетной даты и в отчетном периоде;
 - сумма потенциальных потерь от реализации СОР в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска с начала года до отчетной даты и в отчетном периоде;
 - сумма прямых и сумма косвенных потерь, отнесенных к потерям «Расходы на устранение последствий реализации события операционного риска, направленные на восстановление деятельности или на снижение потерь от реализовавшегося события операционного риска» и «Прочие потери, связанные с устранением последствий или снижением потерь от реализации операционного риска», в части потерь на восстановление деятельности, в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска за отчетный период нарастающим итогом;
 - сумма прямых потерь от регуляторного риска, связанных с реализацией операционного риска и включаемых в состав валовых потерь от реализации СОР;
 - максимальная величина прямых и максимальная величина косвенных потерь от реализации одного СОР с наибольшими потерями из тех СОР, которые были зафиксированы в Системе, в разрезе направлений деятельности, в том числе в

разрезе составляющих их процессов, с начала года до отчетной даты и в отчетном периоде;

- максимальная величина потерь, отнесенных к потерям «Потери (в том числе хищение) средств клиентов, контрагентов, работников и третьих лиц, которые не были компенсированы Банком, включая потери средств физических лиц, в том числе индивидуальных предпринимателей, юридических лиц, штрафы, наложенные на должностных лиц кредитной организации», от одного СОР с наибольшими потерями из тех СОР, которые были зафиксированы в Системе, в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, с начала года до отчетной даты и в отчетном периоде;
- сумма прямых и сумма косвенных потерь от реализации пяти крупнейших (по сумме потерь) СОР из тех событий операционного риска, которые были зафиксированы в Системе, в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, с начала года до отчетной даты и в отчетном периоде;
- сумма потерь, отнесенных к потерям «Потери (в том числе хищение) средств клиентов, контрагентов, работников и третьих лиц, которые не были компенсированы Банком, включая потери средств физических лиц, в том числе индивидуальных предпринимателей, юридических лиц, штрафы, наложенные на должностных лиц кредитной организации», от реализации пяти крупнейших (по сумме потерь) СОР из тех СОР, которые были зафиксированы в АБД, в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, с начала года до отчетной даты и в отчетном периоде;
- сумма возмещений по потерям за счет не связанных с Банком лиц, которые были отражены на балансовых счетах Банка, в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов СОР с начала года до отчетной даты и в отчетном периоде;
- сумма возмещений по потерям за счет связанных с Банком юридических и физических лиц в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов СОР с начала года до отчетной даты и в отчетном периоде;
- сумма чистых (фактических) потерь, которая была отражена на балансовых счетах Банка с начала года до отчетной даты и в отчетном периоде;
- средняя величина прямых и средняя величина косвенных потерь от реализации одного СОР в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов СОР за отчетный период;
- среднеквадратичное отклонение (сигма) величины прямых потерь по группам СОР в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов СОР за год;
- распределение потерь от реализации СОР по группам

10.1.3.5.12 Отчет, формируемый для расчета контрольных показателей уровня операционного риска (КПУОР), включая распределение по направлениям деятельности, в том числе в разрезе составляющих их процессов, подразделениям, видам операционного риска (риск информационной безопасности, риск информационных систем, операционный риск в целом), по следующим элементам:

- общая сумма валовых прямых потерь, понесенных Банком от реализации СОР за вычетом потерь от реализации событий риска информационной безопасности за определенный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года;
- общая сумма чистых (фактических) прямых потерь (включая чистые (фактические) прямые потери от реализации событий риска информационной безопасности), понесенных Банком за год;
- общая сумма валовых прямых потерь от реализации СОР за вычетом потерь от реализации событий риска информационной безопасности, понесенных Банком за год;

- сумма чистых (фактических) прямых потерь от реализации СОР, понесенных Банком за год, за вычетом потерь от реализации событий риска информационной безопасности;
- количество всех зарегистрированным в Системе с валовыми прямыми потерями (за исключением потерь от реализации кредитного риска), превышающими порог регистрации (за исключением потерь от кредитного риска), за годовой период;
- общая сумма валовых прямых потерь от реализации всех СОР, зарегистрированных в Системе с прямыми потерями (за исключением потерь от реализации событий кредитного риска, связанных с реализацией операционного риска), превышающими порог регистрации, за годовой период;
- общая сумма валовых прямых и косвенных потерь от реализации СОР, определяемых расчетным образом, за вычетом потерь от реализации событий риска информационной безопасности, за определенный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года;
- общая сумма валовых прямых потерь от реализации событий риска информационной безопасности за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;
- общая сумма валовых прямых потерь от реализации событий риска информационной безопасности, связанных с переводами денежных средств и платежами в платежных системах, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;
- общая сумма чистых (фактических) прямых потерь от реализации событий риска информационной безопасности, понесенных Банком за отчетный период (первый квартал, полугодие, девять месяцев, год);
- сумма валовых прямых потерь, понесенных Банком при выполнении функций участника платежной системы Центрального банка Узбекистана, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;
- сумма валовых прямых потерь от реализации событий риска информационной безопасности, связанных с переводами денежных средств и платежами в платежных системах, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;
- сумма денежных средств, по которой получены уведомления клиентов о несанкционированном переводе (списании) денежных средств, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;
- количество реализованных, то есть не предотвращенных системой информационной безопасности Банка, событий риска информационной безопасности с ненулевой величиной валовых прямых потерь;
- общее количество всех событий риска информационной безопасности, зарегистрированных в Системе, с ненулевой величиной валовых прямых потерь в течение отчетного периода (первого квартала, полугодия, девяти месяцев, года);
- общая сумма валовых прямых и косвенных потерь от реализации событий риска информационной безопасности за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;
- сумма чистых (фактических) прямых и косвенных потерь от событий риска информационной безопасности;
- сумма валовых прямых и косвенных потерь, понесенных Банком при выполнении Банком функций оператора других платежных систем или оператора услуг платежной инфраструктуры, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;
- общая сумма валовых прямых и косвенных потерь Банка в результате использования электронных средств платежа клиентов Банка без их согласия за отчетный период

(первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;

- Общая сумма валовых прямых и косвенных потерь Банка в результате переводов и снятия денежных средств, связанных с несанкционированным доступом к объектам информационной инфраструктуры Банка, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года.

10.1.3.5.13 Отчет, формируемый в соответствии с разрабатываемыми Центральным банком Узбекистана требованиями (после внесения изменений в нормативные документы Центрального банка Узбекистана). Текущая версия проекта отчета с порядком его заполнения.

10.1.3.5.14 Отчет, формируемый для расчета показателя КВП.

Сформированные отчеты должны быть доступны для экспорта/сохранения в основных стандартных форматах (xls, csv, pdf).

10.1.3.5.15 Прогнозирование ожидаемых потерь по операционному риску:

Прогнозирование ожидаемых потерь должно проводиться с помощью показателя VAR (Value at Risk) методом исторического моделирования.

Основные этапы оценки VAR:

- расчет среднемесячного значения потерь на основе данных базы событий за 3-5 лет (математическое ожидание);
- расчет волатильности потерь по формуле стандартного отклонения, измеряющего степень разброса значений случайной величины относительного ожидаемого значения;
- выбор уровня доверительного интервала: 95%; 99%; 99,9%;
- расчет обратного нормального распределения (квантиля) для заданной вероятности (доверительного интервала);
- расчет величины возможных потерь (VaR) на временном горизонте 12 месяцев;

10.1.3.5.16 Ежеквартальный отчет по управлению операционным риском

13.9. Раздел 1. Отчет о событиях операционного риска и связанных с ними прямых потерях, и возмещениях

13.9.1. Подраздел 1.1. Отчет о прямых потерях и возмещениях от реализации событий операционного риска в разрезе источников операционного риска и типов событий операционного риска

Источник операционного риска	Тип события	Период	Сумма валовых прямых потерь, тыс. сум	Сумма чистых прямых потерь, тыс. сум	Максимальная величина прямых потерь от одного события, тыс. сум		Сумма валовых прямых потерь от пяти крупнейших событий, тыс. сум	Сумма возмещений по прямым потерям, тыс. сум		Сумма потерь (в том числе хищений) средств клиентов, контрагентов, работников кредитной организации и других третьих лиц, компенсированных кредитной организацией, тыс. сум	Максимальная величина потерь (в том числе хищений) средств клиентов, контрагентов, работников кредитной организации и других третьих лиц от одного события, компенсированных кредитной организацией
					до учета возмещений	после учета возмещений		возмещения, принятые к зачету	возмещения, не принятые к зачету		

											й, тыс. сум
1	2	3	4	5	6	7	8	9	10	11	12

13.9.2. Подраздел 1.2. Отчет о количестве событий операционного риска и валовых прямых потерях в разрезе диапазонов потерь и типов событий операционного риска

Диапазон потерь	Тип события	Период	Количество событий операционного риска с валовыми прямыми потерями, единиц	Сумма валовых прямых потерь, тыс. сум
1	2	3	4	5

13.10. Раздел 2. Отчет о потерях и возмещениях от реализации операционного риска (за исключением риска информационной безопасности) и риска информационной безопасности в разрезе направлений деятельности и типов событий операционного риска по видам потерь и возмещений

13.10.1. Подраздел 2.1. Отчет о чистых прямых потерях

Направление деятельности	Тип события	Период	Сумма чистых прямых потерь, тыс. сум		Среднеквадратичное отклонение (сигма) величины чистых прямых потерь, тыс. сум		Средняя величина чистых прямых потерь, тыс. сум	
			от операционного риска (за исключением риска информационной безопасности)	от риска информационной безопасности	от операционного риска (за исключением риска информационной безопасности)	от риска информационной безопасности	от операционного риска (за исключением риска информационной безопасности)	от риска информационной безопасности
1	2	3	4	5	6	7	8	9

13.10.2. Подраздел 2.2. Отчет о валовых прямых потерях

Направление деятельности	Тип события	Период	Вид прямых потерь	Сумма валовых прямых потерь, тыс. сум		Среднеквадратичное отклонение (сигма) величины валовых прямых потерь, тыс. сум		Средняя величина валовых прямых потерь, тыс. сум	
				от операционного риска (за исключением риска информационной безопасности)	от риска информационной безопасности	от операционного риска (за исключением риска информационной безопасности)	от риска информационной безопасности	от операционного риска (за исключением риска информационной безопасности)	от риска информационной безопасности

				ной безопасности)	аснос ти	ной безопасности)	сности	нной безопасности)	ности
1	2	3	4	5	6	7	8	9	10

13.10.3. Подраздел 2.3. Отчет о возмещениях по прямым потерям

Направл ение деятельн ости	Тип событ ия	Перио д	Вид возмеще ния по прямым потерям	Сумма возмещения по прямым потерям, тыс. сум		Средняя величина возмещения по прямым потерям, тыс. сум	
				от операционного риска (за исключением риска информационно й безопасности)	от риска информ ационно й безопас ности	от операционного риска (за исключением риска информационно й безопасности)	от риска информа ционной безопасн ости
1	2	3	4	5	6	7	8

13.10.4. Подраздел 2.4. Отчет о непрямых потерях

Напр авле ние деят ельно сти	Тип собы тия	Пе рио д	Вид непр ямых поте рь	Сумма не прямых потерь, тыс. сум		Среднеквадратичное отклонение (сигма) величины не прямых потерь, тыс. сум		Средняя величина не прямых потерь, тыс. сум	
				от операционно го риска (за исключением риска информацион ной безопасности)	от риска инфор мацио нной безоп аснос ти	от операционно го риска (за исключением риска информацион ной безопасности)	от риска инфор мацио нной безопа сности	от операционно го риска (за исключением риска информацион ной безопасности)	от риска инфор мацион ной безопас ности
1	2	3	4	5	6	7	8	9	10

13.10.5. Подраздел 2.5. Отчет о прямых потерях от реализации событий риска информационной безопасности, связанных с нарушением защиты информации

Напр авле ние деят ельн ости	Тип собы тия	Пери од	Вид события риска информацио нной безопасности , связанного	Валовые прямые потери от реализации событий риска информационной безопасности, связанных с нарушением защиты информации, тыс. сум	Чистые прямые потери от реализации событий риска информационной безопасности, связанных с нарушением защиты информации, тыс. сум
---	--------------------	------------	--	--	---

			с нарушением защиты информации	сумм а	среднеквадрат ичное отклонение (сигма)	средня я величи на	сумм а	среднеквадр атичное отклонение (сигма)	средня я величи на
1	2	3	4	5	6	7	8	9	10

13.11. Раздел 3. Отчет о значениях контрольных показателей уровня операционного риска и риска информационной безопасности в разрезе направлений деятельности или по кредитной организации в целом

Направ ление деятель ности	Контрольный показатель уровня операционного риска (риска информационной безопасности)	Фактическое значение показателя на отчетную дату		Целевые значения показателей			
				сигнальное значение		контрольное значение	
		тыс. сум	в процентах	тыс. сум	в процентах	тыс. сум	в процентах
1	2	3	4	5	6	7	8

10.1.3.5.17 Расчет величины капитала на покрытие операционного риска по Базель 3
Расчет величины капитала на покрытие операционного риска (operational risk capital, ORC) должен соответствовать требованиям стандартизированного подхода (standardised approach) в рамках Базель 3 (Basel III).

Минимальная величина капитала на покрытие должна определяться как произведение Компонента Бизнес-индикатора (Business Indicator Component, BIC) и коэффициента внутренних потерь (Internal Loss Multiplier, ILM).

ORC = BIC · ILM

Компонента Бизнес-индикатора (BIC) должна рассчитываться путем взвешивания Бизнес-индикатора (BI) на предельные коэффициенты (α_i).

Бизнес-индикатор (BI) должен определяться как сумма: Компоненты процентов, аренды и дивидендов (ILDC); Сервисной компоненты (SC) и Финансовой компоненты (FC).

BI = ILDC + SC + FC

ILDC определяется как сумма средних чистых процентных доходов и расходов и средних дивидендных доходов;

SC определяется как сумма максимальной из величин комиссионных доходов и расходов, а также максимальной из величин операционных доходов и расходов.

FC определяется как сумма усредненной по модулю чистой прибыли (убытка) по финансовым операциям торгового портфеля и усредненной по модулю чистой прибыли (убытка) по финансовым операциям банковского портфеля.

Величина коэффициента внутренних потерь (**ILM**) определяется по формуле:

$$ILM = \ln \left(\exp(1) - 1 + \left(\frac{LC}{BIC} \right)^{0.8} \right)$$

LC – (Loss Component) Компонента потерь, вычисляемая на основе базы событий операционного риска, равная 15-кратным средним ежегодным потерям от реализации операционного риска на основе исторических данных за 10 лет (не менее 5 лет), с учетом индекса инфляции.

10.1.4 Требования к возможностям расширения функциональности

10.1.4.1 Блок «Управление данными»

- Хранилище
- Управление бизнес-объектами из интерфейса системы;
- Управление свойствами полей бизнес-объектов;
- Определение вычисляемых атрибутов на основе SQL-процедур или иных функций;
- Настройка истории изменения для сущности;
- Работа на уровне метаописаний сущности;
- Управление бизнес-объектами внешних систем;

10.1.4.2 Блок «Управление процессами»

- Автоматизация
- Созданий новых функциональных возможностей
- Алгоритмизация обработки, расчетов и проверки данных
- Управления процессами и блоками системы
- Запуск процессов по расписанию;
- Поддержка многомерных процессов;
- Поддержка истории изменений процессов;
- Возможность восстановления работоспособности;
- Мониторинг за ходом выполнения сценария;

10.1.4.3 Блок «Управление сервисами»

- Обмена данными с внешними источниками
- Взаимодействие с внешними системам по протоколам RestAPI, SOAP,
- Инструмент разбора поступивших данных в систему
- Инструмент формирования передачи данных из системы
- Инструмент для работы с файловыми источниками
- Оркестровка внешними системами по событию
- Запуск по заданию без участия пользователя
- Создание песочниц из бизнес-данных для внешнего пользования

10.1.4.4 Блок «Управление событиями»

- Система оповещений
- Уведомления по электронной почте,
- Индикация данных в интерфейсе системе по настраиваемым условиям,
- Оповещение внутри системы по настраиваемым событиям
- Сигналы для внешних систем потребителей

10.1.4.5 Блок «Управление пользовательским интерфейсом»

- Создание интерфейса системы
- Создание пользовательских форм для сотрудника, роли, ситуации
- Логические и бизнес-проверки на корректность ввода данных
- Создание, изменение интерфейсных форм из интерфейса системы;
- Настройка поведения, действий, валидаций и правил на форме;
- Неограниченное количество форм для каждого объекта с индивидуальными настройками, доступами, наборами элементов, валидациями, правилами и действиями на форме;
- Создание, изменение списков бизнес-объектов;
- Группировка списков и настройка стилей отображения данных в списках;
- Неограниченное количество списков для каждого объекта с индивидуальными настройками, предустановленными фильтрами, стилями и доступами

10.1.4.6 Блок «Управление документами»

- Отчеты и документы
- Создание формализованных документов с таблицами, стилями и графикой;
- Построение оперативной и управленческой отчетности;
- Представление документов в общеизвестных форматах *.PDF, *.DOC, *.XLS

- Передача документов в письмах по заданию без участия пользователя

10.1.4.7 Блок «Управление ролями и доступами»

- Ролевая модель
- Определение прав доступа на уровне бизнес-объектов
- Определение прав доступа на уровне полей бизнес-объекта
- Определения прав доступа на уровне сервисов
- Определения прав доступа на уровне документов
- Выделение комбинируемых и самодостаточных ролей

10.1.4.8 Блок «Управление безопасностью»

- Аудит действий пользователей
- Накопление истории изменения бизнес-объектов
- Мониторинг процессов системы
- Мониторинг сервисов с внешними системами

10.1.5 Требования к информационной безопасности Системы

Компоненты Системы должны поддерживать защиту каналов передачи данных (SSL/TLS) между клиентским приложением и сервером, а также между сервером и СУБД.

Для Системы должны поставляться регулярные обновления, включающие, в том числе, обновления безопасности при наличии выявленных уязвимостей с возможностью установки без доступа к сети Интернет;

Для обеспечения защиты информации от несанкционированного доступа, доступ в Систему должен предоставляться только авторизованным Пользователям с учетом их полномочий. Пользователю доступны его объекты проверки (направления деятельности), к которым он допущен. Необходимо предусмотреть блокировку Пользователей в случае обнаружения подозрительной активности;

Система должна интегрироваться с Active Directory в части использования доменных учетных записей пользователей по протоколу LDAP.

В Системе должна быть предусмотрена роль Аудитора системы (Администратор безопасности), имеющая права на чтение (просмотр) всех объектов Системы;

В Системе должны фиксироваться действия, исходя из их функциональности и функциональности, связанной с реализацией модели угроз (включая процессы управления пользователями, изменения параметров и системных настроек, влияющих на работоспособность и безопасность системы, а также действия пользователей), и изменения (в формате было - стало), производимые указанными действиями с возможностью однозначного определения их авторства; В Системе должен быть реализован недоступный для редактирования администратором и пользователями интерфейс протоколирования/журналирования (аудита) действий и протоколирования/журналирования (аудита) изменений объектов и прав с возможностью его настройки;

Детализированные требования перечислены в таблице 1 «Требования к информационной безопасности».

Таблица 1 «Требования к информационной безопасности»

№ п/п	Требование
1.	Система должна обеспечить централизованное протоколирование/журналирование всех действий пользователей и администраторов в журналах аудита с возможностью построения отчетов (поиска, фильтрации, формирования отчетов) с помощью средства просмотра журналов аудита (логов). Исключить возможность редактирования журналов аудита пользователями и прикладными администраторами.
2.	Система должна иметь возможность записи в лог файл данных о работе сервера/сервиса приложения.
3.	В Системе должна быть реализована роль аудитора, позволяющая осуществлять просмотр изменений, проводимых с учетной записью Пользователя/администратора системы.

№ п/п	Требование
4.	Блокировка Пользователей должна осуществляться путем перевода их в статус заблокированных без возможности совершения операций под их именами и с возможностью отмены этого статуса.
5.	Система должна предоставлять гибкие возможности разграничения прав доступа Пользователей к данным и функциям Системы в зависимости от подразделения Пользователя, атрибутов объектов и других формальных признаков.
6.	Пользователи, не обладающие бизнес-ролями, не должны иметь доступ и возможность корректировать данные Системы, получать прямой доступ в базу данных Системы в обход подсистемы администрирования.
7.	Должны быть обеспечены возможность определения авторства каждой операции в Системе и отсутствие неавторизованных операций на основе уникальных персонифицированных идентификаторов каждого Пользователя, процедуры аутентификации и протоколирования действий Пользователей в журналах аудита.
8.	Перехваченная передаваемая по каналу связи аутентифицирующая информация не должна позволять осуществлять вход в Систему через прикладную систему. Аутентификационная информация не должна передаваться и храниться в открытом виде.
9.	В Системе должен быть реализован инструментарий управления правами доступа Пользователей, обеспечивающий возможность определения прав на просмотр/изменение любых атрибутов объектов Системы, а также доступа на выполнение действий над объектами Системы, удовлетворяющим требуемым условиям.
10.	Средства протоколирования/аудита должны иметь возможность отслеживать события следующих классов: – начало и окончание работы Системы и ее составных программно-технологических компонент, сеансов, точки входа/вызова; – использование механизмов идентификации и аутентификации; – создание, модификация, удаление объектов; – действий Пользователей и программных процессов; – изменения: политики безопасности, настроек Системы, модуля и его компонент, политики аудита; – управление Пользователями (изменение списка Пользователей, модификация прав доступа и привилегий).
11.	Реализация механизма аудита должна удовлетворять следующим требованиям: – информация в журналах должна представляться в структурированном виде в терминах предметной области; – при протоколировании событий в журналах должно фиксироваться время прикладного сервера.
12.	Должно производиться логирование 5 контрольных точек (ERROR, WARN, INFO, DEBUG, TRACE).

10.1.6 Обновления и патчи выпускаемые для прикладного программного обеспечения использованной в системе АСУОР, не предусматривающие доработки и добавления новых функциональных возможностей предоставляются Лицензиатом на бесплатной основе. Требования к журналированию и логированию

10.1.6.1 Журналирование данных

- Логирование исполняемых сценариев системы
- Ведение истории изменений объектов системы
 - Система должна позволять вести историю изменения объектов Системы
 - Функционал ведения истории изменений объектов является настраиваемым по атрибутно.

10.1.6.2 Логирование данных

Система позволяет отслеживать следующие типы событий:

- Логирование всех взаимодействий клиента с сервером
- Логирование команд обращений к базе данных
- Логирование размера сообщений между клиентом и сервером и времени обработки
- Логирование взаимодействия с внешними системами

10.1.6.3 Виды проверок

10.1.6.3.1 Описание настроек

- EventsLevel
 - Off – логирование события отключено;
 - Critical – фиксировать только критические события;
 - Error – фиксировать ошибки и критические ошибки;
 - Warning – фиксировать предупреждения, ошибки и критические ошибки;
 - Information – фиксировать информационные сообщения, предупреждения, ошибки и критические ошибки;
 - Verbose – фиксировать все сообщения.
 - Activity tracing – активировать логирование события.
- Processingalgorithm
 - Sync – работа логирования в синхронном режиме;
 - Async – работа логирования в асинхронном режиме.
- ProfileName - какие настройки конфигурирования используются
- WritersData
 - DB – логирование пишется в базу данных;
 - File – логирование пишется в файл;
 - Direct – все события по факту появления сразу пишутся в базу данных;
 - Queued – события пишутся в базу данных по мере наполнения очереди.

10.1.6.3.2 Локальные логи

Если в Системе предусмотрен толстый клиент для администрирования решения, то должна быть возможность ведения локальных логов. Локальные логи должны быть отключаемы и по умолчанию выключены.

- Отладочные сообщения
- Исключение (Exception) в коде (общее место для ошибок).
- Результат объединения апартаментов (кол-во и время).
- Трассировочное сообщение холдера кешированных данных.
- Исключение (Exception) при обработке процесса.
- Статистика выполнения процесса (время выполнения, уровень сообщения определяется временем выполнения).
- Статистика выполнения процесса (время выполнения в CPU, уровень сообщения определяется временем выполнения в CPU).
- Трассировка работы менеджера процессов.
- Продолжительность запроса.
- Размер запроса.
- Трассировочное сообщение модуля отчетов.
- Трассировочное сообщение.
- Статистика выполнения sql-команды (время выполнения, уровень сообщения определяется временем выполнения).
- Трассировочное сообщение выполнения sql-команды.
- Трассировочное сообщение (общее место для разнообразных сообщений; замена стандартному трассировщику).

10.1.6.3.3 Серверные логи

В системе должны быть предусмотрены серверные логи:

- Отладочные сообщения
- Исключение (Exception) в коде (общее место для ошибок).
- Результат объединения апартаментов (кол-во и время).

- Трассировочное сообщение модуля аудита.
- Трассировочное сообщение процесса аутентификации.
- Трассировочное сообщение холдера кешированных данных.
- Исключение (Exception) при обработке процесса.
- Статистика выполнения процесса (время выполнения, уровень сообщения определяется временем выполнения).
- Статистика выполнения процесса (время выполнения в CPU, уровень сообщения определяется временем выполнения ...)
- Трассировка работы менеджера процессов.
- Продолжительность запроса.
- Размер запроса.
- Трассировочное сообщение модуля отчетов.
- Трассировочное сообщение планировщика задач.
- Трассировочное сообщение.
- Статистика выполнения sql-команды (время выполнения, уровень сообщения определяется временем выполнения).
- Трассировочное сообщение выполнения sql-команды.
- Трассировочное сообщение (общее место для разнообразных сообщений; замена стандартному трассировщику).

10.1.6.3.4 Запись журнала события

В случае записи логируемых событий в базу данных, зафиксированные данные отражаются в журнале событий системы в следующем объеме данных:

- Идентификатор
- Тип события
- Уровень события
- Время события
- UTC время события
- Подтип события
- Имя приложения
- Серверное событие
- Пользователь
- Головной процесс
- Текущий процесс
- Длительность события (CPU)
- Длительность события (миллисекунд)
- Сообщение
- Стек вызовов
- Полная информация
- Логин пользователя
- Наименование головного процесса
- Наименование текущего процесса
- Идентификатор головного процесса
- Идентификатор текущего процесса

10.1.6.3.5 Событие аудита пользователя

В системе должно быть предусмотрено логирование событий аудита по следующим типам:

Типы событий аудита:

Наименование	Описание
LogIn	Вход пользователя
LogOut	Выход пользователя
OpenForm	Открытие формы

RunFormCommand	Запуск команды формы
OpenList	Открытие списка
SaveObject	Сохранение объекта
GenerateReport	Формирование отчета
RunInterfaceCommand	Запуск команды приложения

Примечание:

Также должна быть возможность просмотреть информацию о дате и времени предыдущей авторизации пользователя для исполнения требования «Оповещение субъекта логического доступа после успешной авторизации о дате и времени его предыдущей авторизации в АС».

Данные приводятся в следующем формате:

- Идентификатор
- Время события
- UTC время события
- Наименование приложения
- Логин пользователя
- Наименование профиля пользователя
- Пользователь
- IP адрес
- IP адрес ТС
- Тип события аудита
- Признак успешного завершения события
- Идентификатор корневого процесса
- Объект процесса
- Дополнительная информация

10.2 Требования к структуре Системы в целом

10.2.1 Требования к информационному обмену и информационной совместимости.

Информационное обеспечение Системы должно быть совместимо с информационным обеспечением взаимодействующих информационных систем по содержанию, системе кодирования, методам адресации, форматам данных и форме представления информации, получаемой и предоставляемой Системой.

10.2.2 Требования к взаимосвязи Системы со смежными системами, обеспечение совместимости

Система должна позволять выстраивать интеграционное взаимодействие с внутренними системами по протоколам RestAPI, SOAP сервисов или dblink.

Система должна иметь встроенный шлюз из коробки для записи любых данных в структуру объектов системы из внешней системы с помощью RestAPI.

11. Требования к выполняемым Работам

11.1 Общие принципы выполнения Работ

При выполнении Работ необходимо руководствоваться следующими принципами:

- **принцип развития.** Исходя из перспектив развития (модификации) Системы, Система должна дорабатываться с учетом возможности пополнения и обновления функций и состава Системы без нарушения ее функционирования;
- **принцип совместимости.** Должны быть реализованы информационные интерфейсы, благодаря которым Система может взаимодействовать с другими информационными системами в соответствии с установленными правилами;
- **принцип стандартизации (унификации).** Должны быть применены типовые, унифицированные и стандартизованные элементы, проектные решения, пакеты прикладных программ, комплексы, компоненты;
- **принцип эффективности.** Должно быть достигнуто соотношение между затратами на модификацию Системы и целевыми эффектами, включая конечные результаты, получаемые в результате автоматизации;
- **принцип относительной независимости подсистем (принцип модульности).** Система должна быть модифицирована как совокупность отдельных максимально независимых функциональных подсистем.

- **принцип открытости.** Система должна быть способна к интеграции, расширению функций уже имеющихся, а также обеспечивать возможность интеграции с внутренними системами. В Системе должны применяться общепринятые стандарты на правила передачи (протоколы, интерфейсы) и хранения информации;
- **принцип санкционированного доступа к информации.** Система обеспечивает санкционированный доступ к информации. Модификация Системы должна учитывать функции администрирования, которые позволяют устанавливать пользователям Системы права доступа к информации.
- **принцип многоуровневости.** Система должна иметь многоуровневую архитектуру:
 - уровень данных – должен обеспечивать информационное взаимодействие с используемой СУБД.
 - уровень функциональной обработки данных – должен обеспечивать обработку данных в соответствии с функциональными требованиями;
 - уровень визуализации обработанных данных – должен обеспечивать отображение обработанных данных для пользователя.
- **принцип подтверждения.** Авторизация действия пользователей – проверка предоставления определенному лицу прав на выполнение определенных действий при попытке их выполнения.
- **принцип масштабируемости.** Система обеспечивает возможность горизонтального и вертикального масштабирования для обеспечения отказоустойчивости и достаточной производительности при следующих изменениях:
 - при увеличении количества пользователей;
 - при росте объемов накопленных данных.

11.2 Общие технические требования к Работам

11.2.1 Требования к составу Работ

Состав Работ, выполняемый Исполнителем, должны включать в себя:

- Методологические консультации по управлению операционными рисками в соответствии с методическими рекомендациями Базель III.
- Передачу прав на использование ГППО, необходимого и достаточного для выполнения Работ, на условиях простой (неисключительной) лицензии.
- Установку, конфигурирование и настройку ГППО.
- Работы по настройке, модификации, адаптации и внедрению функционала Системы, включая:
 - адаптация экранных и печатных форм отчетов и дашбордов;
 - настройка ролевой модели пользователей Системы;
 - установку, конфигурирование и настройку;
 - документирование внедряемых решений и функционала на уровне технической документации по Системе для руководства администраторов, руководства пользователей по каждой подсистеме и/или Системе в целом (должна поддерживаться всегда в актуальном состоянии и обновляться при её доработке (в т. ч. вендором)
 - подготовку выгрузок и средств автоматизации (включая скрипты);
 - реализацию и поддержки интеграции (информационного взаимодействия) Системы с внутренними системами и сервисами Заказчика;
 - проведение консультирования/обучения работников Заказчика.
 - Исполнитель должен обеспечить обучение не менее 20 сотрудников банка в объёме не менее 30 часов по работе с системой АСУОР.
- Устранение ошибок в реализованном функционале Системы.
- Инструктаж Администраторов Системы.
- Инструктаж пользователей Системы.
- Средства разработки должны обеспечивать, в том числе следующее:

- изменение справочников, правил контроля, процедур и функций обработки данных;
- добавление новых объектов, атрибутов объектов, ограничений, увеличение размеров полей данных;
- изменение логики поведения и элементов интерфейса пользователей;
- изменение логики формирования и структуры отчетов;
- разработка новых функциональных блоков, форм, отчетов, процедур, функций Системы;

11.2.2 Требования к применению систем управления базами данных.

При выполнении Работ по данному Техническому заданию в части применения СУБД должно быть обеспечено выполнение следующих требований:

- использование СУБД для долгосрочного хранения данных;
- использование в физической организации данных (при необходимости) методов индексирования различного уровня и кластеризации данных для обеспечения должного уровня производительности;
- физическое проектирование базы данных должно проводиться с учетом оптимизации по критериям повышения реактивности Системы и нормализации данных.

11.2.3 Требования к эргономике и технической эстетике Системы

При выполнении Работ пользовательские интерфейсы Системы должны быть не перегруженными графическими элементами, должно быть обеспечено быстрое отображение экранных форм.

Навигационные элементы должны быть выполнены в удобной для пользователя форме (форма должна способствовать снижению количества шагов для поиска информации, необходимой пользователю). Ввод-вывод данных, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном или автоматическом режимах. Пользовательский интерфейс Системы должен соответствовать современным эргономическим требованиям и обеспечивать интуитивно понятный доступ к требуемым функциям Системы.

Экранные формы должны проектироваться с учетом требований к унификации:

- все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
- для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных и т.д.), а также последовательности действий пользователя при их выполнении, будут унифицированы.
- Система должна контролировать правильность и обязательность заполнения необходимых полей и в случае некорректного заполнения выдавать информационное сообщение на русском языке.

Поля, недоступные для редактирования, и обязательные поля должны иметь соответствующую визуализацию.

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных. Сведения о таких ситуациях должны протоколироваться/журналироваться в подсистеме информационной безопасности.

Недоступные для заполнения в текущем режиме поля в Системе должны блокироваться и подкрашиваться серым цветом.

Каждое поле с признаком обязательности заполнения должно визуально подсвечиваться на экранной форме, что позволит пользователю быстро заполнять обязательные поля.

Поля, в которые вводятся дата и /или время, должны заполняться с использованием электронной формы календаря.

Поля, в которые предусмотрен ввод только цифровых значений, не должны позволять ввести и сохранить буквенные, либо цифробуквенные значения.

При наличии ошибок ввода, в т.ч. при вводе некорректных значений, при попытке сохранить такие данные Система должна вывести пользователю полный список с перечисленными ошибками ввода.

11.2.4 Требования к защите информации от несанкционированного доступа к Системе

При выполнении Работ Исполнитель должен обеспечить выполнение требований действующего законодательства по защите информации, в том числе обеспечении безопасности персональных данных.

11.2.5 Технические требования к защите информации

При разработке программного кода Исполнитель должен применять методы безопасного программирования, включающие:

- ручную и автоматизированную проверку кода на предмет недокументированных возможностей;
- контроль версионности исходного кода;
- устранение выявленных уязвимостей исходного кода Системы.

11.2.6 Требования по стандартизации и унификации

При выполнении Работ должны быть использованы международные и отраслевые справочники и классификаторы.

При выборе применяемых решений преимущество должно отдаваться решениям, основанным на стандартизированных технологиях:

- технологиях, прошедших процедуру стандартизации и утвержденные в качестве стандарта либо рекомендации, признанные международным, федеральным, отраслевым органом по стандартизации;
- технологиях, утвержденных в нормативно-технической документации Заказчика.

В Отчетной документации должны быть использованы унифицированные термины, обозначения и сокращения для описания идентичных понятий, операций и действий пользователей Системы.

12. Требования к составу и срокам выполнения работ.

Выполнение Работ осуществляется поэтапно в таблице указан состав работ, предельное количество чел./ч. необходимых на выполнение Работ, описанных в Техническом задании, а также срок выполнения работ по соответствующему Этапу.

Таблица 2 «Этапы выполнения работ по созданию «Автоматизированной системы управления операционным риском»

№ этапа	Наименование этапов работ	Сроки
Этап 1	Подготовительный этап • Подготовка и подписание пакета договорной документации. • Подготовка дистрибутивов базового модуля для развёртывания на предоставленных мощностях Заказчика. • Передача права пользования на ПО.	2 нед.
Этап 2	Этап обследования и анализа Анализ предоставленных материалов/информации от Банка: • Анализ процесса работы с событиями между подразделениями Заказчика • Анализ предоставленного перечня бизнес-процессов с выделенными подпроцессами,	1 мес.

№ этапа	Наименование этапов работ	Сроки
	соотнесением к направлениям деятельности и указанием владельцев процесса - Анализ существующего реестра операционных рисков в Банке; - Анализ существующей базы событий операционного риска Банка; Подготовка тестового контура системы Заказчика на предоставленных мощностях	
Этап 3	Техническая настройка системы (адаптация под индивидуальные требования Банка) НАСТРОЙКА БАЗЫ СОБЫТИЙ ОПЕРРИСКА Миграция данных по предусмотренной в ГППО - Миграция существующей базы событий операционного риска - Миграция справочника источников риска - Миграция справочника бизнес-процессов - Миграция справочника функциональных подразделений банка - Миграция справочника территориальных единиц банка - Миграция справочника информационных систем - Миграция справочников для классификации событий операционного риска - Миграция справочников для классификации инцидентов операционной надежности - Миграция справочников для классификации потерь - Миграция справочников для классификации возмещений - Миграция мероприятий и справочников для классификации мероприятий Технические настройки - Настройка специализированных подразделений - Настройка владельцев бизнес-процессов - Настройка сценария обработки события операционного риска между подразделениями Банка - Генерация формата сквозного номера при регистрации события операционного риска - Уведомление о создании и/или поступлении события ОР в обработку на электронную почту - Поддержка мультилингвальности решения Интеграционное взаимодействие - Интеграционное взаимодействие с почтовым сервисом	4 мес

№ этапа	Наименование этапов работ	Сроки
	• Интеграционное взаимодействие с AD для авторизации пользователей через доменную учетную запись Дополнительные настройки • Ввод пользователей системы по предоставленному перечню • Назначение ролевой модели для добавленных пользователей • Настройка прав доступа для добавленных пользователей • Настройка почтового сервера для рассылки уведомлений Передача функционала в тестовую эксплуатацию Подготовка руководства пользователя	
Этап 4	Тестирование базового функционала; ввод в опытно-промышленную эксплуатацию ВЕДЕНИЕ БАЗЫ СОБЫТИЙ ОПЕРРИСКА Установка и настройка решения • Установка переданного базового функционала на тестовой среде Заказчика; • Организация подключения пользователей по соответствующим ролям. Обучение пользователей пилотной группы • Согласование состава ключевых пользователей для тестирования ПО • Согласование формата и графика обучения Тестирование решения пилотной группой • Тестирования функционала пилотной группой • Анализ предоставленного перечня замечаний по результатам тестирования • Внесение согласованных изменений и доработок Итог: подписание акта о вводе ПО в ОПЭ	1 мес
Этап 5	Опытно-промышленная эксплуатация ДОПОЛНИТЕЛЬНЫЕ ОПЦИИ ВЕДЕНИЯ БАЗЫ СОБЫТИЙ ОПЕРРИСКА Настройка и доработка функциональных блоков Разовая миграция данных • Миграция существующего реестра операционных рисков Отчетность • Настройка форм управленческой и регуляторной отчетности на основе данных системы • Расчет показателей уровня ОР • Загрузка и настройка КИРов	2 мес

№ этапа	Наименование этапов работ	Сроки
	Интеграционное взаимодействие Интеграционное взаимодействие с АБС Банка для выгрузки информации о бухгалтерских проводках Передача функционала для тестирования перед промышленной эксплуатацией.	
Этап 6	Тестирование и ввод в промышленную эксплуатацию ВЕДЕНИЕ БАЗЫ СОБЫТИЙ ОПЕРРИСКА В СОСТАВЕ ДОРАБОТАННОГО ФУНКЦИОНАЛА Установка и настройка решения - Формирования дистрибутива для подготовки промышленной среды Заказчика; - Подготовка инструкции для установки промышленной среды силами Заказчика. Тестирование решения пилотной группой Итог: подписание акта выполненных работ = ввод ПО в промышленную эксплуатацию	1 мес

13. Порядок контроля и приемки Системы

Организацию и проведение всех видов испытаний осуществляет Заказчик.

Все виды испытаний Системы проходят на объектах Заказчика.

ПСИ представляют собой процесс определения и проверки соответствия характеристик Системы требованиям ТЗ, выявления и устранения недостатков в функционировании Системы.

ПСИ проводятся после установки программного обеспечения модернизированной Системы на аппаратно-программном комплексе Заказчика.

Порядок участия в проведении ПСИ:

- После завершения адаптации Системы, Заказчиком проводятся ПСИ реализованного функционала;
- Исполнитель должен обеспечить работоспособность представленного на испытания функционала, реализованного по Заявке на технических средствах требуемой конфигурации и наличие необходимой документации;
- Сроки проведения ПСИ планируются в соответствии с планом и сроками в Договоре по:
 - реализованному функционалу по требованиям, определенным в ТЗ в соответствии с объемом работ по Договору;
 - устойчивости работы, отсутствия сбоев и отказов Системы при моделировании работы на вычислительной технике и периферийных устройствах Заказчика с использованием объемов информации, соответствующих реальной (промышленной) эксплуатации Системы;
 - корректности работы Системы при ошибочных действиях пользователей, соответствия процесса функционирования Системы процессу, описанному в эксплуатационной документации на Систему;
 - корректности совместного функционирования Системы с другими компонентами и задачами существующих информационных систем Заказчика;

- Все выявленные в процессе испытаний Системы замечания фиксируются в электронной почте и передаются Исполнителю для их устранения в соответствии с условиями Договора.
- Недостатки и ошибки в реализации функционала Системы, выявленные в ходе проведения испытаний, должны быть устранены Исполнителем в рамках выполнения Работ по Договору.
- Акт сдачи-приемки Работ по Заявке направляется Заказчику по итогам устранения выявленных в ходе проведения испытаний недостатков и готовности реализованного функционала по Заявке к опытно-промышленной эксплуатации.
- Исполнитель должен предоставить гарантию на программное обеспечение, настройки и работы, разработанные на основе требований данного Технического задания сроком не менее 12 месяцев с момента ввода сдачи-приёмки.
- Исполнитель должен предоставить техническое сопровождение системы АСУОР сроком в 12 месяцев с момента приём-передачи системы на основе отдельного договора сопровождения с возможностью продления. У исполнителя должна быть система для регистрации заявок и их мониторинга.
- В гарантийный период, исправление ошибок и кодов в системе АСУОР осуществляется исполнителем бесплатно.
- В услуги по Гарантийной поддержке и Технического сопровождения не входят доработки в систему АСУОР, вызванные добавлением новых функций, капитальным изменением процессов, законодательства, требованиями внутренних и внешних регуляторов. Подобные доработки могут быть предоставлены путем отдельного договора и отдельной оценки трудозатрат по соглашению сторон.

14. Требования к документированию

14.1 Требования к содержанию отчетных документов

14.1.1 Документ «Руководство пользователя»

Документ должен содержать полное описание Системы, по освоению и эксплуатации Системы, описание/перечень действий при возникновении проблем в работе системы.

В состав документа «Руководство пользователя» включают:

- аннотацию, в которой приводится краткое изложение документа и его назначение;
- содержание;
- глоссарий;
- главы, описывающие, как использовать систему;
- раздел, описывающий возможные проблемы и пути их решения.

Допускается вводить дополнительные/изменять существующие разделы по согласованию с Заказчиком.

14.1.2 Документ «Руководство администратора».

Документ «Руководство администратора» должен содержать сведения об установке, о проверке, об обеспечении функционирования, настройке системы в определенных условиях ее применения, а также об устранении аварийных ситуаций и основные сведения об эксплуатации (сопровождении) системы.

В содержание документа «Руководство администратора» включают следующие разделы:

- введение;
- общие сведения;
- назначение и порядок применения системы;
- общие принципы и логика работы системы;
- обязательность, регулярность и очередность выполнения операций;
- порядок выполнения операций;
- проблемы в работе системы и способы их решения;
- проверка работоспособности системы;
- порядок обслуживания системы;

- порядок обновления системы;
- порядок работы с журналом системы аудита;
- порядок организации резервного копирования и восстановления системы.

Допускается вводить дополнительные/изменять существующие разделы по согласованию с Заказчиком.

14.1.3 Руководство по установке и настройке решения

- Описание компонент системы
- Подготовка сервера приложений
- Подготовка веб-сервера приложений
- Регистрация сервиса/службы
- Подготовка базы данных
- Базовые настройки, конфигурационные параметры

14.1.4 Руководство по обновлению системы

- Критичные изменения
- Состав обновления
- Описание обновления
- Порядок обновления
- Особенности
- Критичные моменты

14.2 Требования к разработке внутренних нормативных документов (ВНД) по управлению операционным риском и операционной надежности.

В рамках управления операционным риском необходимо разработать следующие ВНД, содержащие основные процедуры управления операционным риском:

14.2.1 Политика управления операционным риском:

- Основные элементы и процедуры системы управления операционным риском.
- Классификация операционных рисков.
- Определение уровня критичности процессов.
- Количественная оценка операционного риска, в том числе требования к капиталу на покрытие потерь от реализации событий операционного риска.
- Определение требований к отчетности по операционным рискам.
- Методика определения и расчета интегрального показателя уровня оценки операционного риска.

14.2.2 Порядок взаимодействия при выявлении событий операционного риска:

- Требования к ведению базы событий операционного риска, в т.ч. структура базы, порог регистрации событий.
- Взаимодействие подразделений при выявлении события операционного риска, обработка события операционного риска.

14.2.3 Порядок определения потерь и возмещений:

- Определение видов и классификация потерь: прямых, не прямых (косвенных, качественных и потенциальных).
- Методика определения и оценки прямых и не прямых потерь, включая методику определения качественных потерь в случаях нарушения операционной устойчивости.
- Порядок выявления расходов, относящихся к операционному риску, из общих расходов Банка.
- Порядок и методы оценки недополученных доходов, связанных с событиями операционного риска.
- Порядок и методы определения стоимости возмещений от событий операционного риска.

14.2.4 Методика качественной оценки операционного риска:

- Процедура самооценки операционного риска.
- Процедура сценарного анализа по операционному риску.

14.2.5 Порядок мониторинга операционного риска:

- Система ключевых индикаторов риска (КИР), способы и методы разработки и контроля КИР.
- Установление контрольных показателей уровня операционного риска (сигнальные и контрольные значения).
- Контрольные процедуры при мониторинге операционного риска.

В части риска информационной безопасности:

14.2.6 Политика информационной безопасности по управлению рисками ИБ:

- Общие положения, термины и определения.
- Процедуры управления риском информационной безопасности.
- Основные принципы функционирования системы обеспечения информационной безопасности и задачи управления риском информационной безопасности.
- Основные принципы организации контроля за функционированием системы обеспечения информационной безопасности.
- Требования к созданию ресурсных (кадровых и финансовых) условий системы обеспечения информационной безопасности.
- Требования к третьим лицам, которым могут быть переданы функции по обеспечению информационной безопасности, а также определение порядка взаимодействия и распределения ответственности между Банком и привлеченными ею третьими лицами.
- Функции и ответственность Коллегиального исполнительного органа и работников Банка в рамках управления риском информационной безопасности.

В части риска информационных систем:

14.2.7 Политика информационных систем (управление рисками информационных систем):

- Общие положения, термины и определения.
- Функции и полномочия лиц и подразделений, ответственных за обеспечение функционирования информационных систем и их компонентов в рамках управления рисками информационных систем.
- Архитектура информационных систем и состав ее элементов.
- Требования к информационным системам в целях управления риском информационных систем.
- Требования к обеспечению качества данных в информационных системах.
- Требования к обеспечению непрерывности и качества функционирования информационных систем.
- Порядок информационного взаимодействия в рамках реализации политики информационных систем.
- Порядок и периодичность формирования отчетов в рамках управления операционным риском информационных систем.

14.2.8 Методика обеспечения качества данных в информационных системах:

- Общие положения, термины и определения.
- Обеспечение качества данных, роли в управлении качеством данных.
- Оценка качества данных и критерии оценки качества данных.
- Методы и алгоритмы расчета, правила измерения показателей качества данных, в том числе с использованием контрольных выборок данных.
- Показатели (индикаторы) качества данных для оценки характеристик качества данных.

14.2.9 Порядок обеспечения качества данных в информационных системах:

- Общие положения, термины и определения.
- Порядок и процедуры обеспечения качества данных.

- Процедуры измерения показателей качества данных, обоснования, утверждения и корректировки предельно допустимых значений показателей качества данных, критериев оценки качества данных.
- Процедуры реагирования на случаи нарушения установленных в Банке предельно допустимых значений показателей (индикаторов) качества данных.
- Процедуры, правила и периодичность контроля качества данных и формирования отчетов о качестве данных, о проведении мероприятий контроля качества данных.
- Процедуры исправления выявленных ошибок в данные и документирования внесенных в них изменений.
- Порядок и периодичность проведения независимой оценки качества данных.
- Порядок взаимодействия органов управления, подразделений и должностных лиц, по вопросам обеспечения качества данных.

В рамках управления операционной надежностью необходимо разработать следующие ВНД, содержащие основные процедуры управления операционной надежностью:

14.2.10 Политика обеспечения операционной надежности:

- Общие положения, термины и определения.
- Общие принципы обеспечения операционной надежности.
- Требования к порядку определения значений целевых показателей операционной надежности и обеспечению контроля за их соблюдением.
- Требования к идентификации и управлению изменениями состава элементов критичной архитектуры.
- Требования к выявлению, регистрации инцидентов операционной надежности и реагированию на них, а также восстановлению выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации указанных инцидентов.
- Требования к взаимодействию с поставщиками услуг в сфере информационных технологий.
- Требования к тестированию операционной надежности технологических процессов.
- Требования к нейтрализации информационных угроз со стороны внутреннего нарушителя.
- Требования к обеспечению осведомленности об актуальных информационных угрозах, которые могут привести к инцидентам операционной надежности.

14.2.11 Порядок обеспечения операционной надежности:

- Общие положения, термины и определения.
- Реализация требований к операционной надежности.
- Требования к системе обеспечения операционной надежности критичной архитектуры, в т.ч. идентификация, классификация и учет; управление изменениями; управление конфигурациями; управление уязвимостями; управление инцидентами операционной надежности (выявление, регистрация, анализ причин, устранение причин, снижение рисков).
- Взаимодействие с поставщиками услуг.
- Тестирование операционной надежности.
- Защита критичной архитектуры при организации удаленной работы.
- Нейтрализация угроз со стороны внутреннего нарушителя.
- Требования к системе организации и управления операционной надежностью.
- Управление информационными системами (классификация информационных систем, режим функционирования, требования к надежности функционирования информационных систем, методика оценки надежности функционирования ИС).
- Порядок ведения реестра учета технологических процессов, технологических участков технологических процессов и соответствующих им объектов критической архитектуры, а также процессов, реализуемых поставщиками услуг в сфере информационных технологий.

15. Техническое сопровождение Системы

Исполнитель на безвозмездной основе должен обеспечить гарантийную поддержку результатов Работ и Системы в течение 360 календарных дней с даты завершения Работ. В рамках гарантийного периода Исполнитель обеспечивает устранение Замечаний согласно срокам и уровню критичности Замечаний.

По истечении гарантийного периода 360 дней с даты завершения Работ, Исполнитель на возмездной основе должен обеспечивать техническую поддержку Системы в рамках услуг по техническому сопровождению составе.

Пакет услуг по техническому сопровождению:

№	Наименование	Объем услуг
1.	Сроки и время оказания услуг	Период: с 08:00 до 17:00 часов (время ташкентское) в режиме 8 (восьми) часового рабочего дня, кроме выходных и праздничных дней, установленных законодательством Республики Узбекистан
2.	Консультация специалистов Заказчика по функциональности ПО, в соответствии со сроком и временем оказания услуг	Консультация первой линии технической поддержки Заказчика (ИТ- Специалистов) не более 5 специалистов. Количество заявок в месяц 10
3.	Исправление Исполнителем ошибок ПО (далее - Замечаний), а также предоставление Заказчику ПО с исправленными ошибками в согласованные сторонами сроки. Стороны договорились, что под Замечанием понимается программная ошибка или недостаток (Дефект), допущенный Исполнителем в ходе разработки и настройки ПО, который может привести к нарушению целостности данных (потеря, искажение данных) или нарушению работоспособного состояния (Отказ) функциональности, отдельной компоненты или всей системы в процессе функционирования.	Количество Заявок в месяц неограничено
4.	Установка пакетов обновлений на тестовую, предпроектную и проектную среду с их тестированием и настройкой конфигурационных параметров системы	Силами первой линии технической поддержки Заказчика (ИТ- Специалистов)

Сроки устранения Замечаний:

Приоритет	Время реакции	Время решения
1 / Критический	2 часа	время обходного решения – 8 календарных часов время решения - 16 часов
2 / Средний	1 рабочий день	3 рабочих дня
3 / Низкий	По согласованию с Заказчиком	По согласованию с Заказчиком

Уровни критичности Замечаний:

Приоритет/ Наименование	Ситуация
1 / Критический	Система полностью не функционирует, Служба сопровождения Заказчика не может решить проблему. Проблема не связана с аппаратным обеспечением Системы. • Для устранения замечания Исполнителем предоставляется временное решение, позволяющее восстановить выполнение бизнес-процессов Заказчика.
2 / Средний	• Неработоспособность большинства компонентов Системы, делающих невозможным использования более половины (50%) функциональности Системы. • Неработоспособность одного или нескольких критических модулей Системы, препятствующие полному выполнению одного из бизнес-процессов Заказчика, автоматизированного Системой. • Имеются ошибки в процессе обработки данных приводящих к остановке бизнес-процессов Заказчика. • Наблюдается ненормальное прекращение функционирования/снижение производительности приложений, решение проблемы отсутствует. • Не приводит к полной остановке Системы.
3 / Низкий	• Неработоспособность менее половины модулей или компонентов Системы, не оказывающего воздействия на основные бизнес-процессы Заказчика, автоматизированные Системой. • Ошибки в процессе обработки данных отсутствуют или имеющиеся ошибки обработки данных не приводят к остановке бизнес-процессов Заказчика. • Консультации по функциональности ПО