САМООЦЕНКА ПО ОПЕРАЦИОННЫМ РИСКАМ

Основные подходы на примере практического опыта Северо-Западного банка ОАО «Сбербанк России»

20 марта 2014 г.

Самооценка

«Если Вам кажется, что у Вас все под контролем,
Вы просто еще не набрали скорость»

Марио Андретти, участник гонок «Формула 1»

- Проведение самооценки позволяет выявить возможности для совершенствования и инноваций, установления приоритетов и разработки планов действий с целью достижения устойчивого успеха;

- Результаты самооценки показывают сильные и слабые стороны, уровень зрелости организации.

План доклада

- Основные цели самооценки;
- Ключевые элементы самооценки и схема взаимодействия;
- Шаблон RSA: профиль риска, KCI, KRI;
- Проведение самооценки в SAS.

Влияние самооценки на показатель экономического капитала

Компоненты, необходимые для расчета экономического капитала

Надзор со стороны руководства банка

Расчет требований к капиталу

Повышение качества контроля

Внутренние данные об инцидентах

Внешние данные об инцидентах

Сценарный анализ

Самооценка и мониторинг индикаторов риска

Роль подразделений Банка

Данные об инцидентах

• Учет инцидентов позволяет выявлять зоны концентрации риска и недостатки в системе контроля

•Качество контроля может быть повышено, что приведет к уменьшению потерь

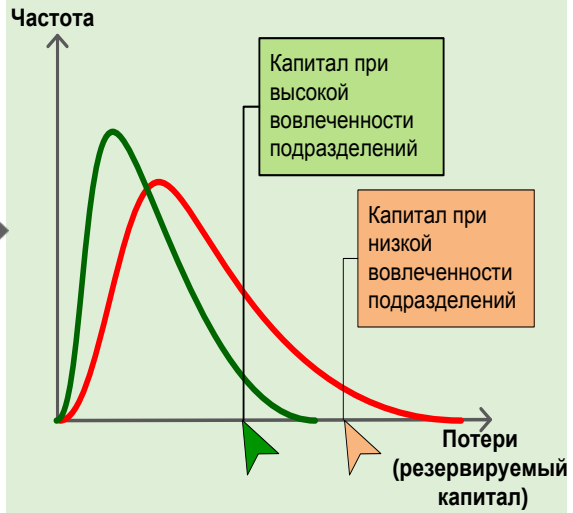
Сценарный анализ, самооценка и мониторинг индикаторов риска

•Процесс самооценки и сценарного анализа позволяет оценить подверженность риску

•Качество самооценки и сценарного анализа может быть учтено для уменьшения требований к капиталу

Влияние на капитал

Высокая вовлеченность в процессы сбора данных, самооценку и сценарный анализ снизит затраты на капитал



Основные цели процесса самооценки RSA (Risk Self-Assessment)

Цели самооценки по рискам (RSA)

- **Выявить основные риски подразделений;**
- **Выполнить количественную оценку для каждого выявленного риска;**
- **Определить и оценить существующие механизмы контроля для каждого выявленного риска;**
- **Определить и оценить существующие индикаторы риска / индикаторы контроля (KRI / KCI) для каждого выявленного риска / механизма контроля;**
- **Предложить и согласовать мероприятия по минимизации рисков.**

Типы событий операционного риска в соответствии с Базель

Типы событий операционного риска

1. Внутреннее мошенничество	2. Внешнее мошенничество	3. Кадровая политика и безопасность труда	4. Клиенты, продукты и деловая практика	5. Ущерб материальным активам	6. Перебои в деятельности и системные сбои	7. Исполнение, оказание услуг и управление процессами
“Несанкционированный выпуск банковских карт; хищение со счетов физических / юридических лиц, компенсационных выплат, военных пенсий”; несанкционированная торговля на финансовых рынках	*“Ограбление банкоматов / ВСП / Кассовых центров; Предоставление кредитов по фиктивным документам; вирусная атака”*	*“Несчастные случаи на рабочем месте; уход ключевых сотрудников, судебные иски со стороны сотрудников / бывших сотрудников банка”*	*“Специалист по работе с клиентами обманным путем продает полисы кредитного страхования”*	*“Ущерб от пожара, наводнения, нанесенный отделению банка”; повреждение автотранспорта в результате ДТП*	*“Сбой ЛВС ЦА; сбой фронтальной системы банкоматов; сбой модуля обработки кредитных заявок”*	*“Кассовые просчеты в результате неверной загрузки кассет в УС; двойные и ошибочные перечисления; неверный расчет процентов по вкладам“*

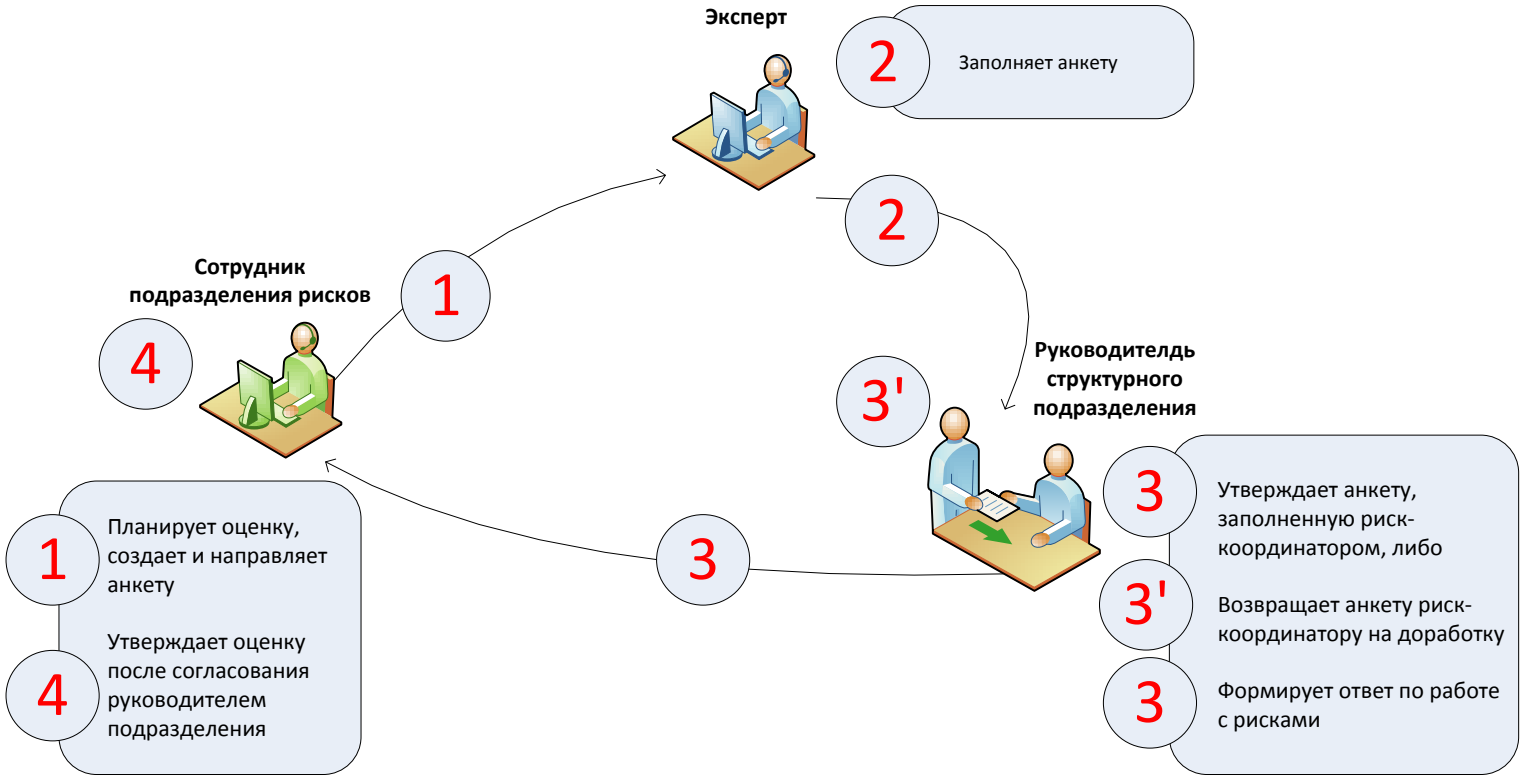
Основные элементы самооценки в ОАО «Сбербанк России»

Основным инструментом для проведения самооценки является разработанный в MS Excel шаблон RSA

Шаблон RSA	• Высокий уровень стандартизации • Всесторонний охват различных разделов и вопросов • Требования к минимальному охвату
Ответственность за RSA	• Уполномоченные сотрудники структурных подразделений • Верификация результатов самооценки осуществляется подразделением рисков Банка
Сроки RSA	• Не позднее 10 числа месяца, следующего за отчетным кварталом • Статус выполнения плана мероприятий по минимизации риска не позднее 5-го рабочего дня каждого месяца

Процесс самооценки по операционным рискам с использованием шаблона RSA

Ежеквартально производится сбор сведений по операционному риску с элементами самооценки от всех структурных подразделений Банка



Роли участников процесса в ходе проведения самооценки

Роль подразделения рисков

- Разработка и ведение методологии, шаблонов и процессов RSA
- Проведение обучения структурных подразделений, задействованных в процессе самооценки
- Проведение верификации данных шаблонов самооценки
- Проведение валидации результатов самооценки для обеспечения их полноты и единообразия
- Подготовка отчетности для руководства Банка,
- Мониторинг планов действий по минимизации риска

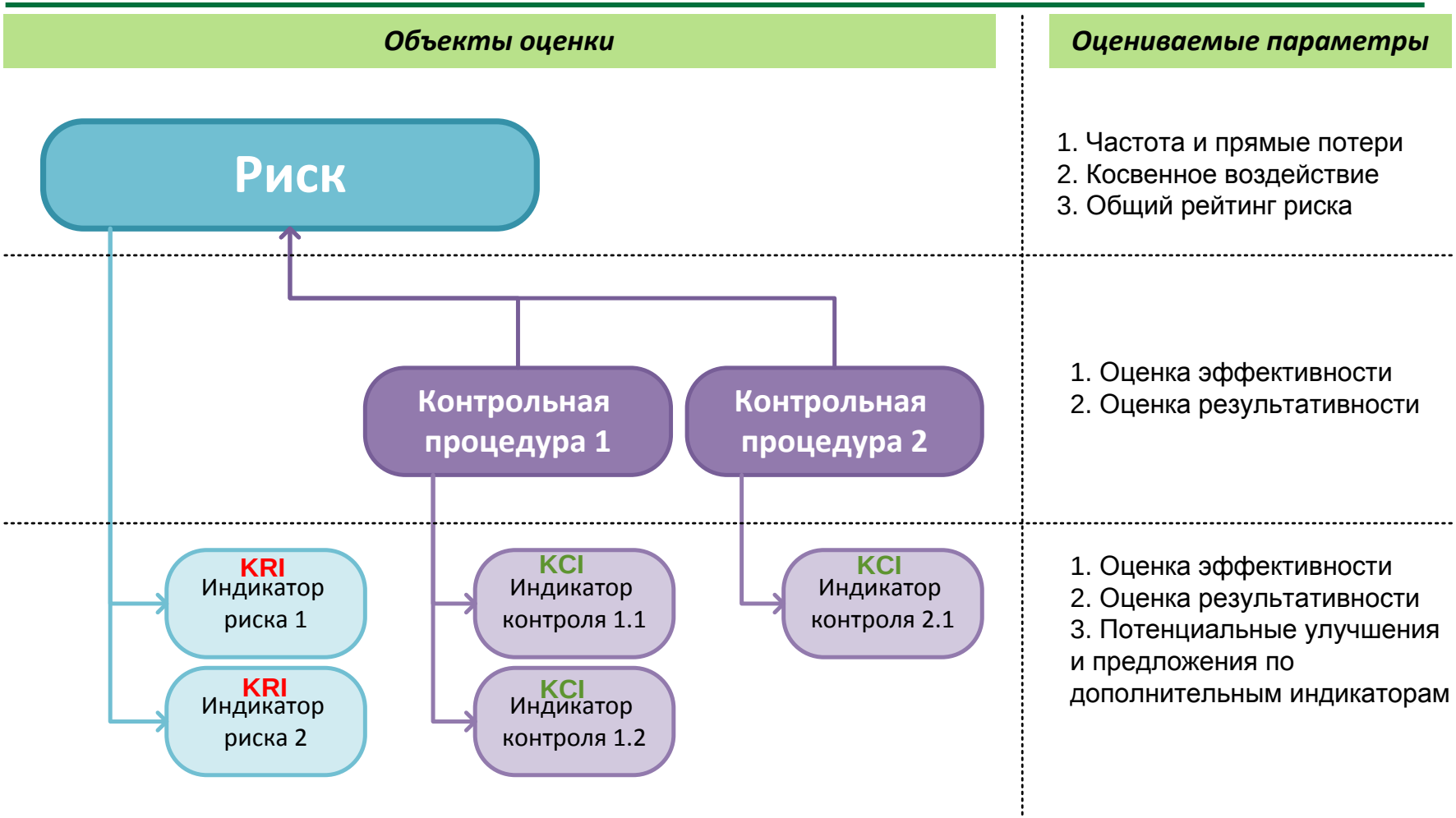
Роль уполномоченного сотрудника структурного подразделения

- **Заполнение шаблонов RSA**
- Определение **планов по минимизации наиболее существенных рисков**
- Предоставление статуса **планов действий** по минимизации рисков на ежемесячной основе

Роль руководителя структурного подразделения

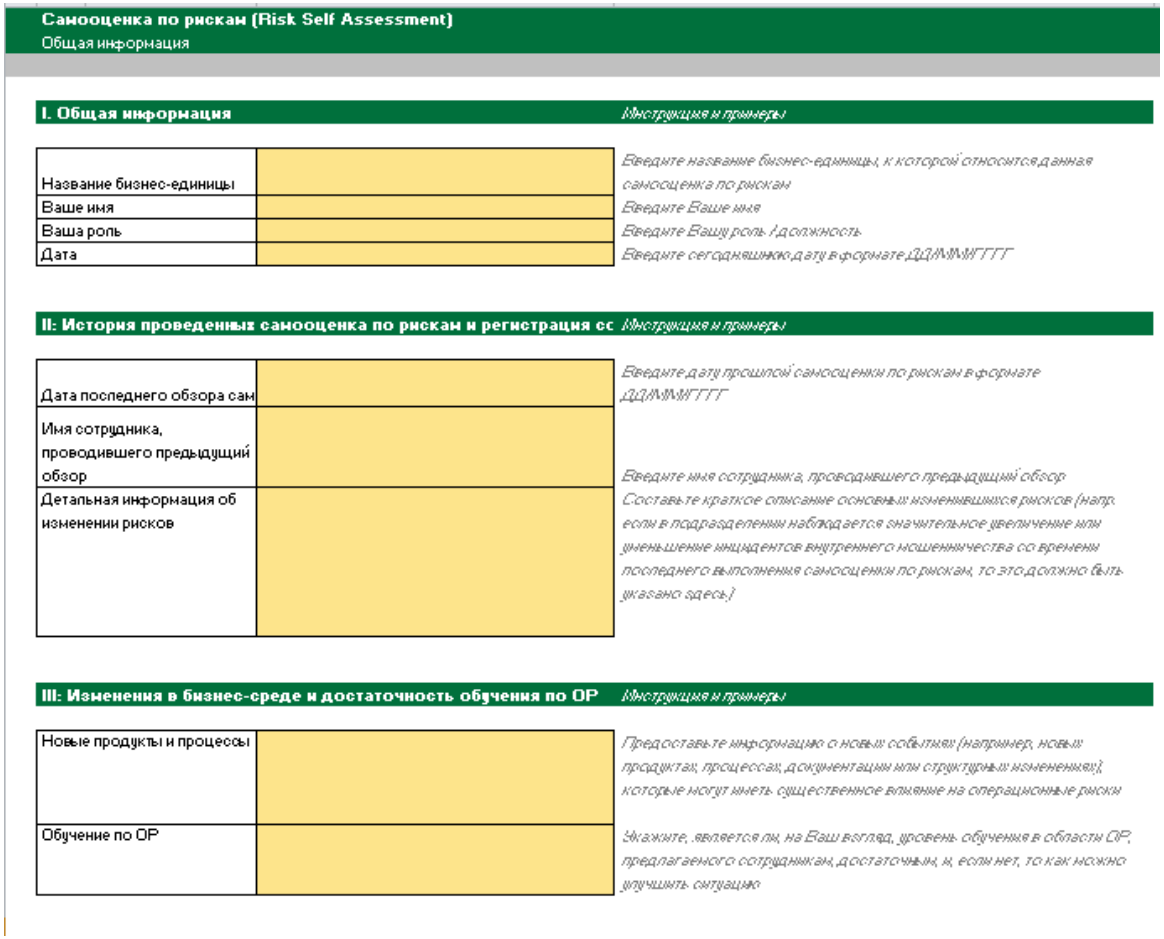
- **Утверждение** результатов самооценки
- **Принятие ответственности** за реализацию выявленных мероприятий по минимизации риска

Ключевые объекты самооценки шаблона RSA



Общая информация шаблона RSA

Общая информация



Самооценка по рискам (Risk Self Assessment)
Общая информация

I. Общая информация — *Инструкция и примеры*

Название бизнес-единицы		*Введите название бизнес-единицы, к которой относится данная самооценка по рискам*
Ваше имя		*Введите Ваше имя*
Ваша роль		*Введите Вашу роль / должность*
Дата		*Введите сегодняшнюю дату в формате ДД/ММ/ГГГГ*

II: История проведенных самооценка по рискам и регистрация со — *Инструкция и примеры*

Дата последнего обзора сам		*Введите дату прошлой самооценки по рискам в формате ДД/ММ/ГГГГ*
Имя сотрудника, проводившего предыдущий обзор		*Введите имя сотрудника, проводившего предыдущий обзор*
Детальная информация об изменении рисков		*Составьте краткое описание основных изменившихся рисков (напр. если в подразделении наблюдается значительное увеличение или уменьшение инцидентов внутреннего мошенничества со времени последнего выполнения самооценки по рискам, то это должно быть указано здесь.)*

III: Изменения в бизнес-среде и достаточность обучения по ОР — *Инструкция и примеры*

Новые продукты и процессы		*Предоставьте информацию о новых событиях (например, новых продуктах, процессах, документации или структурных изменениях), которые могут иметь существенное влияние на операционные риски*
Обучение по ОР		*Укажите, является ли, на Ваш взгляд, уровень обучения в области ОР, предлагаемого сотрудникам, достаточным, и, если нет, то как можно улучшить ситуацию*

- Название подразделения,в котором проводится самооценка, имя и должность сотрудника, проводящего самооценку, а также дата заполнения

- Дата последнего анкетирования по самооценке, имя сотрудника, который провел обзор, а также описание основных изменений в профиле риска подразделения
- К примеру, существенное повышение числа инцидентов, связанных с внутренним мошенничеством, с момента последней самооценки

- Существенные изменения в продуктах, процессах, документации; структурные изменения
- Комментарии, касающиеся обучения по ОР, а также предположения о том, как оно может быть улучшено

Формирование профиля риска

RSA – Идентификация (выявление) рисков

Самооценка по рискам (Risk Self Assessment)
Бизнес-единица: 0
Тип события уровня 1: Внутреннее мошеничество **Тип события уровня 2:** 0

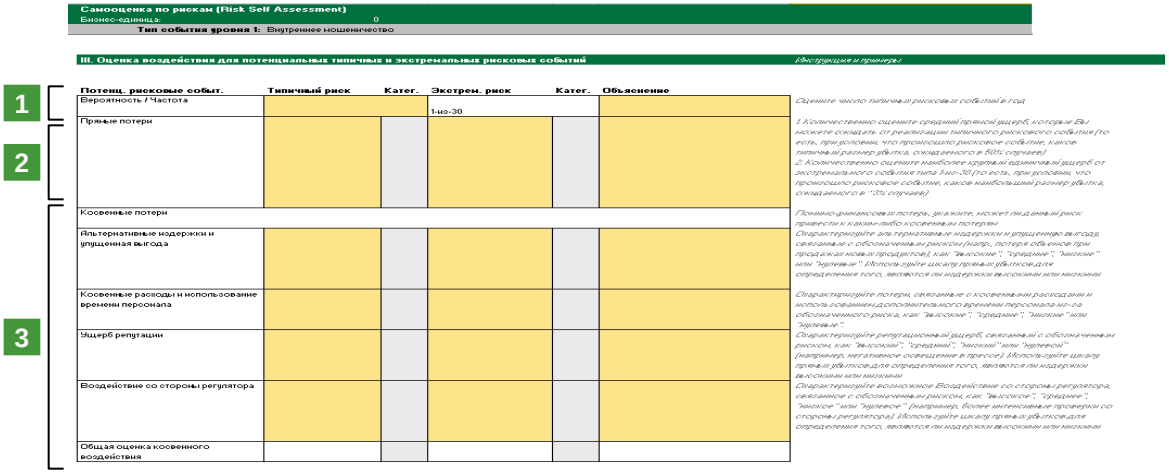
I. Обзор риска		Инструкция и примеры
Название риска		*Кратко опишите риск, например, риск несанкционированного проведения платежа*
Владелец риска		*Укажите основного ответственного за управление данным риском и снижение последствий от него*
Тип риск. события Ур. 1	Внутреннее мошеничество	
Тип риск. события Ур. 2		*Выберите категорию Уровня 2 типа события из выпадающего меню*

II. Описание риска		Инструкция и примеры
Причины		*Опишите причины, которые привели к появлению данного риска*
Событие		*Более подробно опишите оцениваемый риск*
Воздействие		*Качественно опишите прямое и косвенное воздействие от реализации данного риска*
Направления и продукты, на которые оказывает влияние риск		*Укажите направления и продукты, охваченные данным риском (например, IT-системы)*
Процессы, на которые оказывает влияние риск		*Выявите процессы, на которое оказывает влияние данный риск (например, операции с денежной наличностью)*

Уровень 1 по Базель	Уровень 2 по Базель
Внутреннее мошенничество	Несанкционированная деятельность
	Внутреннее хищение и мошенничество
	Нарушения безопасности систем со стороны персонала

Оценка воздействия риска

RSA – Оценка воздействия



Самооценка по рискам (Risk Self Assessment)
Бизнес-единица: 0
Тип события уровня 1: Внутреннее мошенничество

III. Оценка воздействия для потенциальных типичных и экстремальных рисковых событий

	Потенц. рисковые событ.	Типичный риск	Катег.	Экстрем. риск	Катег.	Объяснение
1	Вероятность / Частота			1-из-30		
2	Прямые потери					
	Косвенные потери					
3	Альтернативные издержки и упущенная выгода					
	Косвенные расходы и использование времени персонала					
	Ущерб репутации					
	Воздействие со стороны регулятора					
	Общая оценка косвенного воздействия					

Типичный риск

Пользователь должен:

- оценить, сколько раз за год может возникнуть риск;
- оценить прямые потери - средний прямой ущерб, который можно ожидать от реализации единичного рискового события (то есть, при условии, что произошло рисковое событие, каков размер ущерба, ожидаемого в 50% случаях).

1 Частота

Типичные события

Число событий

2 Прямое воздействие

Оценка	Диапазон	Ущерб
10	> 100 MM RUB	Катастрофический
9	< 100 MM RUB	Критический
8	< 10 MM RUB	Крайне высокий
7	< 5 MM RUB	Высокий
6	< 1 MM RUB	Повышенный
5	< 500,000 RUB	Средний
4	< 300,000 RUB	Умеренный
3	< 100,000 RUB	Сниженный
2	< 10,000 RUB	Низкий
1	< 1,000 RUB	Крайне низкий

3 Косвенное воздействие

Оценка	Косвенное воздействие
4	Высокое
3	Среднее
2	Низкое
1	Нет косвенного воздействия

Ключевые индикаторы риска - KRI

RSA – Выявление и оценка показателей KRI

Самооценка по рискам (Risk Self Assessment)
Бизнес-единица: 0
Тип события уровня 1: Внутреннее мошенничество

IV. Ключевые индикаторы риска (KRI)		*Инструкция и примеры*
Сколько ключевых индикаторов риска (KRI) существует для обозначенного выше риска?	1	*Укажите число ключевых индикаторов риска, используемых для мониторинга изменений, связанных с обозначенным*
Существующий KRI 1	**Оценка**	**Объяснение**
Описание KRI		*Опишите данный индикатор риска. Что именно подвергается мониторингу? К примеру, если риск описывается как "ошибки в торговых операциях", показателем KRI может быть "число транзакций, имевших внутреннюю ошибку", либо "Текучка" (оборачиваемость) персонала в фронт- и бэк-офисе".*
Владелец KRI		*Укажите роль (должность) и имя сотрудника, ответственного за мониторинг KRI*
Источник данных для KRI		*Укажите источник данных для KRI (то есть, человека или информационную систему, ответственную за сбор данных.)*
Частота / периодичность мониторинга		*Укажите, с какой периодичностью происходит мониторинг данного показателя KRI*
Текущая оценка эффективности		*Оцените текущую результативность KRI для оценки обозначенного выше риска*
Потенциальная оценка результативности		*Оцените потенциальную эффективность KRI для оценки обозначенного выше риска и приведите обоснование в том случае, если существуют отличия между потенциальной и фактической результативностью*
Улучшения KRI		
Потенциальные улучшения или дополнительные KRI		*Пожалуйста, предложите меры по совершенствованию существующих ключевых индикаторов риска, либо укажите дополнительные показатели KRI, которые, на Ваш взгляд, помогут более эффективно осуществлять мониторинг обозначенного выше риска и способы их расчета*

Оценка	Эффективность KRI
5	KRI с нулевой эффективностью
4	KRI с ограниченной эффективностью в мониторинге рисковых трендов
3	KRI с достаточной эффективностью в некоторых случаях
2	Эффективный KRI в большинстве случаев, когда могли бы возникнуть риски
1	Эффективный KRI во всех случаях, когда могли бы возникнуть риски

Ключевые индикаторы контроля - KCI

RSA – Выявление и оценка показателей KCI

Сколько ключевых индикаторов контроля (KCI) существует для механизма контроля #2?	3

Выберите число ключевых индикаторов контроля (KCI), имеющихся для обозначенного выше механизма контроля

KCI 1 для мех. контр. 2 Оценка		Объяснение
Описание KCI		
Результативность индикатора контроля		

Опишите показатель KCI (к примеру, если механизм контроля - это "система ввода pin-кода", то KCI может быть "число случаев карточного мошенничества, когда был введен верный pin") Оцените, насколько, на Ваш взгляд, эффективен мониторинг обозначенного выше механизма контроля при помощи данного

Совершенствование показателей KCI	
Потенциальные улучшения или дополнительные KCI	

Пожалуйста, предложите улучшения существующих показателей контроля (KCI), либо дополнительные механизмы контроля, которые помогут осуществлять более эффективный мониторинг обозначенных выше механизмов контроля

Оценка	Эффективность KCI
5	KCI с нулевой эффективностью
4	KCI с ограниченной эффективностью в мониторинге результативности механизмов контроля
3	KCI с достаточной эффективностью в некоторых случаях
2	Эффективный KCI в большинстве случаев, когда применялись механизмы контроля
1	Эффективный KCI во всех случаях, когда применялись механизмы контроля

Обоснование отсутствия риска в подразделении

Обоснование

Самооценка по рискам (Risk Self Assessment)
Обоснование

I. Обоснование

Типы событий Уровня 1	Название риска	Идентификация рисков отсутствует	Для отсутствующих рисков, пожалуйста, приведите обоснование, почему риски неприменимы для Вашего направления бизнеса
1. Внутреннее мошенничество	0	да	
2. Внешнее мошенничество	0	да	
3. Кадровая политика и безопасность труда	0	да	
4. Клиенты, Продукты и Деловая практика	0	да	
5. Ущерб материальным активам	0	да	
6. Перебои в деятельности и системные сбои	0	да	
7. Исполнение, оказание услуг и управление про	0	да	

Если пользователь не выявил и не оценил хотя бы один риск на каждый вид рискового события, необходимо представить объяснение, почему данный вид рискового события не применим для данного подразделения

Утверждение плана мероприятий по минимизации риска

План мероприятий

Самооценка по рискам (Risk Self Assessment)
Обоснование

II. Действия по митигированию (если применимо)

Типы событий Уровня 1	Согласованные действия по митигированию для каждого из типов событий риска Уровня 1	Ответственный
1. Внутреннее мошенничество		
2. Внешнее мошенничество		
3. Кадровая политика и безопасность труда		
4. Клиенты, Продукты и Деловая практика		
5. Ущерб материальным активам		
6. Перебои в деятельности и системные сбои		
7. Исполнение, оказание услуг и управление про		

Обзор проведен

Должность *Дата* *Имя* *Подпись*

Для каждого вида событий сводятся в единый список согласованные действия по минимизации риска с указанием сотрудников, ответственных за реализацию

Заполненный шаблон самооценки должен быть утвержден и подписан ответственным сотрудником, заполняющим анкету, а также руководителем структурного подразделения

Пример карточки риска, KRI, KCI, выявленных в ходе проведения самооценки

Управление кассовой работы

Невыполнение порядка осуществления операций/ошибки при операциях

КИРы

- Сумма непогашенных недостач на 1 работника
- Количество сотрудников, проводящих операции с денежной наличностью
- Количество ошибок, приходящихся на 1 работника

Контроли

- Проведение контрольных процедур со стороны бригадира/контролирующего работника при совершении сотрудниками бригады операций с денежной наличностью
- Обучение/повышение квалификации персонала
- Проведение проверок организации кассовой работы (включая просмотр ТСВ)
- Совершение сотрудниками операций в соответствии с СОПами

KCI

- Количество порверок в квартал
- Количество порверок в квартал

Хищение информации по УС

Нанесение ущерба активам (УС) в результате природных катастроф или вандализма

Получение доступа сотрудников к клиентским данным и использование их в личных целях

Контроли

- Контроль за работой сотрудников путем просмотра ТСВ

Недостачи,связанные со сбоем УС

КИРы

- % количества недостач по причине тех.сбоя от общего количества недостач

Хищение денежных средств банка

Контроли

- Ограниченный вход в хранилище ценностей
- "Принцип 4 глаз"

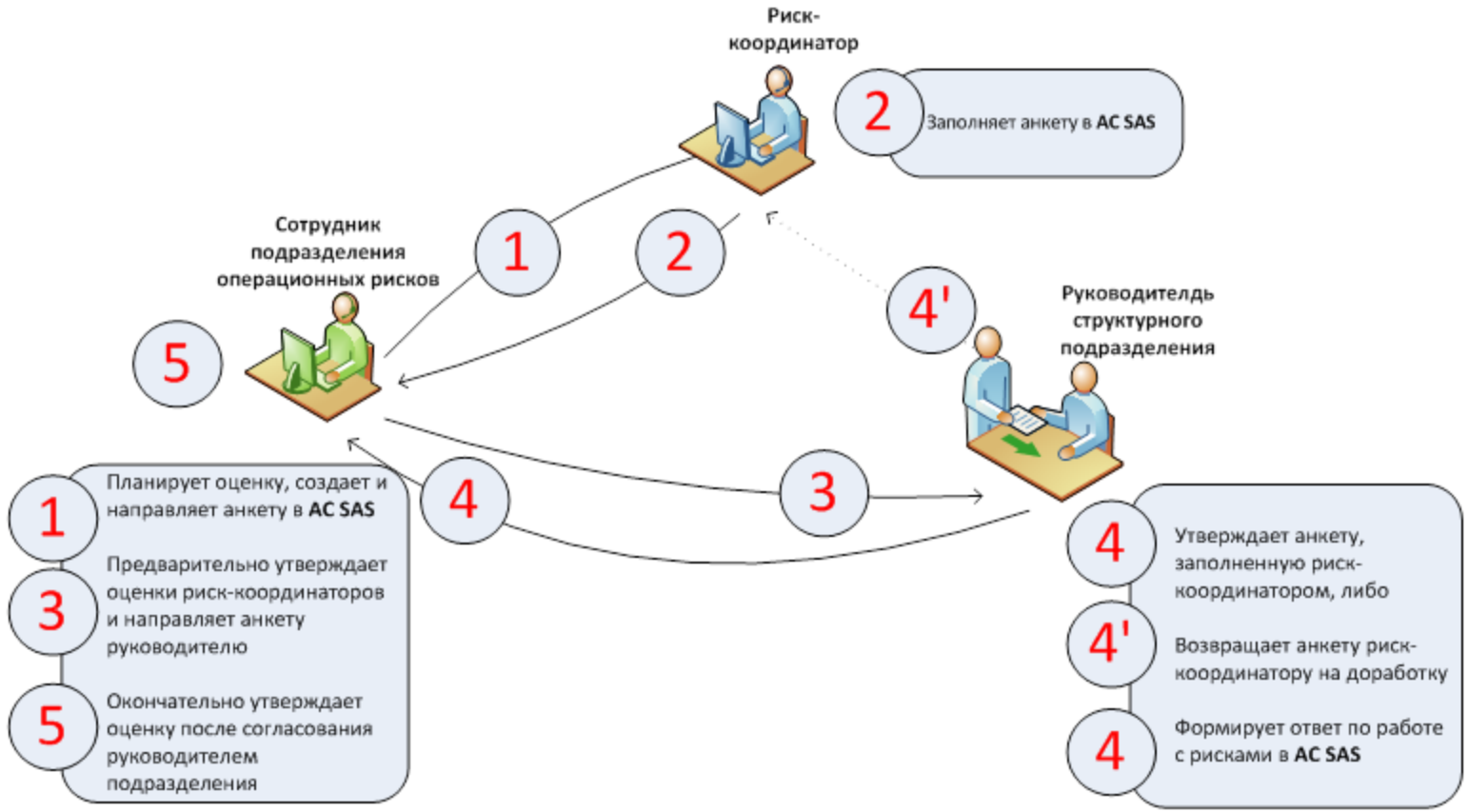
Ограбление кассового центра

Контроли

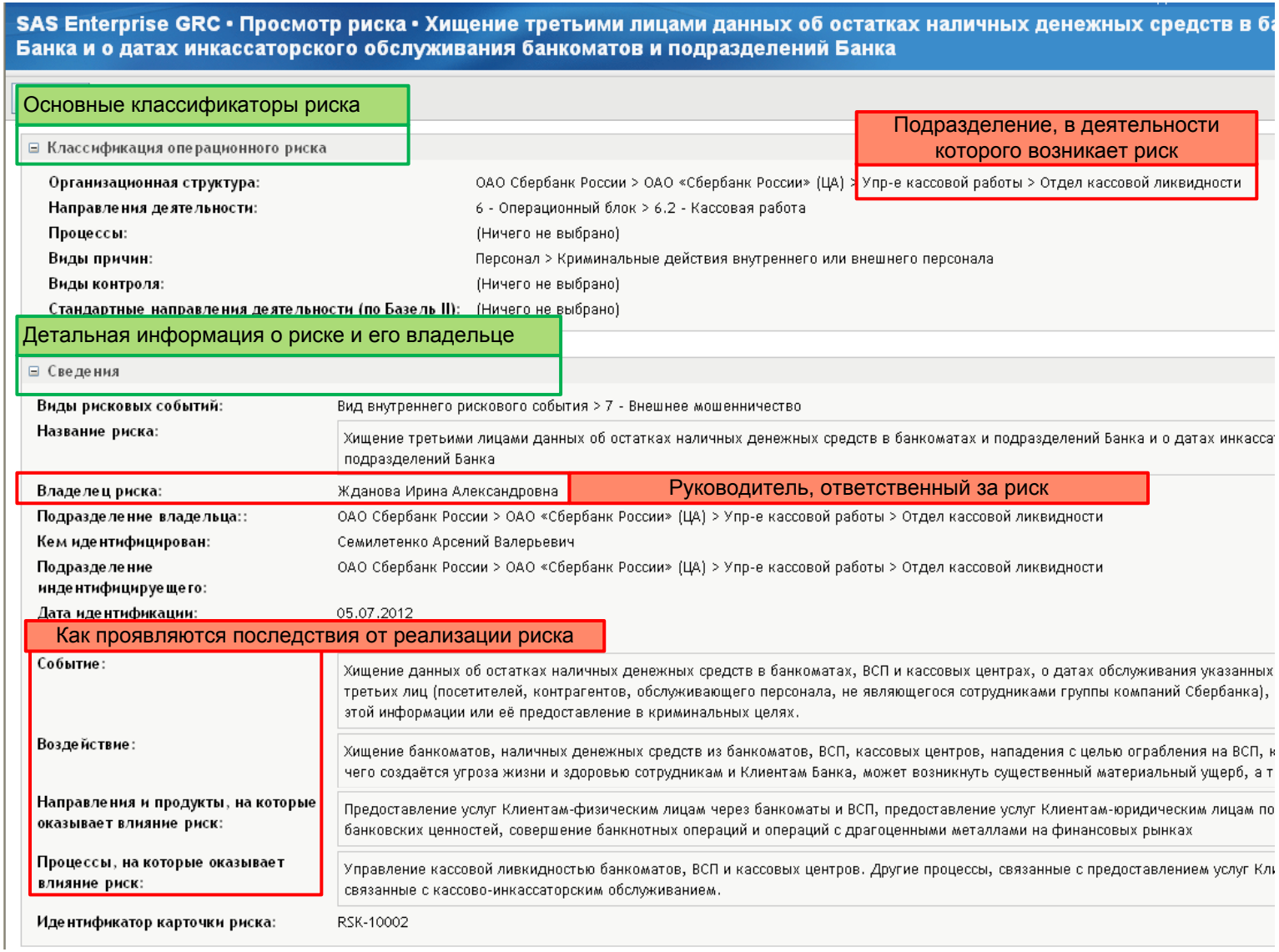
- Контрольные процедуры на уровне автоматизированных систем

Процесс самооценки по операционным рискам с использованием инструмента SAS

Запущен пилотный проект по проведению самооценки по операционным рискам подразделений кассовой работы в АС SAS OpRisk Management



Карточка риска в SAS: основные сведения



Индикаторы риска и контроля в SAS

Перечень индикаторов, привязанных к данному риску

Риск-координатор, который предоставляет оценки КИРов

SAS Enterprise GRC • Просмотр риска • Невыполнение порядка осуществления операций/ошибки при операциях

Готово

Просмотр журнала

Ключевые индикаторы риска (выбранные пользователем)

Удалить... | Добавить...

		Идентификатор КИР	Описание	Владелец	Интервал	Набор классификаторов	Единицы измерения	Удалить
1	☐	KRI-10026	Количество сотрудников, проводящих операции с денежной наличностью	Жиляева Инна Юрьевна	Еженедельно	Виды причин: Персонал > Человеческий фактор, Виды рисковых событий: 1 - Исполнение, оказание услуг и управление процессами, Направления деятельности: 6 - Операционный блок > 6.2 - Кассовая работа, Организационная структура: ОАО Сбербанк России > ОАО «Сбербанк России» (ЦА) > Упр-е кассовой работы > От-л орг-ции кассовой работы	Число	
2	☐	KRI-10027	Количество ошибок, приходящихся на 1 работника	Жиляева Инна Юрьевна	Еженедельно	Виды причин: Персонал > Человеческий фактор, Виды рисковых событий: 1 - Исполнение, оказание услуг и управление процессами, Направления деятельности: 6 - Операционный блок > 6.2 - Кассовая работа, Организационная структура: ОАО Сбербанк России > ОАО «Сбербанк России» (ЦА) > Упр-е кассовой работы > От-л орг-ции кассовой работы	Число	
3	☐	KRI-10028	Сумма непогашенных недостач на 1 работника	Жиляева Инна Юрьевна	Еженедельно	Виды причин: Персонал > Человеческий фактор, Виды рисковых событий: 1 - Исполнение, оказание услуг и управление процессами, Направления деятельности: 6 - Операционный блок > 6.2 - Кассовая работа, Организационная структура: ОАО Сбербанк России > ОАО «Сбербанк России» (ЦА) > Упр-е кассовой работы > От-л орг-ции кассовой работы	Валюта (RUB)	

Строки с 1, по 3, из 3

Механизмы контроля в SAS

SAS Enterprise GRC • Просмотр риска • Возникновение простоев в работе Кассовых центров по причине отсутствия наличных денежных средств

Готово

Просмотр журнала

Риск-координатор может добавлять новые контрольные процедуры к риску

Оценки механизмов контроля и индикаторов контроля

Контрольные процедуры

Контрольные процедуры

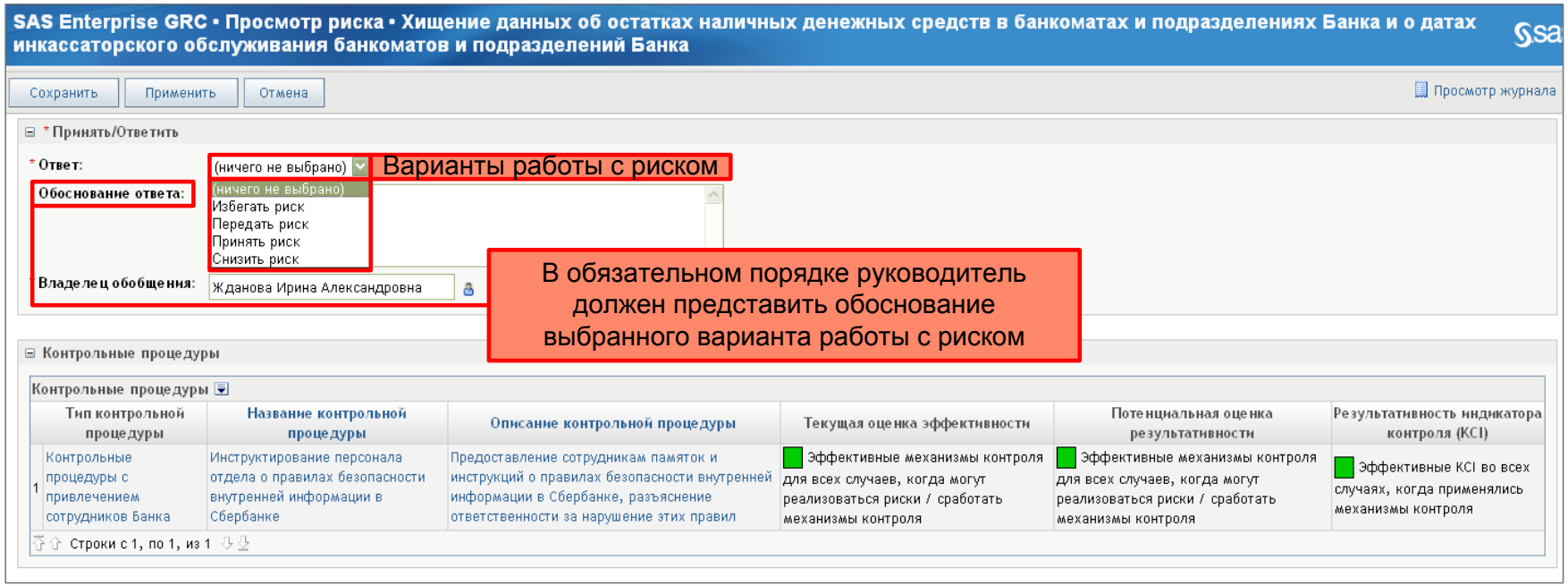
	Тип контрольной процедуры	Название контрольной процедуры	Описание контрольной процедуры	Текущая оценка эффективности	Потенциальная оценка результативности	Результативность индикатора контроля (KCI)
1	Контрольные процедуры с привлечением сотрудников Банка	Удалённое обучение персонала кассовых центров работе в АС "Cash Manager"	Обучение персонала кассовых центров работе в АС "Cash Manager" позволяет избежать ошибок ручного ввода остатков, заявок и прочей информации.	Эффективные механизмы контроля для большинства случаев, когда могут реализоваться риски / сработать механизмы контроля	Эффективные механизмы контроля для большинства случаев, когда могут реализоваться риски / сработать механизмы контроля	Эффективные KCI в большинстве случаев, когда применялись механизмы контроля
2	Контрольные процедуры с привлечением сотрудников Банка	Перераспределение наличных денежных средств между кассовыми центрами	Поддержание в актуальном состоянии технологии перераспределения денежной наличности между кассовыми центрами в случае нехватки денежности наличности в каком-либо Кассовом центре/Кассовых центрах.	Эффективные механизмы контроля для всех случаев, когда могут реализоваться риски / сработать механизмы контроля	Эффективные механизмы контроля для всех случаев, когда могут реализоваться риски / сработать механизмы контроля	Эффективные KCI во всех случаях, когда применялись механизмы контроля
3	Контрольные процедуры на уровне автоматизированных систем	Анализ качества прогноза прихода/расхода наличных денежных средств в/из Кассовые центры/Кассовых центров	Данный механизм контроля тесно связан с прогнозированием потоков наличных денежных средств в ВСП и банкоматах, обслуживаемых ВСП	Эффективные механизмы контроля для большинства случаев, когда могут реализоваться риски / сработать механизмы контроля	Эффективные механизмы контроля для большинства случаев, когда могут реализоваться риски / сработать механизмы контроля	Эффективные KCI в большинстве случаев, когда применялись механизмы контроля

Строки с 1, по 3, из 3

При наличие нескольких контролей для определения суммарного рейтинга риска используется максимальная оценка из всех оценок контролей. В данном примере – эффективные механизмы контроля для всех случаев

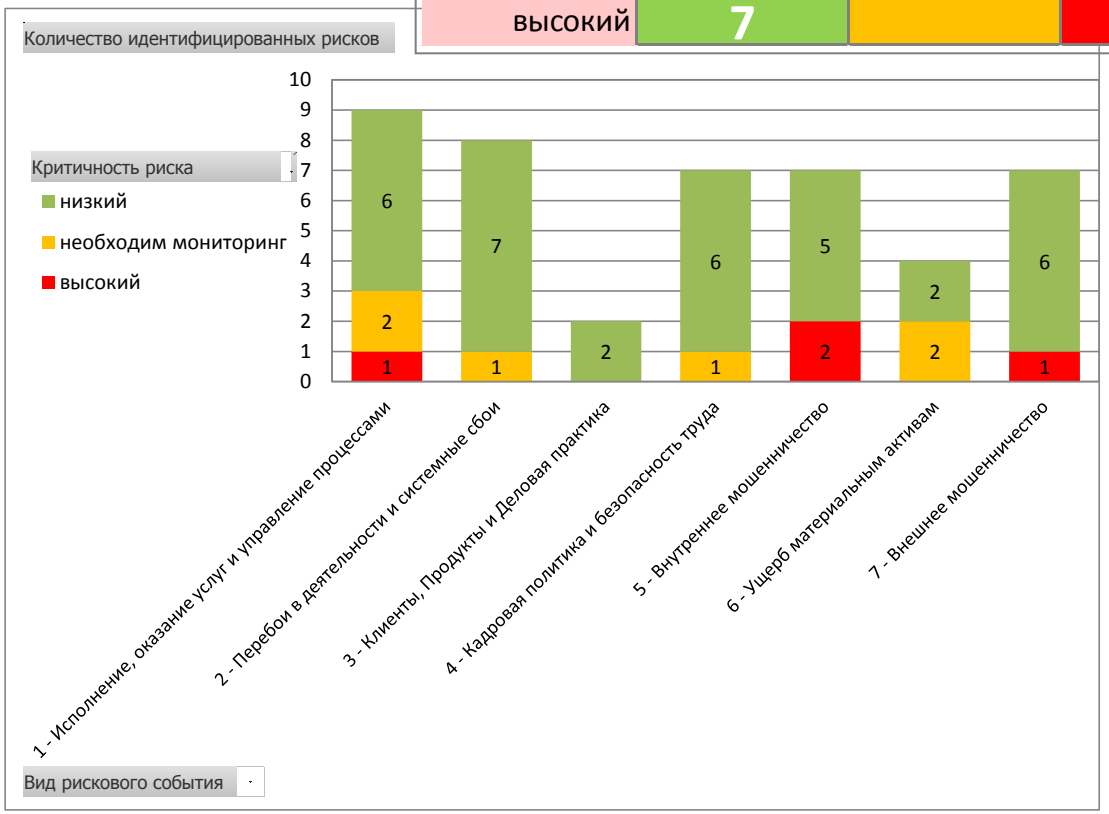
Варианты реагирования на риск руководителя подразделения

Принять риск	Избегать риск	Передать риск	Снизить риск
Действий не требуется, согласие с оценкой риска и самостоятельная ответственность руководителя за риск	Прекращение деятельности/ инициатив, связанных с данным риском	Передача ответственности за риск; страхование	Предложения по мероприятиям, направленным на снижение подверженности риску: сокращение вероятности его реализации и объема потерь, улучшению контрольной среды



Матрица рисков и контролей: пример отчета по самооценке

Управление кассовой работы					
	Эффективность контрольных процедур				
Рейтинг риска	Высокая	Достаточная	Средняя	Ограниченная	Нулевая
низкий	13	1	1	2	3
средний	7	2		1	3
высокий	7		2		2



Что необходимо для запуска самооценки по операционным рискам

Ключевые шаги

СПАСИБО ЗА ВНИМАНИЕ!