AKTIV.
CONSULTING

Границы ответственности службы ИБ в процессе управления операционными рисками

Олег Симаков
Руководитель направления по работе с клиентами AKTIV.CONSULTING

О чем сегодня пойдет речь

Блок I	Управление ОР в структуре организации
Блок II	Функциональные границы ИБ при различных сценариях
Блок III	Проект внедрения изменений

AKTIV.
CONSULTING

Блок I

Управление ОР в структуре организации

Управление операционными рисками. Какая польза?

Финансовая организация

Менеджмент
- процессы управления

Выгоды:
- непрерывность бизнеса
- эффективное распределение ресурсов

Операционная деятельность
- критичные бизнес-процессы
- основные бизнес-процессы
- обеспечивающие бизнес-процессы

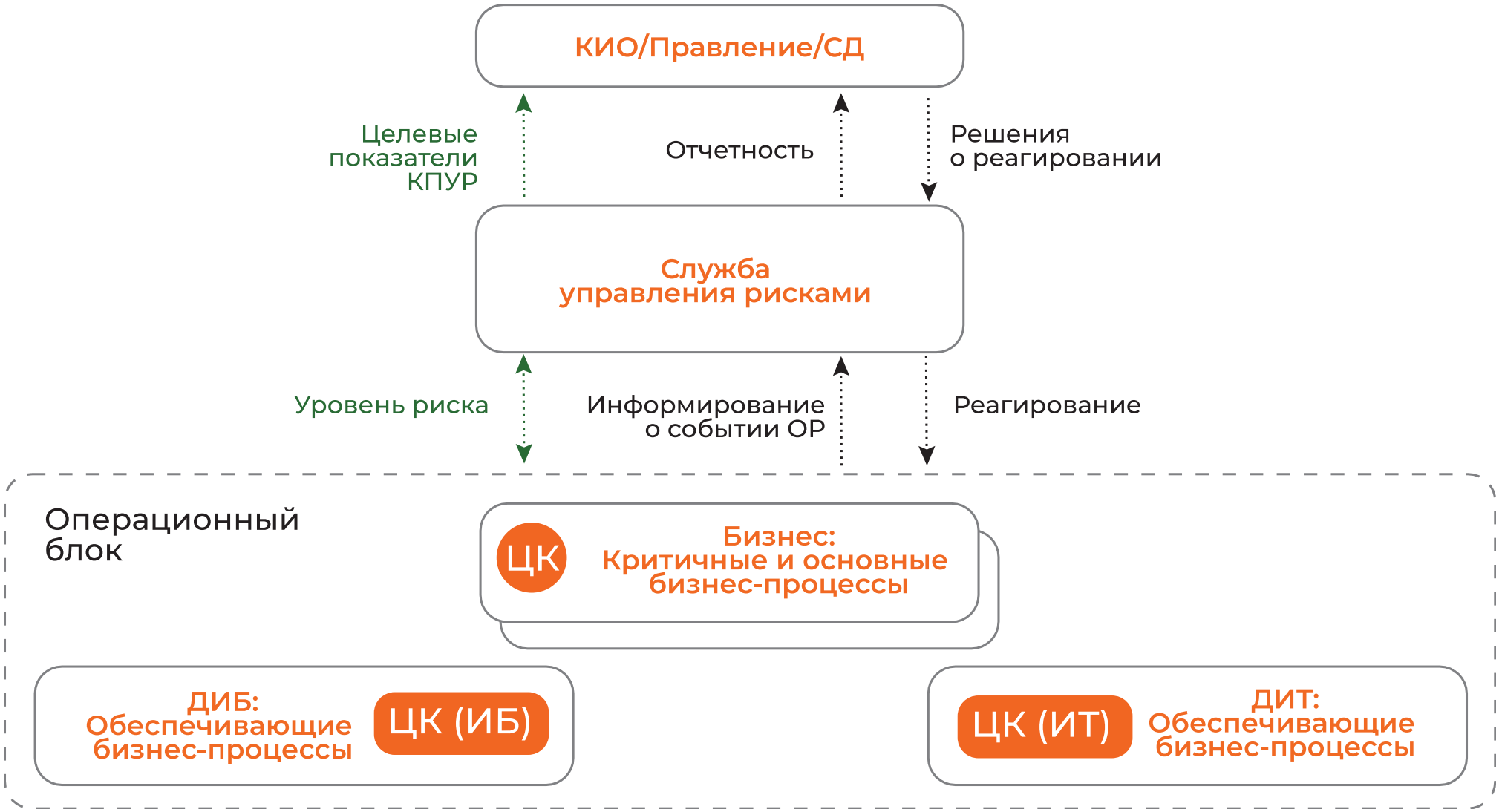
Выгоды:
- обоснование ресурсов

Функция управления операционным риском

Государство (ЦБ РФ)

Цель — устойчивость банковской системы

Организационная структура и основные процессы УОР



Сценарии внедрения СУОР

	Текущая ситуация	Сценарий для службы ИБ	Роль службы ИБ	Управление риском ИБ по 716-П
I	СУОР внедрен или планируется в службе управления рисками	1 Служба ИБ формирует свою часть процессов и встраивает их в СУОР	Ведомая: • СУР руководит проектом внедрения системы • СУР владеет процессом управления рисками ИБ	Да
II	Служба управления рисками не внедряет СУОР/ не включает в СУОР риски ИБ	2 Служба ИБ адаптирует процессы в рамках своего подразделения	Автономная	Нет
		3 Служба ИБ создает собственную систему управления риском ИБ, при этом формируется отдельный контур управления ОР	Ведущая: • Руководит проектом внедрения системы • Владеет процессом управления рисками ИБ	Да

Важное по первому блоку

1. У внедрения управления оперрисками есть преимущества, как для менеджента, так и для обеспечивающего подразделения (ДИБ)

2. Даже если СУОР в организации нет, функцию по управлению рисками требуется выполнять

3. Для службы ИБ есть три сценария реализации требований регулятора, как минимум. В зависимости от сценария, роли, участие и ответственность будут отличаться

4. Служба ИБ не может взять на себя полностью управление оперриском. Даже если СУОР будет выстраиваться внутри ДИБа, менеджмент будет выполнять функции согласования и контроля

AKTIV. CONSULTING

AKTIV.
CONSULTING

Блок II

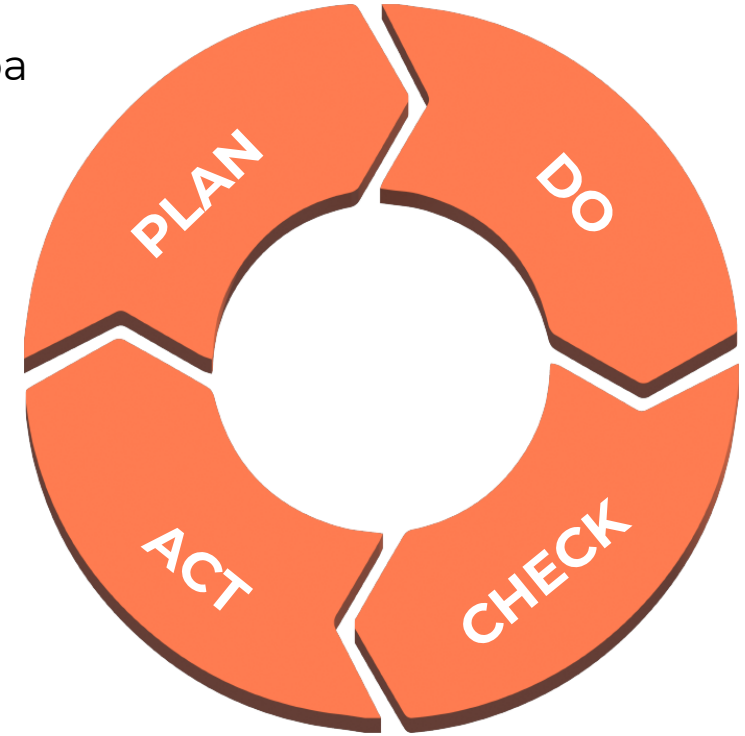
Функциональные границы ИБ при различных сценариях

Целевое состояние процесса управления риском ИБ

Процесс управления, выстроенный по циклу Деминга:

1 Формирование реестра

2 Утверждение КПУР



3 Сбор и регистрация событий

4 Мониторинг

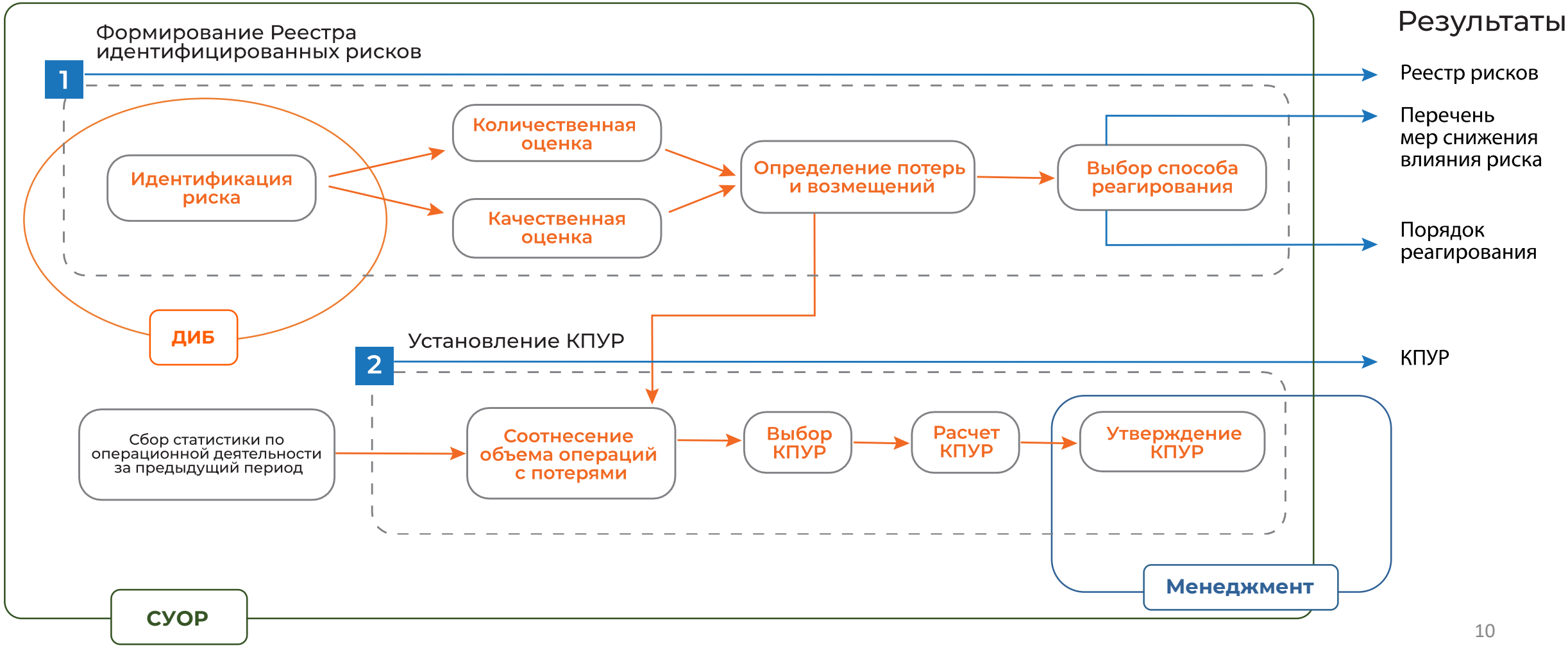
5 Отчетность

6 Реагирование

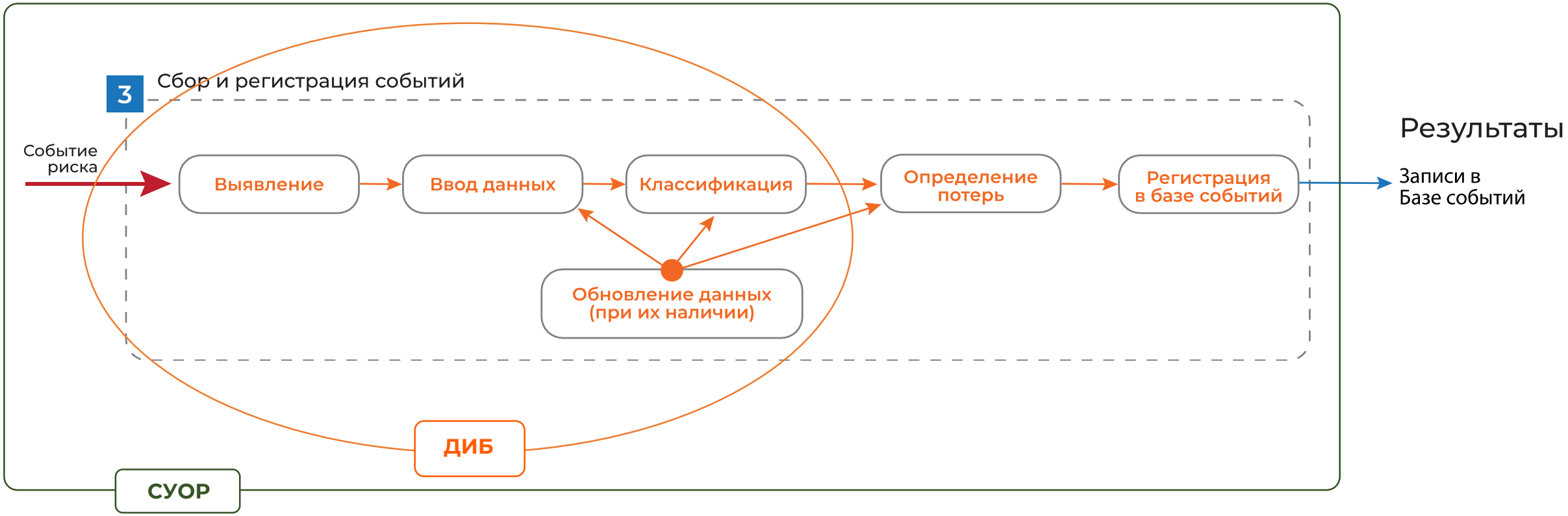
7 Аудит

8 Повышение качества

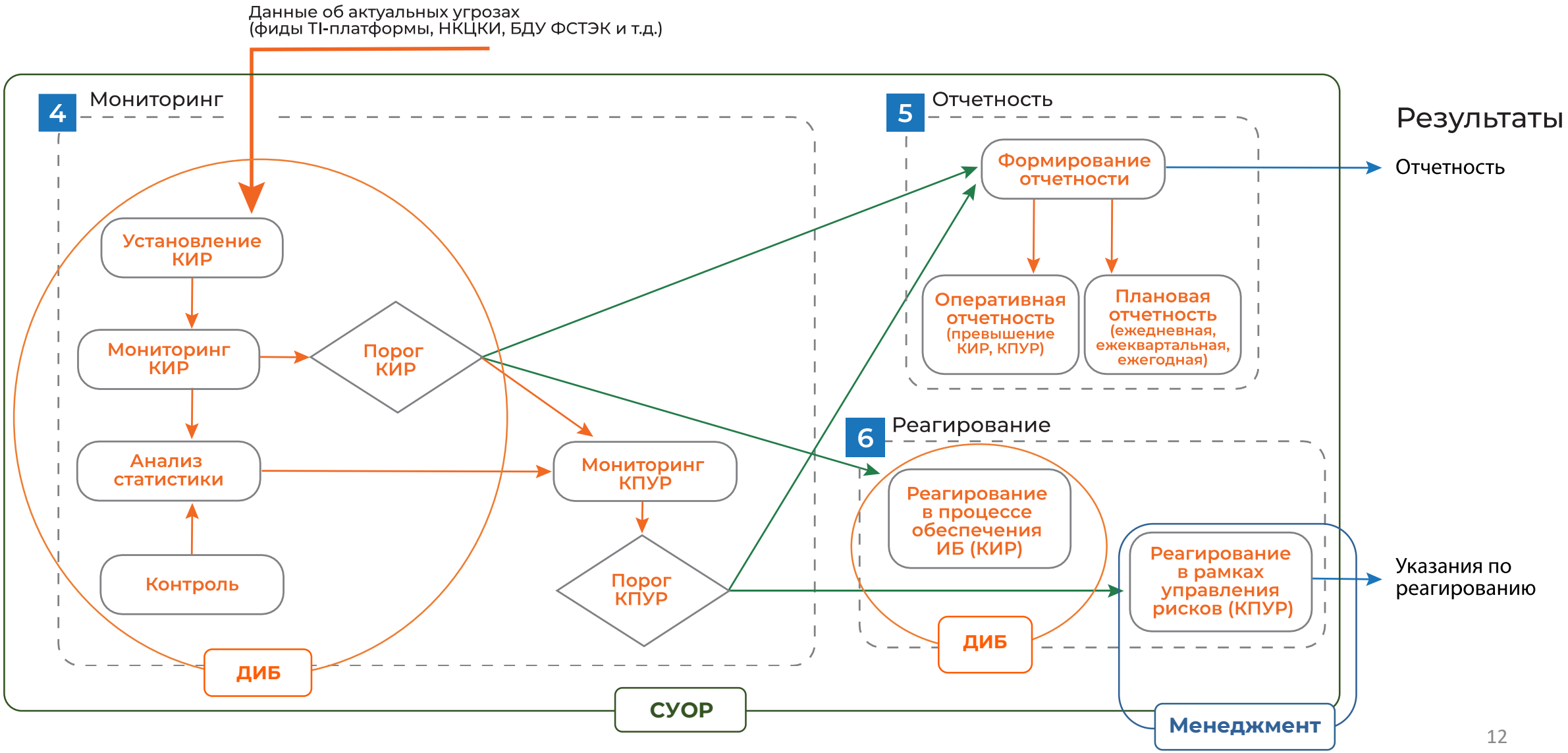
Планирование



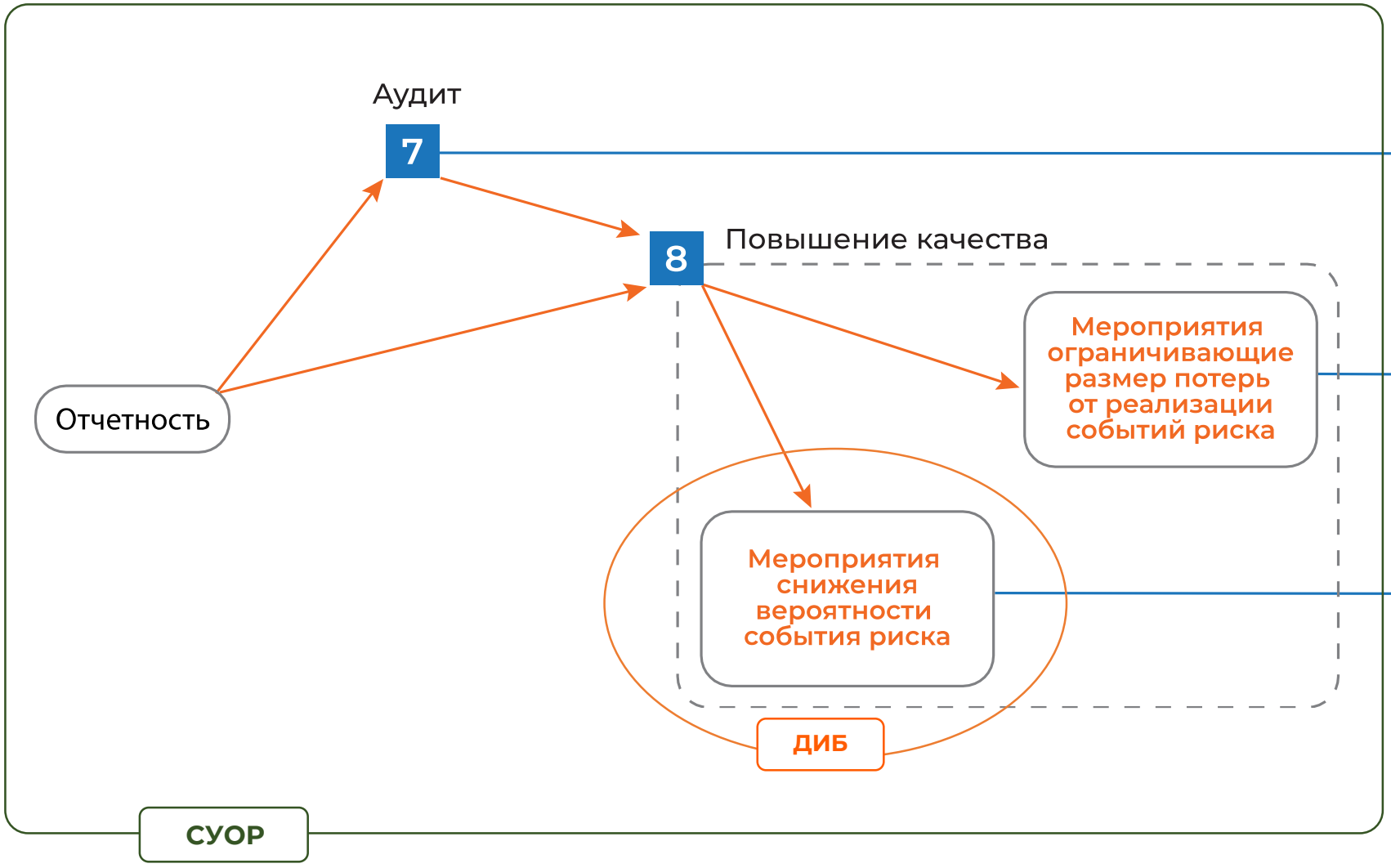
Реализация


3
Сбор и регистрация событий
Событие риска
Выявление
Ввод данных
Классификация
Определение потерь
Регистрация в базе событий
Обновление данных (при их наличии)
ДИБ
СУОР
Результаты
Записи в Базе событий

Контроль


Данные об актуальных угрозах
(фиды TI-платформы, НКЦКИ, БДУ ФСТЭК и т.д.)
4 Мониторинг
Установление КИР
Мониторинг КИР
Порог КИР
Анализ статистики
Контроль
ДИБ
Мониторинг КПУР
Порог КПУР
5 Отчетность
Формирование отчетности
Оперативная отчетность (превышение КИР, КПУР)
Плановая отчетность (ежедневная, ежеквартальная, ежегодная)
6 Реагирование
Реагирование в процессе обеспечения ИБ (КИР)
ДИБ
Реагирование в рамках управления рисков (КПУР)
Менеджмент
СУОР
Результаты
Отчетность
Указания по реагированию

Совершенствование



Результаты

Отчет по результатам аудита системы управления риском

План мероприятий по снижению вероятности события риска

План мероприятий по ограничению размера потерь от реализации событий риска

Важное по второму блоку

1. Процессы ложатся в PDCA. Для каждого этапа цикла не трудно выделить свою ответственность в ходе декомпозиции процессов

2. Служба ИБ не может взять на себя полностью управление оперриском, так как даже если СУОР будет выстраиваться внутри ДИБа, менеджмент будет выполнять функции согласования и контроля

AKTIV. CONSULTING

AKTIV.
CONSULTING

Блок III

Проект внедрения изменений

Пример проекта по внедрению

01 этап **Инициация**

- Определение целей проекта
- Определение задач проекта
- Определение границ проекта

Результат этапа:

Решение руководства о выделении ресурсов и полномочий

02 этап **Аудит**

- Обследование текущих бизнес процессов разработки
- Формирование целевого состояния процессов
- GAP-анализ
- Разработка организационных и технических мер безопасности

Результат этапа:

Перечень мероприятий

Пример проекта по внедрению

03 этап **Планирование**

- Ранжирование мер
- Определения взаимных связей и зависимостей
- Формирование план-графика

Результат этапа:
Дорожная карта

04 этап **Внедрение процессов**

- Разработка ВНД
- Подготовка Базы событий
- Разработка классификатора
- Выбор методики расчета КПУР (СЗ, КЗ)
- Выбор методики расчета резервируемого капитала
- ...

Результат этапа:
Запущен процесс управления рисками ИБ

05 этап **Контроль**

Проверка полноты и достаточности

Результат этапа:
Отчет уполномоченного подразделения (СВА)

Важное по третьему блоку

1. На этапе инициации мы получаем ресурсы и полномочия на изменения

2. Проектный поход гарантирует соблюдение сроков и достижения поставленных целей

AKTIV. CONSULTING

В качестве резюме

1 В любом сценарии реализовать требования 716-П — решаемая задача:

- Границы ответственности проще сформировать при проектировании целевого процесса
- Внедряем изменения проектом

2 Риск-ориентированный подход обосновывает выделение ресурсов

3 При отсутствии СУОР у руководителя службы ИБ создается уникальная возможность выйти за пределы обеспечивающих процессов

AKTIV. CONSULTING

AKTIV.
CONSULTING

Олег Симаков

Руководитель направления по работе
с клиентами AKTIV.CONSULTING

simakov@aktiv.consulting