

КОНФЕРЕНЦИЯ · КОМПЛАЕНС, ВНУТРЕННИЙ КОНТРОЛЬ И
АУДИТ В ФИНАНСОВЫХ ИНСТИТУТАХ

Роль внутреннего аудита при оценке эффективности системы внутреннего контроля и управления рисками компании

Практика риск-ориентированного внутреннего аудита
в публичной Fintech-компании (листинг AIX)

Алла Цих

Руководитель ООО «Полет Финанс»



Алла Цих

FCCA,

Руководитель СВА Группы NanduQ, ООО «Полет Финанс».

Опыт работы в области СУРiBK и аудита более 10 лет,
в области подготовки МСФО отчетности более 10 лет.

Почему оценка СУРиВК критична для публичной Fintech-компании

Публичный статус (AIX)

Раскрытие, ответственность Совета, ожидания инвесторов к качеству контролей и отчётности.

Регуляторное давление

AFSA, AML/CFT, требования к KYC, защите данных, операционной устойчивости.

Скорость продуктовых релизов

Платежи, антифрод, кредитные продукты меняются быстрее контрольной среды.

Концентрация ИТ- и кибер-рисков

Зависимость от облака, API-партнёров, процессинга. Один инцидент — материальное событие.

Доверие клиента и капитал

Утрата доверия монетизируется в отток, стоимость капитала и мультипликатор.

Прозрачность для Совета и КА

Совет ждёт объективной картины зрелости — не отчёта менеджмента «о себе».

Три линии защиты: место и независимость внутреннего аудита

Линия 1

Управление риском

Бизнес и операции: продукт, платежи, KYC, IT. Идентификация рисков, дизайн и исполнение контролей.

Линия 2

Надзор за риском

СУР, СВК, Служба COMPLIANCE: Политики и стандарты, лимиты, методология, мониторинг.

Линия 3

Внутренний аудит

Независимая объективная оценка эффективности СУРиВК. Подотчётность Комитету по аудиту и Совету директоров.

Роль внутреннего аудита: независимо подтвердить, что СУРиВК спроектирована в соответствии с риск-ориентированным подходом и работает на практике; выявленные недостатки и планы мероприятий по устранению эскалировать Совету директоров.

Риск-ориентированный внутренний аудит: 6 основных принципов

01

Объекты: Процессы и риски

Существенные процессы и риски, а не «отделы по списку».

02

Связь со стратегией

План формируется в соответствии со стратегией и целями, риск-аппетитом, утверждёнными Советом директоров.

03

Мониторинг рисков

Все существенные риски — ротационный мониторинг на горизонте 1–3 лет.

04

Анализ остаточного риска

Чем выше остаточный риск, тем шире выборка и глубже тестирование.

05

Независимость

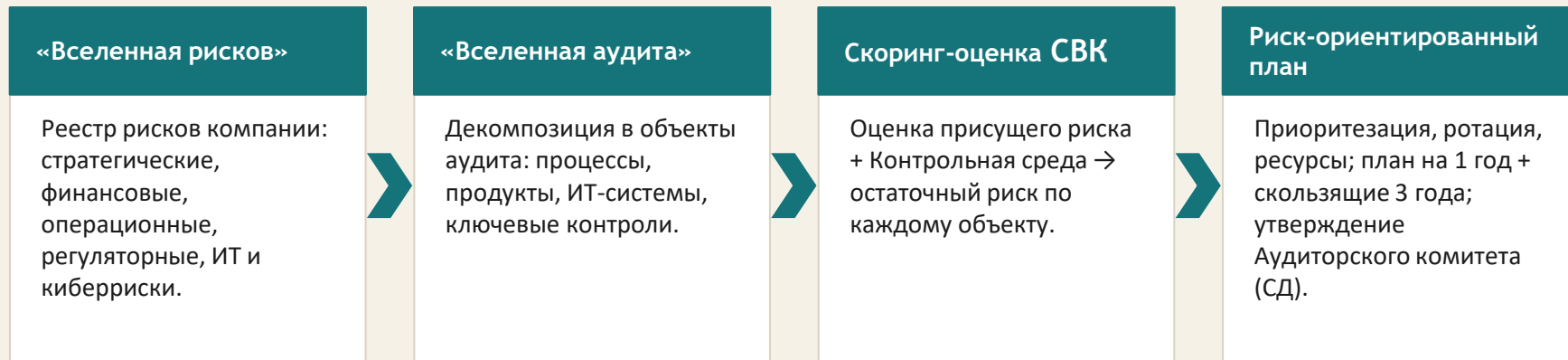
Подотчётность Аудиторскому комитету (СД); ресурсы и бюджет защищены от давления менеджмента.

06

Доказательность

Каждый вывод — на основе доказательств; каждая рекомендация и сроки согласованы с владельцем.

От «Вселенной рисков» к плану аудита: единая цепочка обоснования



Контрольная среда — мультипликатор: высокий «присущий» риск + слабая контрольная среда = высокий остаточный риск → объект имеет высокий приоритет для плана аудита.

Практический годовой цикл планирования внутреннего аудита

Q1

Оценка

Обновление «Вселенной рисков»; интервью/опрос топ-менеджмента /владельцев процессов; обзор контрольной среды; обновление скоринг-оценки СВК.

Q2

Планирование

Формирование плана на отчетный год с учетом 3-летнего цикла; согласование ресурсов; утверждение Аудиторским комитетом.

Q3

Исполнение

Тематические аудиты по плану; тестирование СВК, запросы руководства по мере возникновения;

Q4

Отчётность

Отчёт Аудиторскому комитету по итогам отчетного года; агрегация недостатков; пересмотр плана по устранению недостатков; планы мероприятий; мониторинг.

Ежеквартальный пересмотр риск-скоринга. Перебалансировка плана при новом продукте, сделках M&A, инциденте, изменении регулирования.

Скоринг-модель оценки СУРиВК: «Имеется» + «Работает»

Логика оценки одного критерия






Имеется в наличии Да = 0,5 / Нет = 0

Работает Да = 0,5 / Нет = 0

Оценка критерия Сумма = 0 / 0,5 / 1,0

Итог по компоненту = Σ фактических / Σ максимальных × 100%

Шкала зрелости

	1	Слабый	0–20 %
	2	Устойчивый	21–40 %
	3	Развитый	41–60 %
	4	Интегрированный	61–80 %
	5	Продвинутый	81–100 %

8 компонентов оценки СУРиВК — около 120 критериев

1**Внутренняя среда**

~30 крит.

2**Постановка целей**

~13 крит.

3**Оценка рисков**

~19 крит.

4**Реагирование
на риски**

~8 крит.

5**Контрольные
процедуры**

~8 крит.

6**Информация
и коммуникации**

~16 крит.

7**Мониторинг**

~10 крит.

8**Функции
и обязанности**

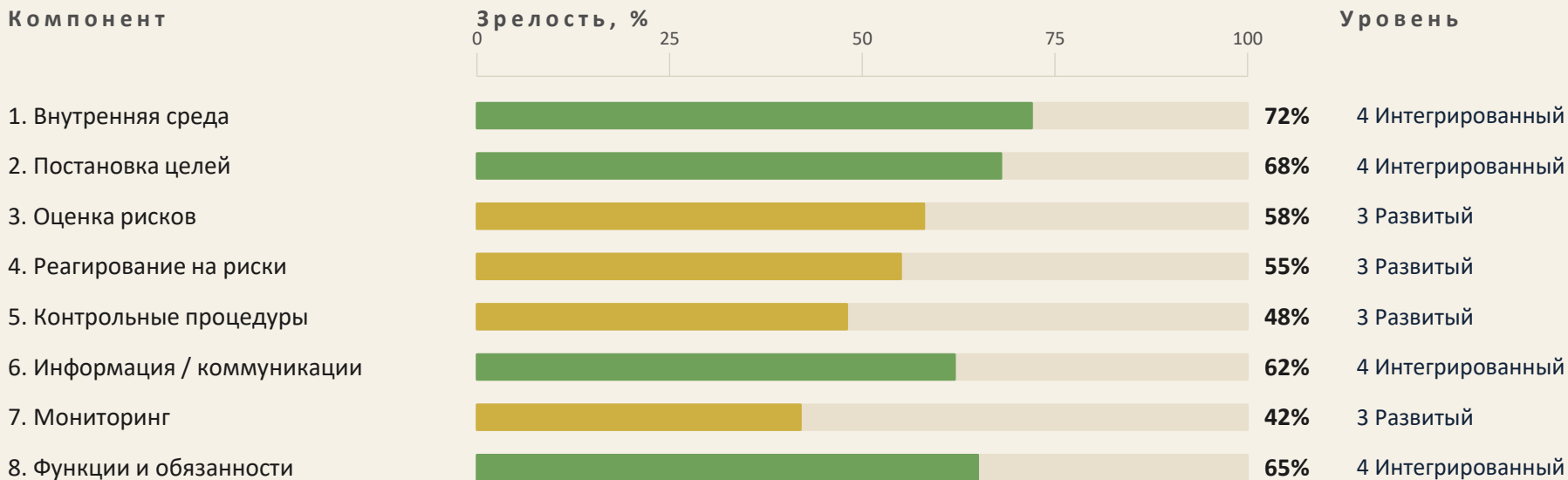
~16 крит.

Итог по каждому компоненту — отдельный процент зрелости. Общий индекс СУРиВК — среднее по компонентам с весами, утверждёнными Аудиторским комитетом (СД).

Матрица зрелости: что означает каждый уровень

№	Уровень	Диапазон	Характеристика
1	Слабый	0–20 %	Процессы не определены; результат зависит от индивидуальных усилий; нет единых стандартов СУРиВК.
2	Устойчивый	21–40 %	Определены базовые принципы; формализованы основные процессы СУРиВК для ключевых бизнес-процессов.
3	Развитый	41–60 %	Внедрены и активно используются системы; формализованы все процессы СУРиВК; ориентация на развитие.
4	Интегрированный	61–80 %	Процессы и стандарты СУРиВК интегрированы с бизнес-процессами и ИС; решения — на основе аналитики.
5	Продвинутый	81–100 %	Непрерывное улучшение; автоматический сбор и анализ данных для выявления рисков и оптимизации системы.

Профиль зрелости компонентов: пример Fintech-компании



Общий индекс СУРиВК: 58% — «Развитый» (уровень зрелости 3). Цель года: 65% — «Интегрированный» (уровень зрелости 4).

Узкие места: компоненты 5 - уровень зрелости 3 (48%) и 7 - уровень зрелости 3 (42%).

Как формируется план: пример приоритезации в Fintech

Объект аудита	Inherent	Контр. среда	Остаточный	Покрытие
Платежная инфраструктура	Высокий	Средняя	Высокий	Полный аудит, Q3
KYC / клиентская идентификация	Высокий	Средняя	Высокий	Тематический, Q2
Антифрод (онлайн-транзакции)	Высокий	Слабая	Критический	Углублённый, Q2–Q3
ИТ и киберриски (cloud, доступы)	Высокий	Средняя	Высокий	Сквозной, Q3
Операционная устойчивость / BCP	Средний	Средняя	Средний	Тематический, Q4
Финансовая отчётность и раскрытие	Высокий	Сильная	Средний	Ежегодно, Q1+Q4
AML/CFT мониторинг	Высокий	Средняя	Высокий	Полный, Q2

Приоритет = $f(\text{остаточный риск, материальность для публичной отчётности, регуляторное давление, время с последней проверки})$.

Как выполняется проверка: 5 шагов тестирования контролей

01	Planning & scoping	Уточнение объёма, рисков, контролей; определение assertions; согласование с владельцем процесса.
02	Walkthrough	Прохождение процесса end-to-end на единичной транзакции; верификация дизайна контролей.
03	Design effectiveness	Оценка достаточности дизайна каждого ключевого контроля относительно риска и assertion.
04	Operating effectiveness	Выборочное тестирование исполнения: re-performance, inspection, observation; ITGC для авто-контролей.
05	Conclusion & reporting	Формирование наблюдений с уровнем риска; обсуждение с владельцем; формализация в отчёте.

IPE-тестирование: если в контроле используется отчёт из системы — проверяем полноту и точность/аккуратность отчёта.

Выявление слабых мест в СУРиВК: где и как мы их находим, примеры

Платежная инфраструктура

Несогласованные изменения релизов; неполное логирование; ручные обходы лимитов.

КУС и идентификация

Устаревшая верификация; нет EDD для high-risk сегментов; пробелы в источниках.

Антифрод

Правила не пересматриваются; высокий уровень ложных срабатываний; нет разборов событий после выявления и завершения.

ИТ и киберриски

Расширенные доступы; нет разделения полномочий (Разработчик ПО и Администратор ПО); Прочие конфликты разделения полномочий (SoD-конфликты).

Операционная устойчивость

Планы непрерывности деятельности (BCP) без реальных учений; зависимость от ключевых партнёров без exit-plan.

Финансовая отчётность

Недостаточный анализ нестандартных проводок; недостаточный контроль по обязательным раскрытиям (disclosure-checklist).

На что следует обратить внимание: критерий «Имеется = Да, Работает = Нет» — формальный документ без операционной эффективности.

Классификация и агрегирование недостатков

Уровень 1	Уровень 2	Уровень 3	Уровень 4
Низкий <i>Deficiency</i> Изолированный пробел; компенсирующие контроли работают.	Средний <i>Deficiency</i> Существенный пробел в дизайне или исполнении; план митигации в текущем квартале.	Высокий <i>Significant deficiency</i> Значимый недостаток; внимание Комитета по аудиту; срочный план.	Критический <i>Material weakness</i> Материальная слабость; немедленные действия; раскрытие Совету директоров.

АГРЕГИРОВАНИЕ

Несколько недостатков «низкий/средний» в одном процессе или по одному утверждению по существенной статье (assertion) → могут агрегироваться в Significant deficiency или Material weakness. Анализируем выявленные недостатки в совокупности, а не только каждый выявленный недостаток контроля изолированно.

Коммуникация с Комитетом по аудиту и Советом директоров

Ежеквартальный отчёт

Статус плана, ключевые находки, статус митигации, обновлённый риск-скоринг.

Годовой отчёт о СУРиВК

Индекс зрелости в совокупности и в разрезе по 8 компонентам, динамика, бенчмарк к цели года.

Немедленная эскалация

Material weakness и инциденты с потенциалом раскрытия — внеплановый доклад Аудиторскому комитету (СД).

Закрытая сессия

Руководитель СВА— закрытая сессия с Председателем Аудиторского комитета без присутствия менеджмента, не реже раза в год.

Прозрачность ресурсов

Бюджет, штат, независимость, методология — на утверждении Аудиторского комитета.

Связка с внешним аудитом

Координация по областям аудита, обмен наблюдениями, без потери независимости.

Дорожная карта улучшений: от «Развитого» к «Интегрированному»

Q1

Критические зоны

Привилегированные доступы; обходы лимитов в платежах; Расширенные проверки для клиентов с высоким риском (KYC).

Q2

Антифрод и мониторинг

Пересмотр правил; метрика ложных срабатываний (false positives); ежемесячный анализ (post-mortem) инцидентов.

Q3

Автоматизация

Непрерывный мониторинг для платежей и KYC; единый дашборд для Аудиторского комитета.

Q4

Среда и культура

Регулярное обучение владельцев процессов и контролей; обновление политик; учения BCP.

Контрольная точка: цель года — индекс СУРiBK $\geq 65\%$ (уровень 4, «Интегрированный»).
Внутренний аудит верифицирует и подтверждает оценку эффективности СУРiBK.

В Ы В О Д

Внутренний аудит — независимая уверенность для Совета директоров

- Риск-ориентированная модель связывает риски компании, контрольную среду и план аудита в одну логику.

- Шаблон «Имеется + Работает» по 8 компонентам и ~120 критериям даёт измеримую оценку зрелости СУРиВК.

- В Fintech приоритеты — платежи, KYC, антифрод, ИТ и киберриски, операционная устойчивость, раскрытие.

- Слабые места классифицируются и агрегируются; материальные — раскрываются Комитету по аудиту.

- Цель аудита — не «найти больше», а непрерывно развивать и повышать уровень зрелости СУРиВК.