Как выбрать правильный периметр ИТ и ИБ аудита: риск-ориентированный подход и Red Flags

ISACA Nur-Sultan Chapter
Институт внутренних аудиторов РК

The Institute of Internal Auditors Kazakhstan

ISACA Nur-Sultan Chapter

Март 2026

Oleg Prokudin

CISA, CISSP, ISO27001 Lead Implementer and Auditor
Head of IT/IS methodology and compliance
Freedom Holding

The Institute of Internal Auditors Kazakhstan

ISACA Nur-Sultan Chapter

Содержание

The Institute of Internal Auditors Kazakhstan

ISACA Nur-Sultan Chapter

Что такое Scope (область аудита)

Scope (скоуп) — это документированная граница проверки:
что именно мы проверяем и в каких рамках, чтобы дать обоснованное assurance.

Scope фиксирует:

- Цель и вопросы аудита (что хотим подтвердить/оценить)
- Границы охвата: системы/процессы/подразделения/локации + период
- Критерии оценки: политики/стандарты/регуляторика/внутренние требования
- Исключения и ограничения (что не покрываем и почему)

Артефакт на выходе (что должно «остаться на бумаге»)

Scope Statement : цель + включено/исключено + критерии + период + ограничения.
Audit Program / Программа аудита: процедуры + источники доказательств + методы + сроки.

Аудитор часто проверяет НЕ то, что создает риск

Рутина может привести к неправильному выбору скоупа

- Фокус смещается на формальное выполнение контролей, а не на области с наибольшим риском
- Проверяются стандартные процессы, в то время как ключевые источники риска могут оставаться вне скоупа
- Аудит концентрируется на том, что легче проверить, а не на том, что критично для бизнеса
- Контроли оцениваются изолированно, без анализа реальных сценариев сбоев и инцидентов
- В результате аудит может подтвердить соответствие, но не выявить уязвимости

Результат: аудит может подтвердить соответствие, но не выявить уязвимости

Как не попасть в ловушку «не того скоупа»

Скоуп аудита должен определяться не перечнем процессов, а источниками риска.

- Начинать не с контролей, а с понимания бизнес-контекста
- Определять, где формируется риск, а не где есть процедуры
- Учитывать архитектуру, данные и зависимости
- Анализировать реальные сценарии инцидентов
- Использовать Red Flags как триггеры для углубления

Ключевой вопрос: Где компания наиболее уязвима? Почему мы это проверяем?

Что на практике определяет скоуп аудита?

Risk Drivers — факторы, формирующие риск в ИТ и ИБ

- Данные (что защищаем?)
- Доступы (кто имеет доступ?)
- Архитектура (как устроена система?)
- Подрядчики (кто ещё вовлечен?)
- Изменения (что меняется?)

Чтобы выяснить Risk Drivers – нужно иметь информацию.

Давайте задавать вопросы?

Вопросы

Которые меняют скоуп ИТ и ИБ аудита

1. Данные и критичность

Где хранятся критичные/финансовые/персональные данные?

Есть ли централизованные БД / DWH / Data Lake?

Есть ли репликация данных (в т.ч. cross-border)?

Кто является владельцем данных (data owner)?

2. Доступы и пользователи

Есть ли привилегированные доступы (DBA, админы)?

Используется ли MFA для критичных систем?

Есть ли удаленный доступ (VPN, external access)?

Есть ли shared accounts или прямой доступ к БД?

3. Архитектура и технологии

Используется ли cloud / hybrid инфраструктура?

Есть ли прямая интеграция систем (API, ETL)?

Есть ли legacy-системы без поддержки?

4. Подрядчики и third parties

Есть ли подрядчики с доступом к системам/данным?

Есть ли доступ подрядчиков в продакшн?

Есть ли DPA / SLA / контроль третьих лиц?

Есть ли внешние команды?

5. Изменения и процессы

Были ли крупные изменения (M&A, миграции, новые системы)?

Используется ли DevOps / частые релизы?

Есть ли ручные операции в критичных процессах?

Есть ли зависимость от ключевых сотрудников?

6. Регуляторика и бизнес-контекст

Подпадает ли компания под регуляторные требования (SOX, GDPR и др.)?

Зависит ли бизнес от непрерывности ИТ (24/7)?

Есть ли высокая стоимость простоя / инцидента?

Были ли инциденты или замечания аудиторов ранее?

Превращение

ответов на вопросы в скоуп аудита

1. Смотрим не на отдельные ответы, а на их комбинации

- Один фактор риска — это сигнал
- Несколько факторов — это уже область повышенного риска

Важно: риск формируется на пересечении

2. Определяем, где может пойти не так

- Где возможен несанкционированный доступ
- Где возможна утечка данных
- Где возможен сбой из-за изменений
- Где есть зависимость от третьих лиц

3. Формируем фокус аудита

Проверяем не **«процесс»**, а **область риска**

Например

Есть:

- централизованный DWH
- доступы DBA
- подрядчик с доступом

Концентрируемся при проверке:

- IAM (привилегированные доступы)
- Third-party risk
- Контроль доступа к данным

Red Flags

Red Flags — это сигналы, указывающие на повышенный риск, ещё до начала детальной проверки

Управляемость

- Нет понятного владельца системы/риска
- Размытые зоны ответственности
- Много статусов — мало ясности

Риск не управляется системно

Наблюдаемость

- Нет уверенности, что происходит в системе
- Метрики есть, но не отражают риск
- Разные команды видят ситуацию по-разному

Проблемы выявляются слишком поздно

Зависимость от людей

- Ключевые процессы держатся на отдельных сотрудниках
- Знания не зафиксированы
- Работа строится через личные договоренности

Процесс есть, но не устойчив

Архитектура

- Сильная зависимость от одной системы/решения
- Сложные и неочевидные интеграции
- «Временные» решения живут годами

Среда хрупкая и сложная

Непрозрачность операций

- Сложно понять, что именно менялось
- Инциденты повторяются
- Формально всё есть, но нет прозрачности

Контроль не дает полной картины

Внешние зависимости

- Подрядчики влияют на критичные процессы
- Неясно, где и как обрабатываются данные
- Договор есть, контроля нет

Риск частично вне контроля компании

The Institute of Internal Auditors Kazakhstan
ISACA Nur-Sultan Chapter

Red Flags.
Где видно аудитору?

Управляемость

- оргструктура / RACI (кто владелец ИС/риска)
- протоколы комитетов / решения
- реестр ИС/сервисов (назначение ответственных)

Зависимость от людей

- отсутствие runbooks/базы знаний
- нет дублёров / «ключевой человек» в интервью
- ручные операции в критичных задачах

Непрозрачность операций

- история заявок/операций (кто-что-когда)
- RCA по инцидентам, повторяемость
- расхождение «регламент vs реальность» по интервью/выборкам

Наблюдаемость

- покрытие логированием/мониторингом критичных компонентов
- отчёты SOC/тренды инцидентов
- качество алертов (шум vs критичные сигналы)

Архитектура

- архитектурные схемы/карта интеграций (или их отсутствие)
- «temporary fixes/костыли» в исключениях
- частые обходные процедуры при сбоях

Внешние зависимости

- SLA/OLA/DPA, условия по инцидентам и логам
- фактические доступы подрядчиков (в т.ч. prod) + ревизии
- результаты оценок/опросников поставщиков

Как Red flags превращаются в риск

Один Red Flag — это сигнал
Несколько Red Flags — это уже риск

Данные + доступы + подрядчики

риск утечки или злоупотребления

Изменения + непрозрачность + ручные действия

риск ошибок и инцидентов

Зависимость от людей + сложная среда

риск потери контроля

Слабая наблюдаемость + критичные процессы

риск позднего обнаружения проблемы

Риск формируется на пересечении факторов, а не внутри одного процесса

Что это меняет в подходе аудитора

Если риск формируется как комбинация факторов аудит не может оставаться:

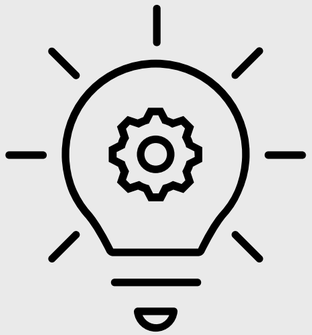
- строго по процессам
- строго по чеклисту
- строго по стандартным областям

Это требует другого подхода

- Смотреть на пересечения процессов и зон ответственности
- Анализировать сценарии, а не только контроли
- Выходить за рамки формального скоупа
- Углубляться там, где есть концентрация сигналов

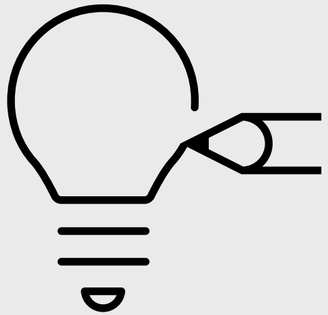
Чеклист не всему «голова»

Невозможно всегда и везде использовать стандартные методы



Чеклисты

- Помогают покрыть базу
- Структурированную проверку
- Покрытие базовых контролей
- Сопоставимость аудитов



Ограничение чеклистов

- Проверяют наличие, но не всегда эффективность
- Оценивают контроли по отдельности
- Не учитывают контекст и архитектуру
- Не показывают комбинации факторов риска

Как выбрать?

4 ориентира для аудитора

Влияние на бизнес

насколько критичен процесс или система

Концентрация сигналов (Red Flags)

сколько факторов сходится в одной зоне

Вероятность сбоя или инцидента

насколько «реалистичен» сценарий

Неопределенность / отсутствие прозрачности

насколько мы понимаем, как это работает

3 простых шага

Для определения фокуса проверки

Шаг 1 – Ищем зону риска

Ищите, где сходятся:

- критичные процессы или данные
- доступы (особенно расширенные)
- изменения
- внешние участники

это кандидаты в скоуп

Шаг 2 — Проверяем понимание

Задайте 3 вопроса:

- Что произойдет при сбое?
- Как быстро это обнаружат?
- Кто и как это контролирует?

Шаг 3 — Обращаем внимание на ответы

Сигналы риска:

- «нужно уточнить»
- «этим занимается другой отдел»
- «в целом работает»

это приоритет аудита

Кейс: Capital One 2019

Когда контроли есть, но риск реализуется

Контекст

- Крупный банк (США)
- Активное использование cloud (AWS)
- Хранение персональных и финансовых данных клиентов

Что было «нормально»

- Использовалась облачная инфраструктура с базовыми контролями
- Были процессы управления доступом
- Были механизмы логирования и мониторинга
- Проверка контролей по SOX

Что случилось?

- Злоумышленник получил доступ через ошибку в конфигурации
- Дальше использовал расширенные права внутри среды
- Получил доступ к данным ~100 млн клиентов

Что не учли

- Cloud среда (сложная архитектура)
- Недостаточный контроль взаимодействия компонентов (Компоненты системы доверяли друг другу)
- Неправильная конфигурация доступа, сервис имел доступ шире, чем нужно
- Логи были, но не предотвратили инцидент

Кейс: Capital One 2019

Когда контроли есть, но риск реализуется

Что делали аудиторы

Проверили:

- Есть ли управление доступами -> да
- Есть ли cloud-политики -> да
- Есть ли логирование -> да

Все - ОК

Что надо было сделать

- Как сервис получает доступы
- Насколько они ограничены
- Что произойдет при компрометации
- Какие данные доступны через этот доступ

Кейс: CrowdStrike 2024

Когда “правильный” процесс приводит к глобальному сбою

Контекст

- Критичное защитное ПО (EDR)
- Широко используется в инфраструктуре
- Автоматические обновления

Что было «нормально»

- Контроли и процессы существовали
- Обновления применялись как требуется

Что случилось?

- Выпущено обновление с ошибкой
- Массовый сбой систем (Windows не запускается)
- Остановлены ключевые бизнес-процессы

Что не учли

- зависимости от одного решения
- автоматическом rollout
- отсутствии локального контроля

Кейс: CrowdStrike 2024

Когда “правильный” процесс приводит к глобальному сбою

Что делали аудиторы

Проверили:

- Используется ли защитное решение -> да
- Обновляется ли система -> да
- Есть ли договор с поставщиком -> да

Все - ОК

Что надо было сделать

- Насколько критична зависимость от решения?
- Как контролируется распространение обновлений?
- Можно ли остановить или ограничить rollout?
- Что произойдет при сбое (fallback / recovery)?
- Есть ли сценарии отказа и их тестирование?

Что в итоге смотреть аудитору

Где формируется риск

пересечения процессов
взаимодействие систем и команд
точки концентрации факторов

Связи между элементами

как процессы влияют друг на друга
где возможен «эффект домино»

Что произойдет при сбое

сценарии отказа
влияние на бизнес
готовность к восстановлению

Какой уровень прозрачности

насколько мы понимаем, что происходит
где есть «слепые зоны»
Кто и как реально контролирует в операционке

Где границы контроля

что мы контролируем
что зависит от третьих сторон
где контроль ограничен

Чаще всего проблема не в:

- глубине проверки
- наличии контролей
- используемых методах

А в том как определялся скоуп:

Так как риск формируется как результат взаимодействия процессов, систем и людей,

а аудит часто рассматривает его изолированно

Где чаще всего возникает ошибка в аудите?

Не ищите там, где светло

Скоуп определяется риском, а не удобством тестирования

Вопросы и ответы

Q & A

The Institute of Internal Auditors Kazakhstan

ISACA Nur-Sultan Chapter