HOW TO: Как спроектировать контроль, который действительно работает

1. Определи цель контроля (Purpose)

Контроль должен чётко отвечать на вопрос: *что именно мы предотвращаем или выявляем?*

Пример: предотвращение подписания договоров сверх утверждённого лимита бюджета.

Без ясной цели контроль теряет смысл

2. Формула WHO- WHAT - WHEN - HOW

Это основа любого эффективного контроля.

Элемент	Вопрос	Пример
WHO	Кто выполняет и кто проверяет?	Контролер по закупкам выполняет, менеджер по бюджету утверждает
WHAT	Что именно проверяется?	Сумма договора против утвержденного лимита
WHEN	Когда выполняется контроль?	До подписания договора
HOW	Как выполняется контроль?	Через SAP-отчет и подтверждение в workflow

3. Ответственные и исполнители (Accountability & Capability)

- Определи, кто ответственный (Accountable) и кто исполнитель (Responsible).
- Проверь, чтобы у исполнителя были доступы, знания и навыки для выполнения контроля.
- Зафиксируй это в RACI-матрице или в процедуре.
  Пример: *Procurement Controller - Responsible, Finance Manager -Accountable.*

4. Информация, используемая компанией (IUC - Information Used by the Company)

Даже идеально описанный контроль не будет работать, если основа - данные, ненадёжна.

IUC - это информация, на которую опирается компания при выполнении или подтверждении контроля.
Примеры: отчёты SAP, выгрузки из BW, Excel-файлы, BI-дэшборды.

Как правильно включить IUC в дизайн контроля:

1. Определи источник данных:
   – из какой системы, отчета или файла берётся информация;
   – кто готовит отчёт и кто владеет данными.

2. Проверь качество данных (Data Quality):
   ☑ Полнота - все транзакции учтены
   ☑ Точность - нет ручных корректировок
   ☑ Своевременность - актуальный период
   ☑ Авторизация - отчет получен из утвержденного источника

3. Документируй IUC:
   - укажи название отчета, путь, параметры фильтрации;
   - сохрани метаданные (дата выгрузки, имя пользователя, период);
   - зафиксируй это как часть доказательства выполнения контроля.

5. Доказательства и документирование (Evidence & Documentation)

Контроль без доказательств = контроль, которого не было.
- Укажи, какие именно артефакты подтверждают выполнение (отчёт, скрин, подпись).
- Определи, где хранить доказательства (SharePoint, SAP, GRC).

– Сделай доступ для проверки (one-click proof).
– Назначь ответственного за сохранность документов.

6. Связь с политиками и процедурами (Policy Reference)
– Каждый контроль должен иметь ссылку на документ, которому он соответствует.

Это повышает осознанность и прозрачность системы контроля.

7. Инструкция (SOP - Standard Operating Procedure)

Разработай краткую пошаговую инструкцию по выполнению контроля:

1. Сформируй SAP-отчет;
2. Проверь лимиты;
3. Сохрани скрин;
4. Загрузите в GRC;
5. Подтверди выполнение.
   – Приложи шаблон отчета и примеры доказательств.
   – Убедись, что SOP доступен исполнителям.

8. Встроенность в процесс (Embeddedness)
Контроль должен быть частью процесса, а не дополнительным шагом.
– Включи контроль в процессную карту, чек-лист или approval workflow.
– Избегай «дополнительных» проверок после факта.
– Если возможно, автоматизируй контроль.
Пример: SAP блокирует договор при превышении лимита - контроль встроен в процесс.

9. Аудитопригодность (Auditability)
Контроль должен быть легко проверяем:
– Должно быть видно: кто, когда, что сделал и чем это подтверждено.
– Вся логика и доказательства должны быть доступны аудитору.
– Контроль должен быть включен в реестр (Control Register) и иметь собственный ID.

10. Разница между процессом и контролем
– Процесс - это поток действий, создающих результат.
– Контроль- это встроенная точка проверки, которая гарантирует достоверность

результата.
Пример:
Процесс - оформление договора.
Контроль - проверка лимита до утверждения.

11. Самопроверка качества контроля (Control Self-Check):

☑ Есть цель
☑ WHO / WHAT / WHEN / HOW определены
☑ Назначены роли
☑ Исполнитель обучен
☑ Есть качественная IUC
☑ Есть доказательства
☑ Есть ссылка на политику
☑ SOP оформлен
☑ Контроль встроен в процесс
☑ Контроль можно проверить

Пример

Процесс: Закупки и договоры
Контроль: Проверка лимитов по Policy

Элемент	Реализация
WHO	Контролер по закупкам
WHAT	Проверка суммы договора vs лимит бюджета
WHEN	До подписания
HOW	SAP отчет ZMC_LIMITS
IUC	Отчет SAP, выгружается автоматически, проверка полноты данных

Evidence	Скриншот и отметка в GRC
Policy	Procurement Policy §4.2
SOP	Contract approval workflow checklist
Audit trail	Хранится в SharePoint
Embeddedness	Проверка встроена в SAP approval flow