

Контрольно-ориентированный аудит

Елизавета Азаренкова



**Елизавета
Азаренкова**
Заместитель
директора
Консалтинг
KPMG Казахстан

+79104084111

elizavetaazarenkov
a@kpmg.kz



— Научно-исследовательский университет Высшая Школа Экономики по специальности Экономика и Информационные технологии.



— Дипломированный внутренний аудитор (CIA);
— Сертифицированный член Института Внутренних Аудиторов.



Общий стаж работы больше 18 в КПМГ и включает следующее:

- Операционные аудиты
- Оценка функции внутреннего аудита на соответствие международным стандартам ВА
- Оценка зрелости системы управления рисками и внутреннего контроля на соответствие международным стандартам
- Подготовка процессов компаний к выходу на биржу
- Разработка и оптимизация внутренних контролей
- Разработка программы экзамена по модулю управление рисками и внутренний контроль
- Оценка процесса корпоративного управления в соответствии с международными стандартами и принципами
- Контроль качества трансформации и/или автоматизации процессов
- Разработка политик и методологий в области внутренних контролей и аудита.
- Проведение семинаров по вопросам внутреннего аудита и внутреннего контроля
- Участие в проектах трансформации процессов
- ИТ аудит, тестирование ИТ контролей
- Аудит финансовой отчетности

Этапы развития СВК в процессах



Легенда

- Единоновременные действия
- Регулярные действия

Пример связи между процессами, рисками и контрольными процедурами

Процесс закупок



Пример выполнения аудита контрольным подходом

Этапы планирования с использованием риск-ориентированного подхода включают:

Цель аудита

Верхнеуровневый анализ процесса

- Общее представление о целях, структуре, ключевых рисках и контрольных процедурах процесса, чтобы определить области с наибольшей значимостью или потенциальной уязвимостью для последующего детального аудита

Выявление рисков и существующих контролей

- Детальный анализ бизнес-процессов и подпроцессов, чтобы определить, что может пойти не так, какие риски существуют и какие контрольные процедуры применяются для их минимизации..

Предварительная оценка рисков и их приоритизация

- Определение уровня присущих и остаточных рисков бизнес-процессов на основе экспертной оценки и доступной информации.

Выбор ключевых рисков и процессов и определение перечня аудиторских процедур

- Исходя из рисков объекта аудита необходимо определить аудиторские процедуры: визуальный обзор документов/систем/записей, пересчет данных, сверка данных, наблюдение за действиями персонала, и т.д.

Функциональный и «сквозной» подход к анализу бизнес-процессов



Существуют два подхода, используемых при дизайне бизнес-процессов

1

Функциональный подход

При использовании функционального подхода выделение процессов происходит на основе специализированных задач, выполняемых **внутри функциональных подразделений организации**, например: Производство, Управление логистикой, Управление финансами, Маркетинг и т.д.

Данный подход к описанию удовлетворяет целям руководителя конкретного функционального подразделения, однако он может не отражать процессы и цели организации в целом, за счет дублирования части типовых шагов и отсутствия стыковки с процессами и задачами других подразделений

2

Сквозной подход

Сквозной подход предполагает выделение процессов, в которых участвуют несколько функциональных подразделений, и направленных на достижение результата и повышение ценности для организации. Сквозной подход позволяет устранить проблемы взаимодействия между различными функциональными подразделениями компании и повысить результативность процесса



Процесс

Совокупность различных видов деятельности, выстроенная в цепочку последовательных шагов и направленная на достижение конечного результата

Функция

Совокупность однородных, специализированных видов деятельности, чаще сосредоточенных в рамках одного структурного подразделения

Примеры процессов

Процесс «Управления Персоналом»



Процесс 1-ого уровня

Процесс 2-ого уровня

Структурное подразделение/
Функция

Процесс «От заключения договора до старта проекта»



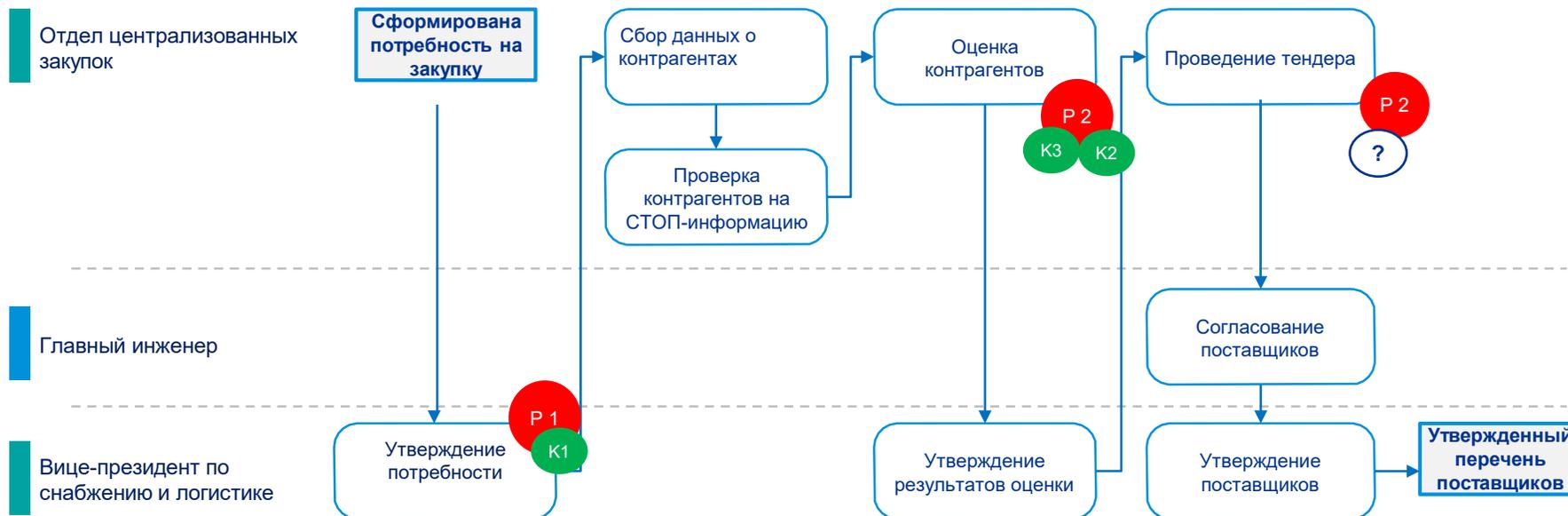
Процесс 1-ого уровня

Процесс 2-ого уровня

Структурное подразделение/
Функция

Пример схемы процесса «Выбор поставщика» с указанием рисков

Участники процесса Процессы 3-го уровня (упрощенная схема)



На этапе планирования анализ бизнес-процесса включает:

- Определить ключевые subprocesses для анализа
- Контролировать полноту объема проверки
- Определить потенциальные зоны риска
- Определить распределение полномочий в процессе



Закупка ТМЦ/услуг без потребности, или в объемах выше реальной потребности



Качество закупки ТМЦ/услуг ниже требуемого уровня



SOD контроль. Согласование потребности проводится несколькими подразделениями – производство, закупки, финансы.



Критерии и процедуры оценки контрагентов формализованы и выполняются для всех закупок категории X.



Проводится проверка благонадежности поставщиков.

Пример

Подпроцесс 2/3/4 уровней Закупки	KPI	Оценка зрелости процесса	Оценка риска X	Запрос менеджмента	Прочие факторы	Включено в периметр тестирования
Планирование	В рамках бюджета	Средний	Не применимо	✓	Процесс вне SAP	✓
Выбор поставщика	Нет/не внедрено	Низкий	Высокий		Процесс не формализован	✓
Договор	Нет/не внедрено	средний	Высокий		Большое количество старых договоров	✓
Заказ	KPI в части аккуратности и своевременности заказов	средний	высокой		Риск дробления заказа	✓
Мониторинг исполнения	KPI по доставке		Средний		В плане тестирования 2018 год	X
Учет, отчетность	н/п		Не применимо			X



Проверку на полноту эффективно выполнить через анализ стандартной карты процесса

Определение процедур проверки

Сквозное тестирование



Примеры сквозных тестов для процесса закупок:

- Тест суб-процесса X от заказа предмета закупки до оплаты (2-3 позиции);
- Тест суб-процесса X от выбора поставщика до заказа (5 позиций по 1 для каждого вида).

Тестирование контрольных процедур



Примеры тестирования контрольных процедур:

- Контроль согласования заказа;
- Контроль 3х-сторонней сверки;
- Контроль приемки товара на склад;
- Контроль согласования и выполнения KPI;
- Выборка XX позиций для каждого вида закупки.

Аналитическая проверка



Примеры критериев аналитической проверки:

- Анализ закупок в сравнении с предыдущим периодом в разрезе поставщиков, анализ отклонений свыше установленного порога;
- Анализ выполнения KPI.

Детальное тестирование операций/транзакций



Примеры детального тестирования операций/транзакций:

- Физическая инвентаризация (проверка наличия и состояния материальных активов);
- Запрос подтверждения операций от третьих сторон;
- Проверка наличия первичной документации по выборке транзакций

Детальное тестирование: этапы оценки контролей



Что такое эффективность дизайна контролей



Эффективность дизайна контроля это

- организация контроля, при которой контроль достигает своей цели, то есть, обеспечивает выявление или предотвращение существенных искажений данных или отклонений от предписанных процедур.



Оценка эффективности дизайна контрольных процедур также позволяет выявить:

- Нарушения принципов разграничения полномочий;
- Некорректное понимание/трактовка цели контроля Исполнителем КП и/или некорректное выполнение демонстрационного примера контроля;
- Частичное закрытие риска текущим контролем;
- Отсутствие следа контроля.



Техники оценки эффективности дизайна контрольных процедур включают:



Повторное исполнение

Проверка доказательств

Наблюдение

Запрос/ Интервью

Примеры недостатков в контрольной процедуре



На этапе оценки дизайна:

- Некорректная трактовка цели контроля Исполнителем КП или дизайна контроля
- Некорректное распределение полномочий для принятия решений. Избыточные полномочия и доступы у руководителей департамента
- Некорректное делегирование полномочий для принятия решений
- Отсутствие требований к критериям проверки в рамках контроля, отсутствие уточнений что делать Исполнителю КП в случае выявления отклонений
- Возможность использовать упрощенный вариант согласования операций
- Описание дизайна контроля покрывает не все необходимые утверждения отчетности/не весь периметр операций. Например, отсутствует подтверждение полноты данных, подлежащих контролю.
- Некорректная трактовка методологии учета или политики, регламентирующей процесс.



На этапе оценки операционной эффективности:

- Отсутствие/несоответствие документов данным учета для позиций из выборки
- Отсутствие ключевых следов контроля
- Существенный отчет, который используется для выполнения контроля, формируется некорректно в системе, отсутствуют механизмы контроля выявить данное отклонение.
- несоответствие маршрута согласования Регламенту. При этом, Исполнитель КП не трактует текущий маршрут, как некорректный.
- Использование неактуальных данных для расчета.
- Хранение нефинальных версий файлов по результатам контроля. При этом, несоответствие возможно выявить только при сверке файла с исходными данными и повторной проверке.

Специфика организации контролей за существенными отчетами

Риск	Описание риска	Возможные контроли
Data input risk	Риск некорректных входящих данных	Контроли за полнотой и корректностью ввода данных в системы (например, контроли двойной авторизации мастер-данных)
Data integrity risk	Риск некорректного формирования отчета (логики отчета)	Контроль за корректностью формирования логики отчета
Data extraction and manipulation risk	Риск некорректной выгрузки и изменений системного отчета	Исполнитель КП проверяет корректность параметров выгрузки отчетов (ИРЕ) и/или сверяет итоговые суммы с первоначальной выгрузкой.

НЕКОРРЕКТНЫЙ отчет, который используется в контроле = НЕЭФФЕКТИВНЫЙ КОНТРОЛЬ!

**Методика
определения
выборки в рамках
аудиторских
заданий**

Методика выборки в рамках аудиторских заданий

При формировании выборки аудитор может применить следующие методы:

- Нестатистическая выборка специфичных позиций (включая вид выборки для целей тестирования контрольных процедур);
- Статистическая выборка;
- Выбор 100% популяции данных.

Внутренний аудитор согласует подход к выборке и размер выборки с руководителем аудиторского задания до начала тестирования. В случае наличия сомнений в правильности выбранного метода для достижения целей аудиторского задания руководитель аудиторского задания может обсудить приемлемость выбранного подхода с руководителем СВА.

Требования к популяции:

- Совокупность данных, из которой производится выборка, должна быть корректной и полной;
- Популяция должна соответствовать целям проверки;
- Период популяции должен быть задокументирован и, если возможно, соответствовать периоду аудита
- Популяция должна содержать однородные элементы, подлежащие тестированию

Нестатистическая выборка – контрольные процедуры

- Выборка для целей тестирования контрольных процедур — это вид нестатистической выборки, который должен использоваться для целей оценки операционной эффективности контрольных процедур за тестируемый период. По результатам оценки аудитор делает вывод «эффективен/неэффективен», т.е. определяет, эффективно ли функционировал контроль за период.
- Размер выборки для целей тестирования операционной эффективности контрольных процедур зависит от следующих факторов:
 - Частота осуществления контрольной процедуры;
 - Тип контрольной процедуры (ручная/ИТ-зависимая или автоматическая).

ЕДИНИЦА контроля	Исполнитель контроля	Дата выполнения контроля	Наличие следа контроля	Сумма резерва согласно проверочному файлу	Сумма данных систем Учета	Разница	Корректность логики расчета	Контроль эффективен?
Расчет резерва за июнь								

Определение размера выборки для ручных контролей

Частота выполнения контрольной процедуры	Минимальный размер выборки	
	Риск ошибки	
	Более низкий	Повышенный
Ежегодно	1	1
Ежеквартально (включая конец периода, то есть +1)	1+1	1+1
Ежемесячно	1-3	2-4
Еженедельно	4-6	7-10
Ежедневно	10-15	25-40
Повторяющийся ручной контроль	20-30	30-60



Подход к идентификации и оценке наблюдений

Стандарт 14.3 «Оценка наблюдений»

«Внутренние аудиторы должны оценить каждое потенциальное наблюдение с точки зрения его существенности. При оценке потенциальных наблюдений внутренние аудиторы должны совместно с руководством выявить первопричины (при возможности), определить возможные последствия и оценить существенность проблемы.

Для определения существенности риска внутренние аудиторы должны рассмотреть вероятность реализации риска и влияние, которое риск может оказать на процессы руководства организацией, управления рисками и внутреннего контроля.

Если внутренние аудиторы определяют, что организация подвергается существенному риску, это должно быть документально оформлено в виде наблюдения и доведено до сведения соответствующих лиц.

Внутренние аудиторы должны решить, следует ли сообщать о других рисках в качестве наблюдений в зависимости от обстоятельств и принятой методологии.

Внутренние аудиторы должны приоритизировать все наблюдения в зависимости от их существенности, в соответствии с принятой руководителем внутреннего аудита методологией.»

Для целей анализа наблюдений используется метод «6 шагов»:

01	Подтверждение наблюдения
02	Выявление первопричин наблюдения (root cause analysis)
03	Определение наличия прочих наблюдений, связанных с уже обнаруженным наблюдением
04	Определение соответствующего компенсирующего контроля
05	Оценка существенности наблюдения с учетом величины вероятности возможной реализации рисков и эффективности компенсирующих контролей
06	Агрегирование схожих наблюдений в обнаружения и оценка их влияния

**Мониторинг
рекомендаций
ВА и проверка
исполнения**

Мониторинг выполнения рекомендаций (1/2)

Стандарт 15.2 «Подтверждение выполнения рекомендаций или планов мероприятий»

«Внутренние аудиторы должны подтверждать выполнение ответственными лицами рекомендаций внутренних аудиторов или планов мероприятий в соответствии с установленной процедурой, которая включает:

- Направления запросов о ходе выполнения.
- Проведение последующих оценок на основе риск-ориентированного подхода.
- Обновление статуса планов мероприятий в системе мониторинга.

Объем данных процедур должен определяться в зависимости от существенности наблюдений. Если руководство не выполнило мероприятия в установленные сроки, внутренние аудиторы должны получить и документировать объяснение руководства, а также обсудить этот вопрос с руководителем внутреннего аудита. Руководитель внутреннего аудита определяет, приняло ли высшее исполнительное руководство, в силу задержки выполнения или бездействия, риск, превышающий уровень толерантности к риску.»

Ежеквартальные шаги мониторинга сотрудником СВА - пример:

- 1 Запрос статуса исполнения плана корректирующих мероприятий и подтверждающей документации у руководства Объекта аудита
- 2 Предоставление статус-файла с обновлениями руководителям аудиторских заданий для подтверждения исполнения плана
- 3 Письменное подтверждение по результатам закрытия статуса после получения подтверждения от руководителя аудиторского задания
- 4 Обновление статус-файла с результатами мониторинга для последующей проверки и подготовки отчетности для Комитета по Аудиту и высшего руководства



При задержке внедрения рекомендаций

Ответственный сотрудник СВА запрашивает объяснение у руководства Объекта аудита и обсуждает его с руководителем аудиторского задания. Если причины объективны — срок может быть продлён по согласованию с Руководителем СВА. В иных случаях проводится анализ, превышают ли риски допустимый уровень.

Оценка зрелости СУРиВК

Пример вывода по оценке СУРиВК

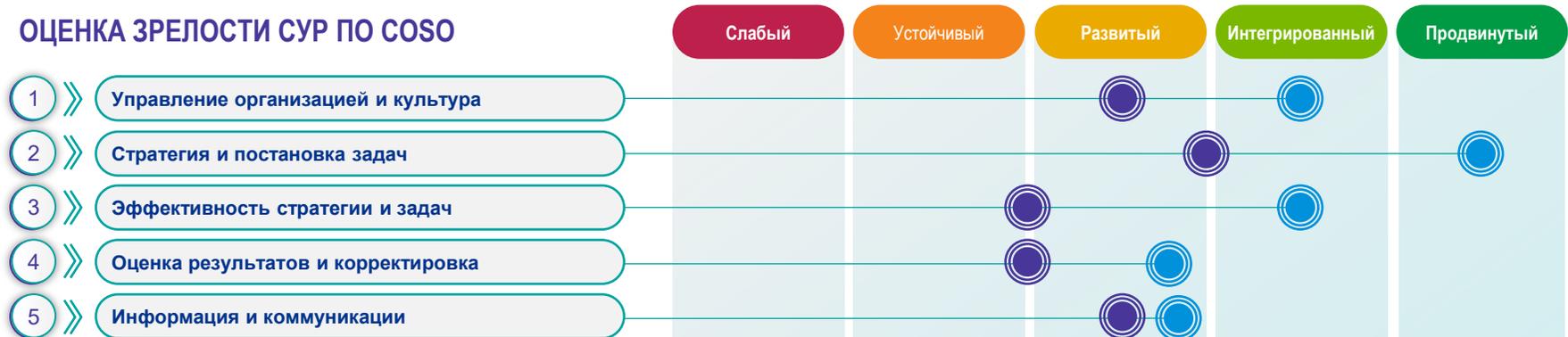
СУРиСВК в целом соответствует основным международным, применимым методологическим документам (COSO (ERM, IC), ISO31000) и **функционируют в целом эффективно**, но необходимы отдельные улучшения их компонентов.

Орг единица 1 уровни зрелости: СУР **«Развитый»**, СВК **«Устойчивый»**, СУРиВК* **«Развитый»**

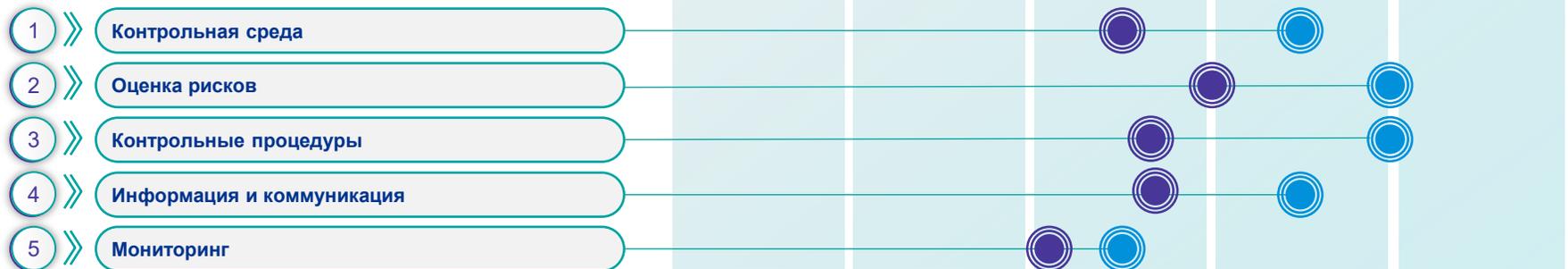
Орг единица 2 уровни зрелости: СУР **«Интегрированный»**, СВК **«Интегрированный»**, СУРиВК* **«Интегрированный»**

* Комплексная система управления рисками и внутреннего контроля.

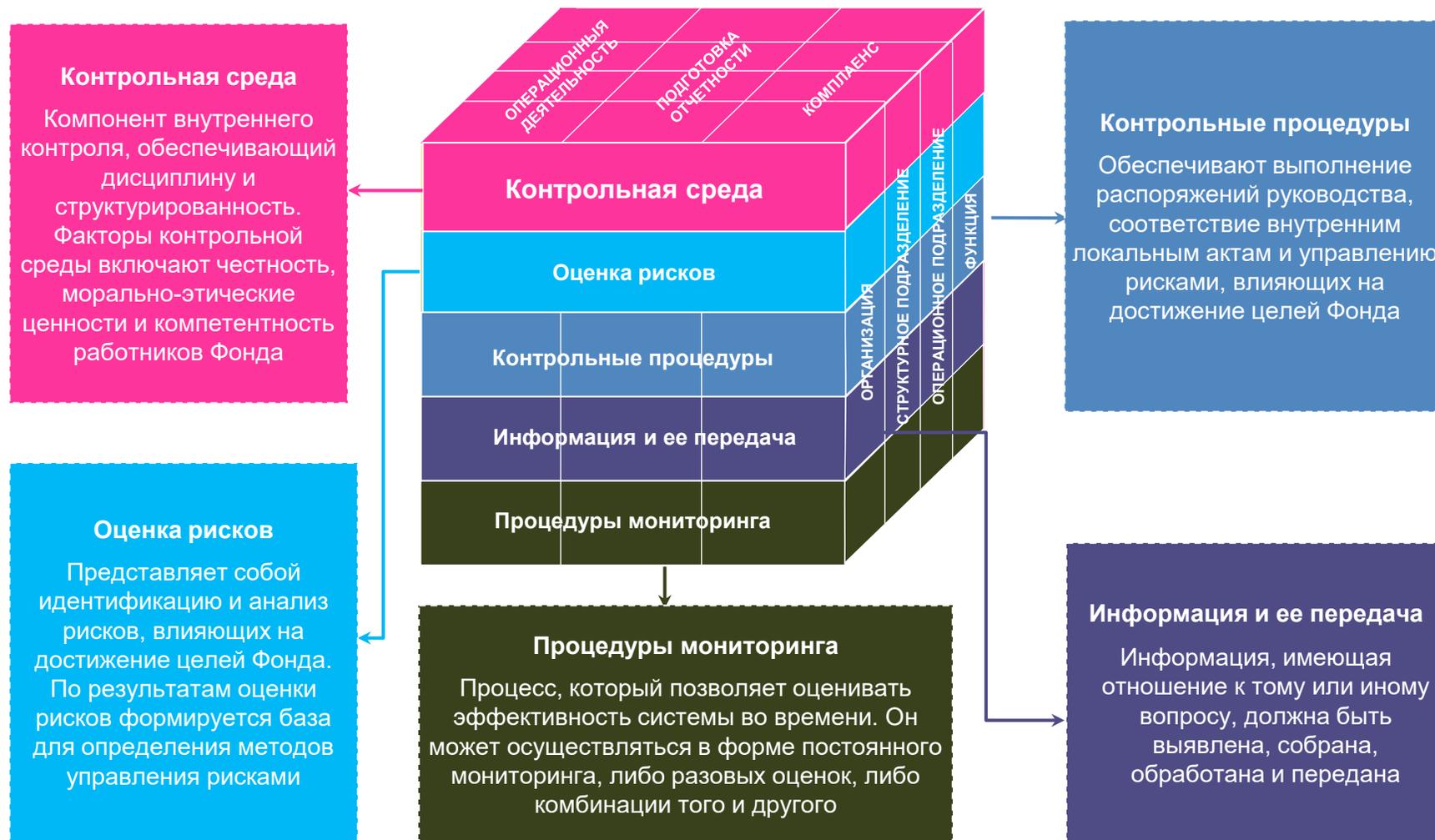
ОЦЕНКА ЗРЕЛОСТИ СУР ПО COSO



ОЦЕНКА ЗРЕЛОСТИ СВК ПО COSO



Модель COSO «Внутренний контроль - Интегрированная модель»



Пример работы контролей в общей системе

Пример контроля приемки услуг по договору:

- Цель: Обоснованная оплата по закупке услуг



Спасибо за внимание!

