Роль решений SAP GRC AC и SAP GRC PC, RM в процессе оптимизации внутреннего контроля

Андрей Нифатов
менеджер по развитию бизнеса

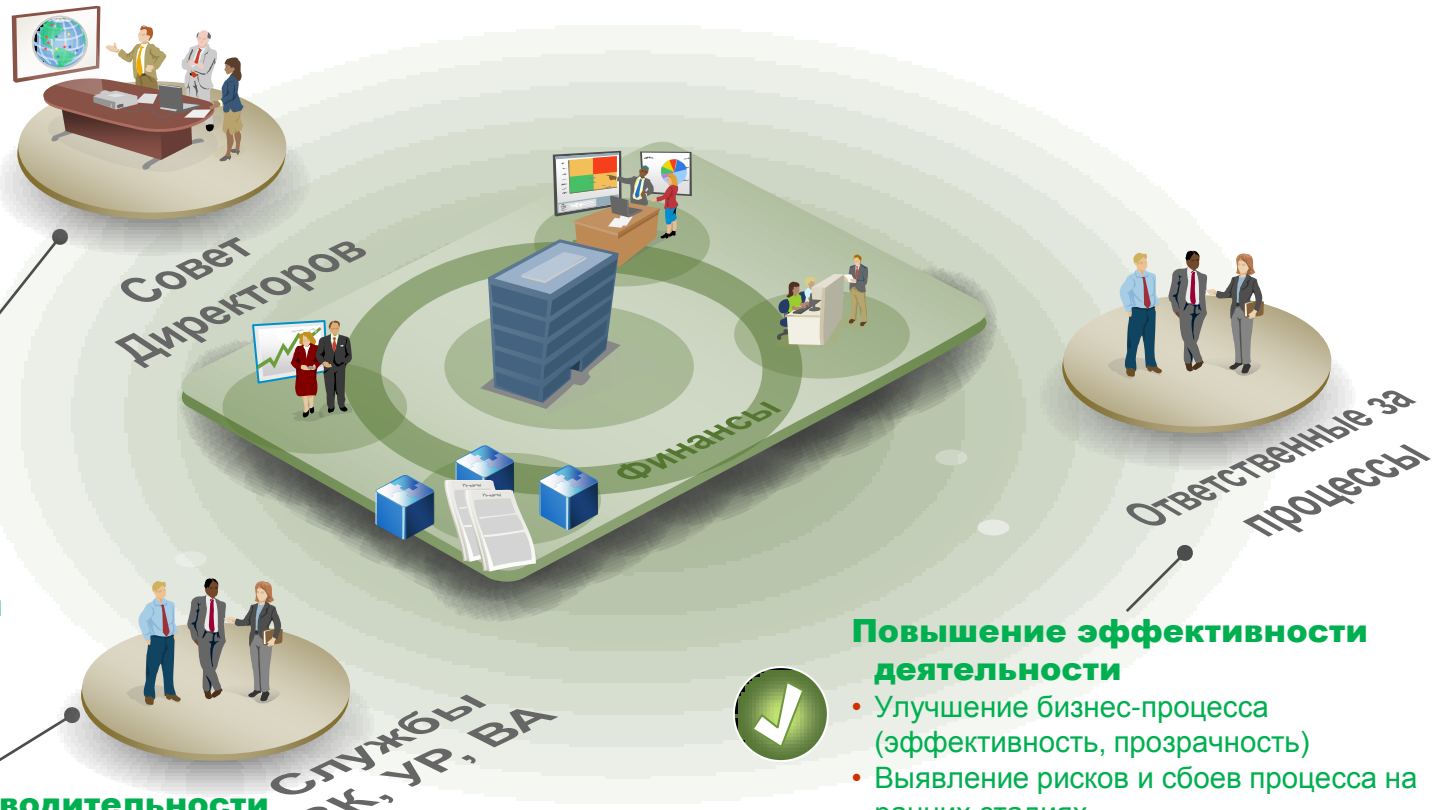
Решение по управлению рисками и соответствию требованиям SAP Governance, Risk & Compliance позволяет:

“выявить и управлять рисками, выявить хищения, слабые места, ошибки, нарушение политик, мошенничество и другие недостатки бизнес-процессов“

“ обеспечить комплексный подход”

“создать уверенность в достижении целей”

Ожидаемые выгоды бизнеса от использования СВК (на разных уровнях организации)



Повышение прозрачности организации

Инвестиционная привлекательность (IPO, Иностранный инвестор, другие виды инвестиций)

- Анализ воздействия рисков в реальном времени
- Анализ влияния рисков на цели и бизнес планы
- Классификация рисков по бизнес процессам и направлениям деятельности

Повышение производительности

- Электронный документооборот по оценке рисков, эффективности реакций и контролей
- Непрерывный мониторинг (проверка)
- Масштабируемая поддержка соблюдения множественных требований (внутренние и регуляторов, отраслевые)

Повышение эффективности деятельности

- Улучшение бизнес-процесса (эффективность, прозрачность)
- Выявление рисков и сбоев процесса на ранних стадиях
- Акцент внимания руководителя, только там и тогда, когда это нужно
- Эффективная работа с удаленными подразделениями

Централизованный подход к решению задач корпоративного управления рисками

Централизованный подход к решению задач корпоративного управления, управления рисками, соблюдения законодательных норм повысит эффективность управления за счет проактивного снижения рисков

Служба по управлению рисками

- Уверенность в достижении поставленных целей
- Выявление и снижение рисков по направлениям бизнеса
- Оперативное принятие решений с учетом информации по возможным сценариям развития

Служба Внутреннего контроля, аудита

- Корпоративная ответственность
- Прозрачность системы контроля
- Риск-ориентированность системы контроля
- Снижение затрат на тестирование и мониторинг

Служба Безопасности

- Предотвращение несанкционированного доступа и утечек
- Мониторинг конфликта интересов
- Безопасные контрагенты
- Оптимальные цены

Решение по управлению рисками SAP Risk Management

Мониторинг

Мониторинг риска и отчетность

Отчеты

Реагируй

Реакция на риск

Реакции

Смотреть
Принять
Перенос
....

Контроли

ЛНД

Анализируй

Анализ рисков

Групповая оценка

Выявляй

Выявление рисков

Оценка

Планируй

Документирование

Служб, Процессов, Рисков,, …

Контекста

Ключевые индикаторы риска
(Стандартный контент)

Финансы

- Перерасход бюджета
- Анализ открытой валютной позиции на текущий день
- Анализ кредитного риска покупателя
- Анализ дебиторской задолженности

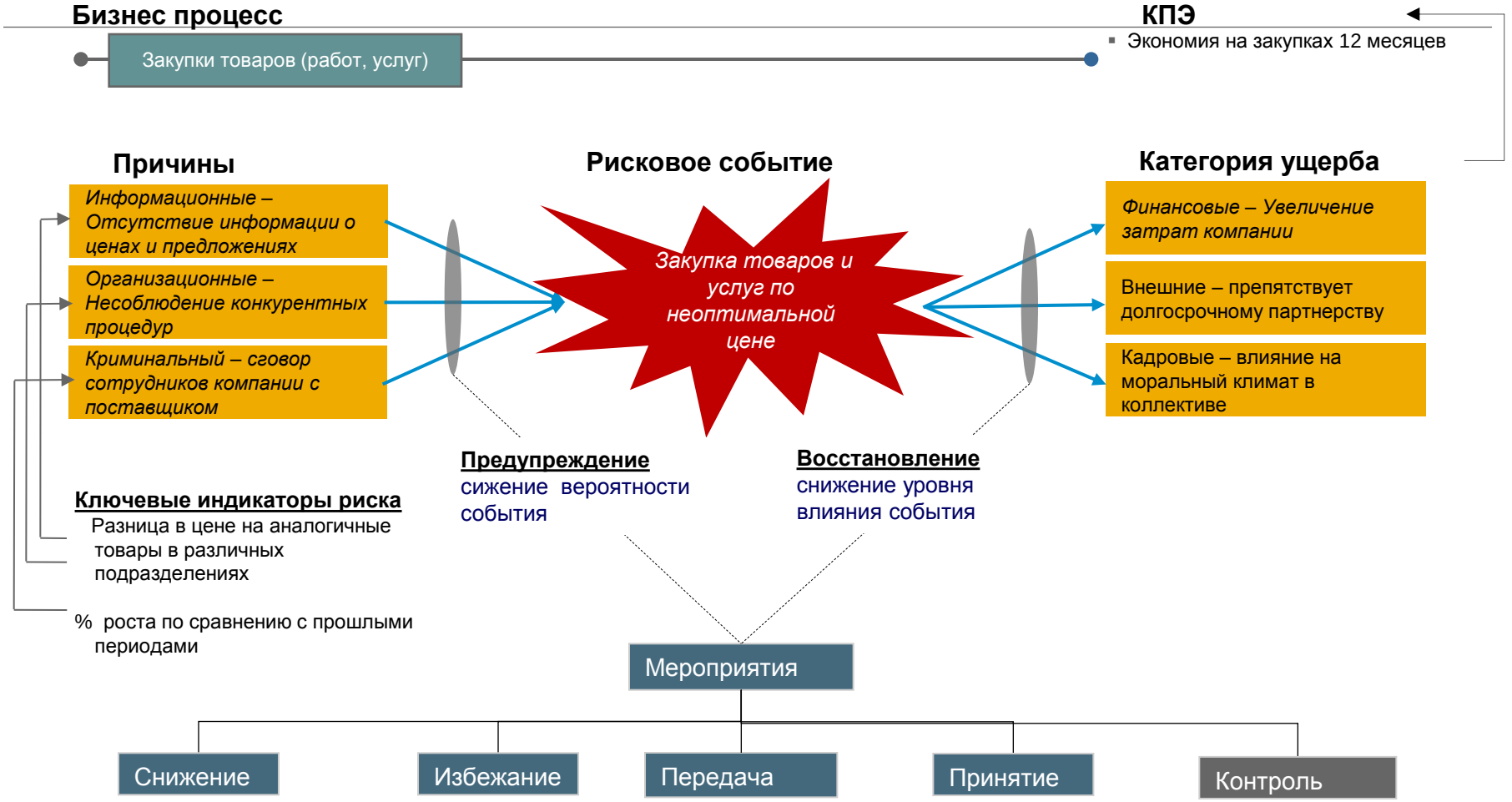
Закупка товаров и услуг

- Проверка отклонения цены в счете фактуре по сравнению с заказом на закупку
- Проверка отклонения количества закупаемого товара и накладной, заказом на закупку и накладной
- Проверка на расхождения в дате поставки
- Динамика изменения цен за последние три месяца
- Закупка без контракта
- ...
- Возвраты готовой продукции
- Текучка кадров

Примеры бизнес сценария

Формализация основных характеристик риска

Пример – *Закупка товаров или услуг по неоптимальной цене*



- Централизация закупок на основе электронных процедур. Единый справочник товаров и услуг
- Мониторинг рыночных цен
- Анализ КПЭ поставщиков

- Аутсорсинг

- Контроль тендерных процедур
- Контроль регламента заключения договоров

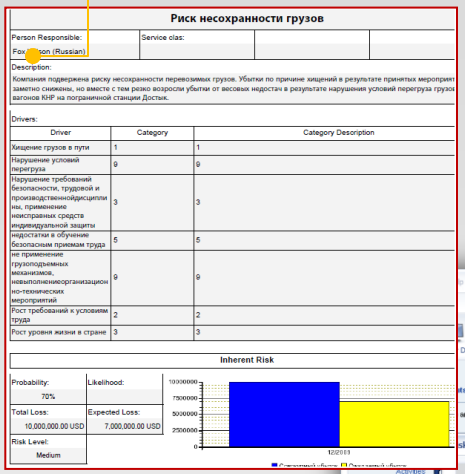
Отчетность и аналитика – примеры встроенных отчетов

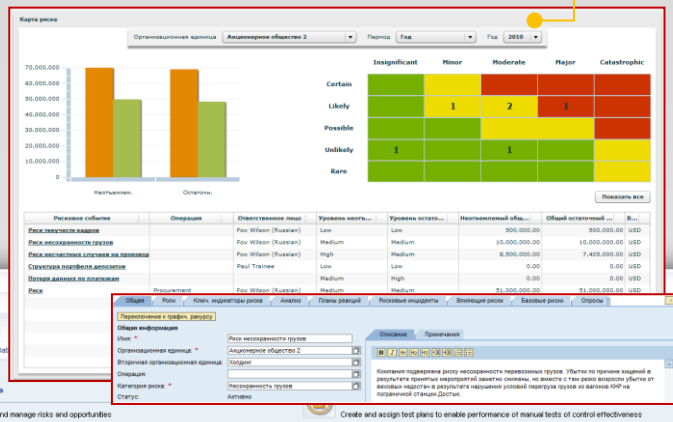
Актуальная информация по рискам для принятия решений

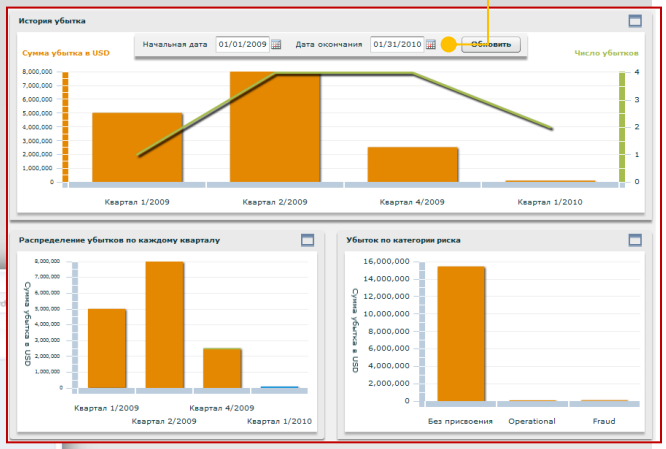
Опросы по рискам

«Тепловая карта», доступ к детальным данным

Статистика по инцидентам







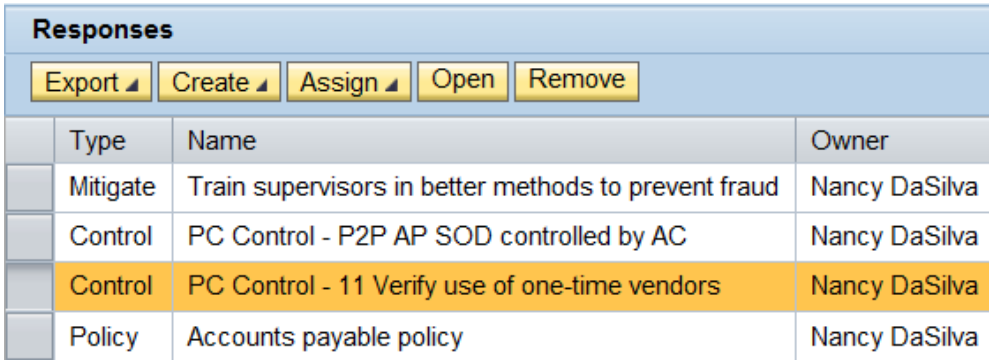
Групповая оценка риска

Экспертная оценка риска

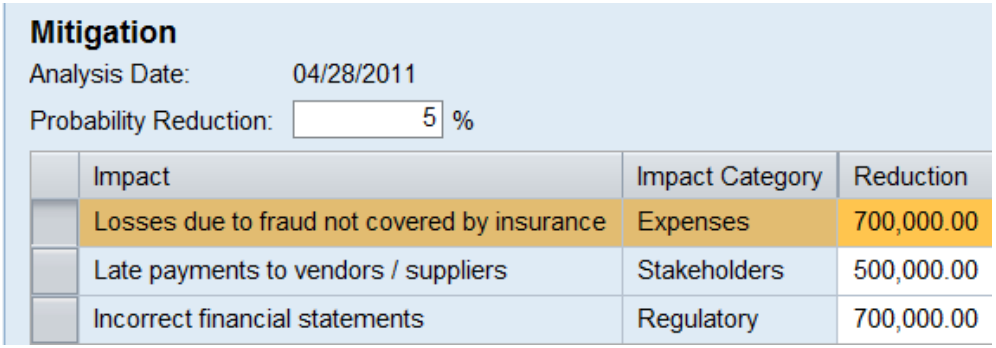
Консолидированная оценка

Возможности SAP GRC Risk Management

- **Вы можете присваивать контроли из библиотеки GRC Process Control, политики, другие мероприятия в качестве реакции на риск**



- **Оценить эффективность реакции на риск для определения плановой и остаточной величины риска**



- **Оценить снижение риска по результатам полноты и эффективности назначенного контроля SAP Process Control**

Условия работы службы аудита и внутреннего контроля

- **Никто не хочет тратить больше на аудит и внутренний контроль**
- **Правила контроля усложняются, как правило, без соответствующего увеличения объема ресурсов**
- **Появились новые бизнес-риски, но многие в компании по-прежнему "смотрят в зеркало заднего вида"**
- **Организационные изменения продолжают бросать новые вызовы изменения бизнес-процессов и их связей**

Ключ к успеху

Фокус на том, что наиболее существенно

- Необходимо понимать существенные риски и дублирующие контроли
- Не нужно тратить время на документирование и тестирование несущественных контролей
- Используйте стратегию оценки существенности риска и его покрытие контролями

Унифицируй и стандартизуй там, где это возможно

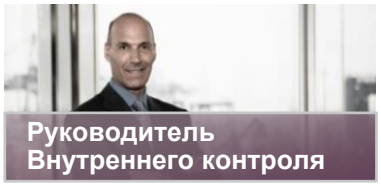
- Унифицируйте структуру процессов и контролей релевантные множеству организаций, инициатив, регулирований
- Балансируй между централизацией и возможностями локального изменения централизованных контролей

Используй автоматическое тестирование и мониторинга контрольных процедур

- Максимизируй использование автоматизированных контролей и процессов work-flow
- Необходимо пересмотреть методику тестирования для полностью ручных контролей, в пользу частичной или полной автоматизации тестирования и мониторинга

SAP Process Control

Ключевые возможности



Legacy Apps

PeopleSoft

greenlight

SAP

JDEDWARDS

ORACLE

Отчетность

Отчетность

Контроль

Мониторинг и
контроль исполнения

Оценка

Автоматич.
провека

Проверка
В ручную

Объем

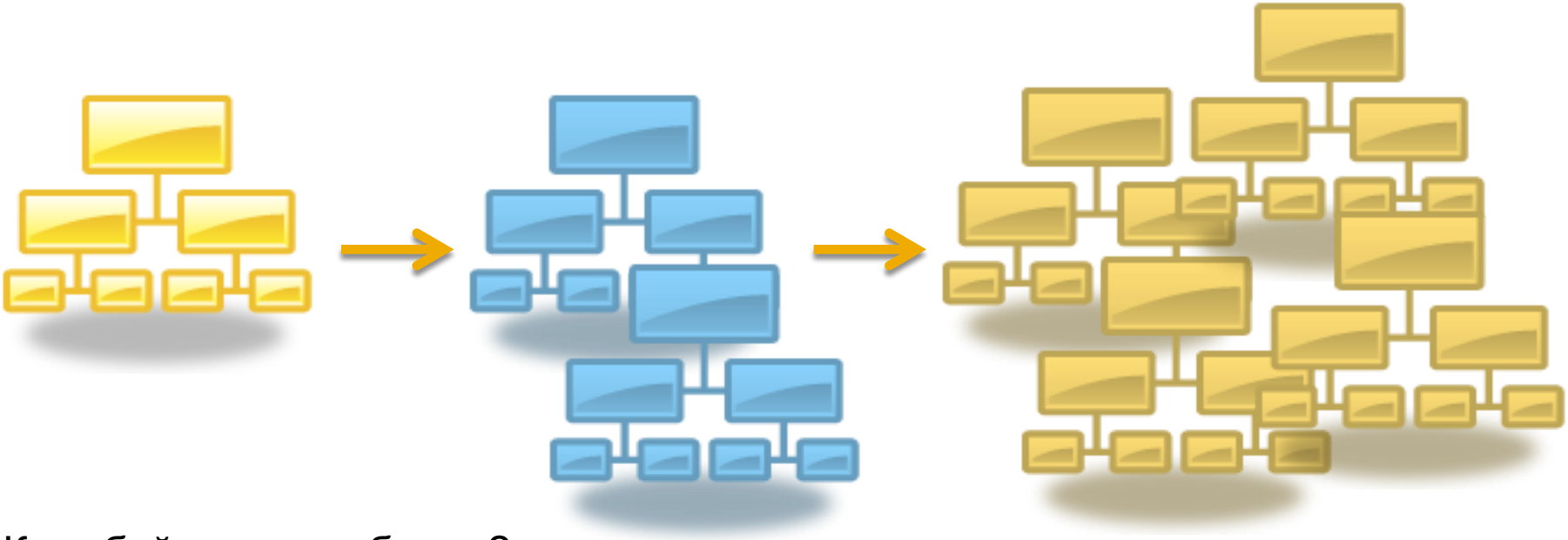
Формирование объема (scoping)
Риск-ориентированный
Внутренний контроль

Докум.

Документирование
Подразделений, Процессов,
Рисков, Контролей, …

Политики

Популяция контролей становится все больше и больше и ей все сложнее управлять



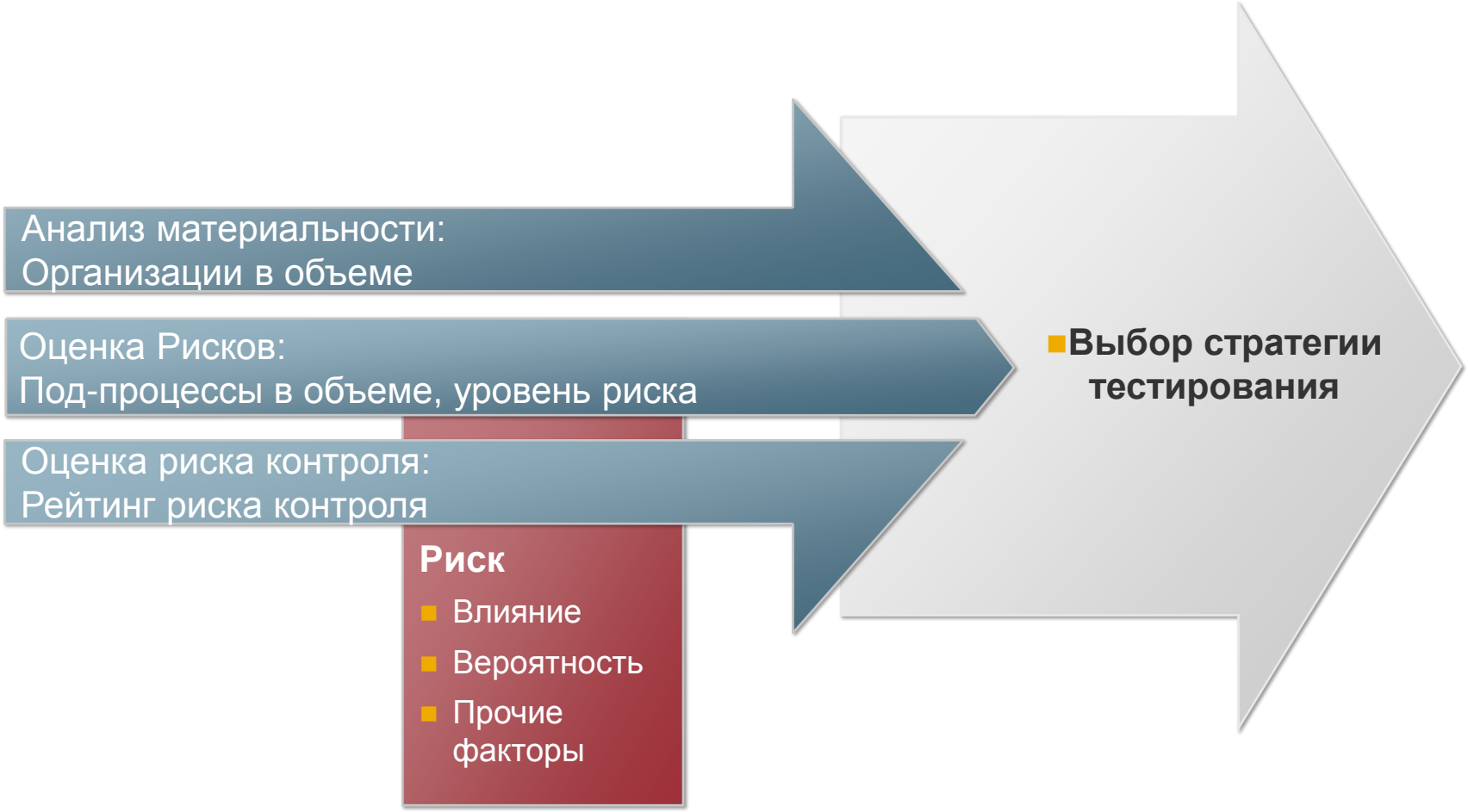
Как обойти эту проблему?:

- Управление значимыми контрольными процедурами
- Централизация ведения контрольных процедур и возможность их использования для любой организации и инициативы (регулирования)
- Используйте преимущества функциональности контролей корпоративного уровня

Как Process Control поможет вам?

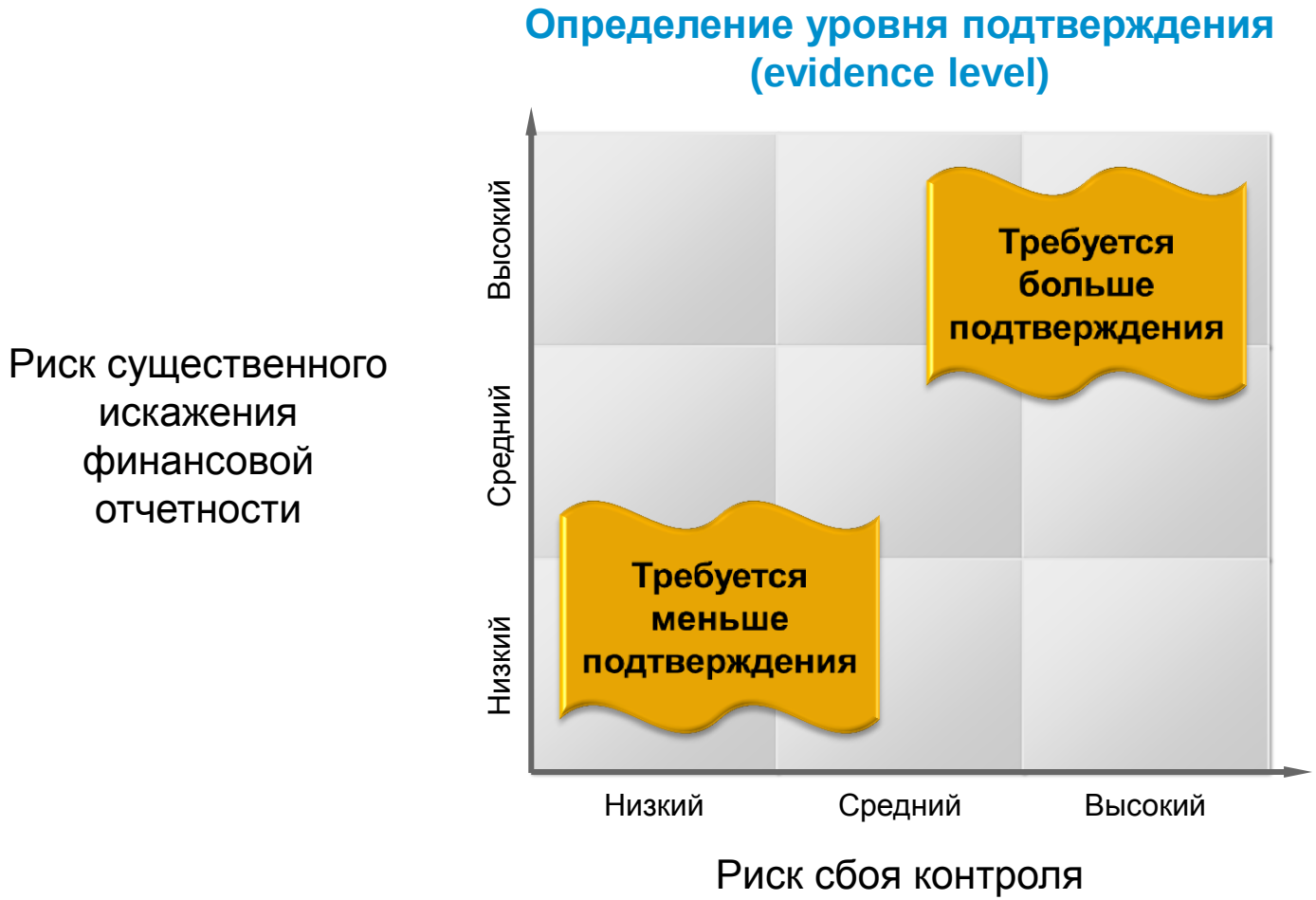
Возможности	Эффекты
1. Единая структура процессов (бизнес процессов, под-процессов, рисков, контролей)	1. Стандартизация и унификация контролей
2. Поддержка нескольких регулирований для целей документирования, оценки, составления отчетности	2. Позволяет разделение общей документации между разными регулированиями
3. Присвоение процессов и контролей с возможностью централизованного, локального и смешенного типа ведения данных	3. Помогает балансировать уровнем централизации и возможностью локального изменения данных
4. Возможность документирования и оценки контролей уровня бизнес-процесса и корпоративного уровня	4. Позволяет покрыть большое кол-во рисков не снижая эффективность
5. Поддержка Общего центра обслуживания бизнеса	5. Обеспечивает ОЦО необходимой отчетностью для всех организаций

Риск ориентированный подход к построению системы внутренних контролей (RBIC), формирование объема



Каждый из этих шагов опционален в соответствии с бизнес-требованиями

Определение уровня подтверждения (evidence level) (с целью достоверности финансовой отчетности)



Source: SEC Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting, June 20, 2007

Что контролировать?

Направления контроля

- Контроль материального учета (включая управление неликвидами)
- Ремонты ТОиР и инвестиции
- Закупки \ Продажи
- Договора
- Система бюджетирования

Выгоды

- Регулярный контроль позволит высвободить оборотный капитал
- Начиная с определенного возраста оборудования срок окупаемости его замены значительно сокращается
- Экономия на закупках за счет плановых закупок

Выявить системные нарушения -> изменение бизнес процесса и существующих процедур

Формирование корпоративной культуры

Внутренний контроль ФХД (Пример: автоматическая проверка декларации до сдачи в ФНС)

- Обеспечение инвестиционной привлекательности
  - Полное отражение выручки
  - Переоценка активов
  - Минимизация налоговых рисков
- Эффективность схемы
  - Отсутствие переплаты налогов
  - Потеря ликвидности

Пример автоматического налогового контроля в SAP GRC

Формула	Значения	Показатели	
ст. 2300 Чистая прибыль (убыток) ОФР < 0	2445,81 > 0	ст. 2300 ОФР - прибыль (убыток) до налогообложения	Отражение в бухгалтерской отчетности убытков на протяжении нескольких налоговых периодов (2 или более года)	Если организация отражает в бухгалтерской отчетности убытки на протяжении двух лет или более, то существует риск занижения налоговой базы по ННП. Однако если убытки отражены только в финансовой отчетности, а в декларации по ННП отражается прибыль, налоговый риск значительно ниже

Контроль закупок товаров и услуг (автоматический мониторинг)

- Выявить дублирование счетов на оплату
- Найти документы без ссылки на документы оригиналы
- Показать исходящие платежи на большую сумму сделанные за последние 60 дней
- Найти исходящие платежи где адрес плательщика или данные банка могут быть изменены в процессе выполнения платежей
- Найти поставщиков и сотрудников имеющие один счет на оплату
- Показать поставщиков, которые помечены для удаления но еще не блокированы
- Показать поставщиков для которых в условиях платежа «немедленный платеж»
- Показать поставщиков для которых метод платежа «наличный расчет»
- Мониторинг изменений ключевых данных поставщиков «альтернативный плательщик»
- Выявление случаев когда сумма в заявке на закупку меньше, чем в накладная
- Найти заявки на закупку, которые были созданы в один день с поступлением товара
- Выявить закупки, которые не были согласованы
- Выявить случаи расхождения закупаемого количества в связанных документах на закупку
- ...

SAP Access Control
Предотвращение рисков доступа при помощи распределения полномочий «защита от дурака»

Уменьшение времени на соответствие	*Постоянный мониторинг доступа*	*Отчеты для Руководства и аудита*
Вычистка	*Поддержание заданного уровня*	*Контроль*

Анализ рисков доступа

Быстрая вычистка, с минимальными затратами

Управление ролями

Проверка SoD при создании и изменении ролей

Электронные заявки на доступ Предотвращение SoD во время предоставления доступа

Расширенные права доступа Позволяет предоставить расширенный доступ

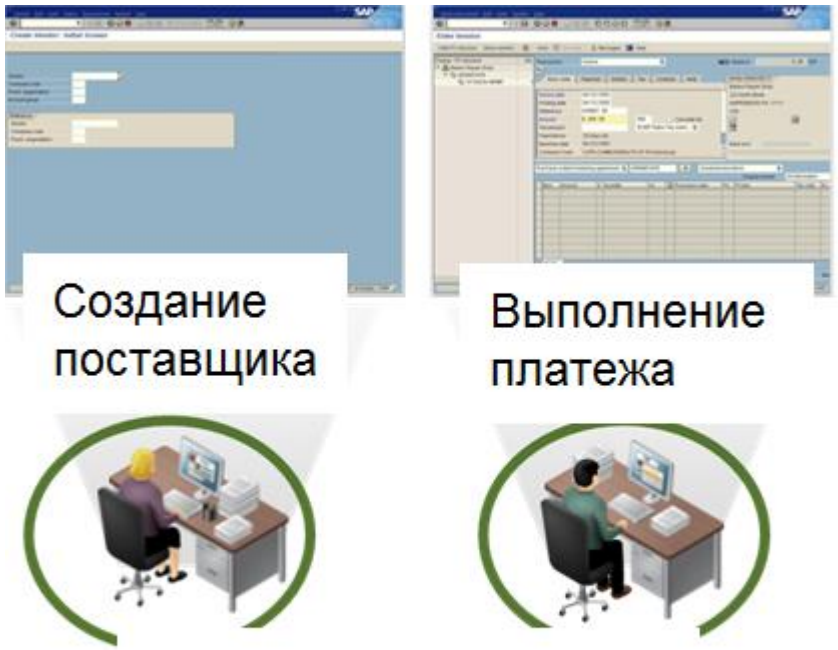
Периодический мониторинг и аудит

Фокус на постоянное совершенствование

Анализ рисков и планирование мероприятий по их снижению

Матрица конфликтов доступа предоставлена компанией аудитором PWC

Предотвращение рисков противоправных действий на примере процесса закупки



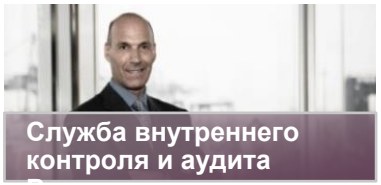
Драйвер риска:
Отсутствие SoD

Предотвращение рисков противоправных действий на примере процесса закупки

Предотвращение мошенничества в процессе закупки

Access Control

Предотвращение рисков противоправных действий на примере процесса закупки

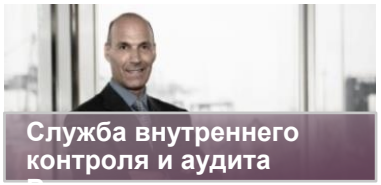


Пример угрозы: «Злоупотребления разовыми платежами»!!!

Контроли процесса: Закупки

Общие ИТ контроли: Access Control

Предотвращение рисков противоправных действий на примере процесса закупки

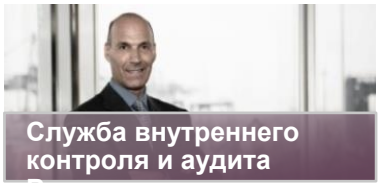


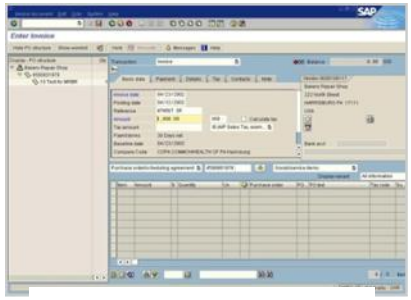
Вопрос:

Являются ли конфликты SoD единственным риском процесса ???

Общие ИТ контроли: Access Control

Предотвращение рисков противоправных действий на примере процесса закупки





Платежи поставщику

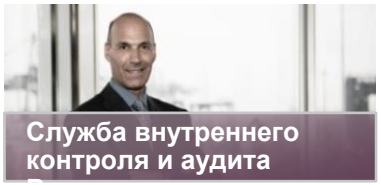
Платежи		
Дата	Поставщик	Сумма
1.10.	ABC Chemicals	1,599.-
2.10.	Anonymous1	1,000.-
2.10.	Northstar Energy	563.-
5.10.	Anonymous1	10,000.-
9.10.	Hardware Central	23,61

Пример:
Угроза “платеж разовому поставщику”
???

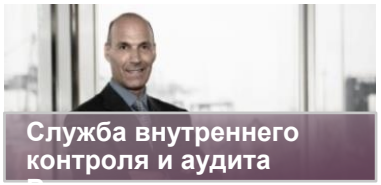
Контроль разовых платежей

ИТ общие контроли: Access Control

Предотвращение рисков противоправных действий на примере процесса закупки



Предотвращение рисков противоправных действий на примере процесса закупки

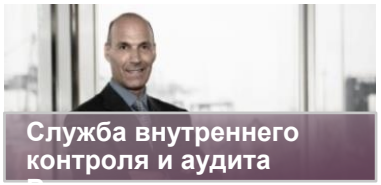


Контроли уровня **Процесса и Доступа защита всего процесса**

Контроли БП: Закупки

Общие контроли: Access Control

Другие риски?
В других процессах?



Если речь идет о рисках других процессов?

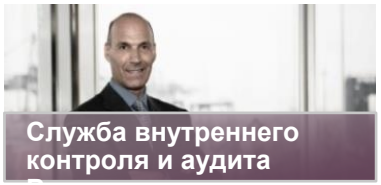
Процесс 1: Закупки

Процесс n: Казначейство

Общие ИТ Контроль 1: Access Control

Общие ИТ Контроль n

Другие риски?
В других процессах?



Группы/Корпорации: Контроли уровня компании

Группы/Корпорации: Контроли уровня компании

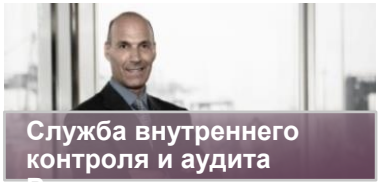
Процесс 1: Закупки

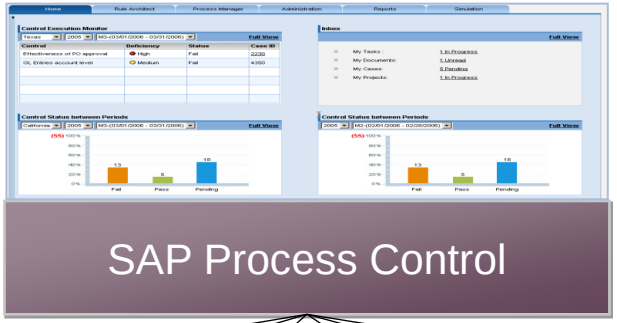
Процесс n: Казначейство

Общие ИТ Контроль 1: Access Control

ИТ контроль n: (ИТ Общие)

SAP Process Control
Контроль на всех уровнях





Группы/Корпорации: Контроли уровня компании

Группы/Корпорации: Контроли уровня компании

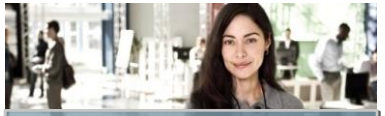
Процесс 1: Закупки

Процесс n: Казначейство

Общие ИТ Контроль 1: Access Control

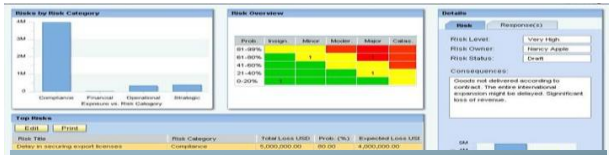
ИТ контроль n: (ИТ Общие)

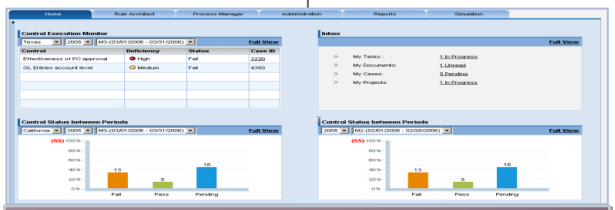
Риск-ориентированный подход


Служба по управлению рисками


Служба Внутреннего контроля


Служба Безопасности


SAP Risk Management


SAP Process Control

Группы/Корпорации: Контроли уровня компании

Группы/Корпорации: Контроли уровня компании

Процесс 1: Закупки

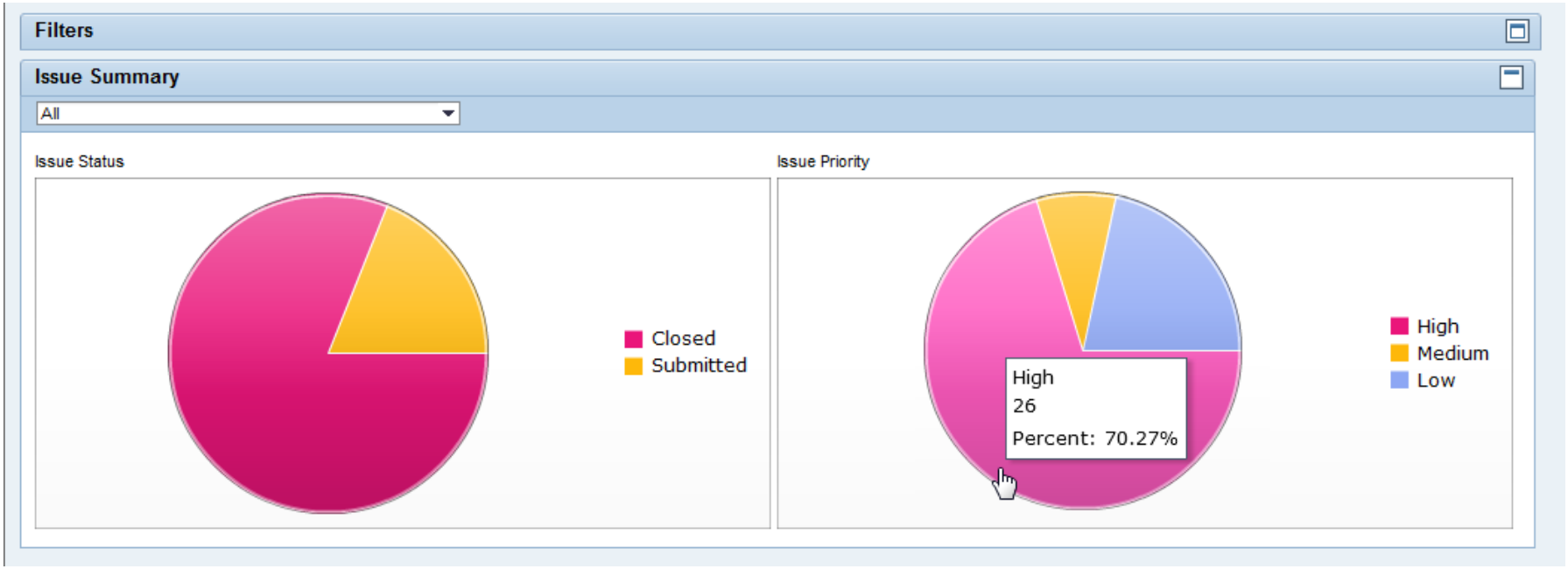
Процесс n: Казначейство

Общие ИТ Контроль 1: Access Control

ИТ контроль n: (ИТ Общие)

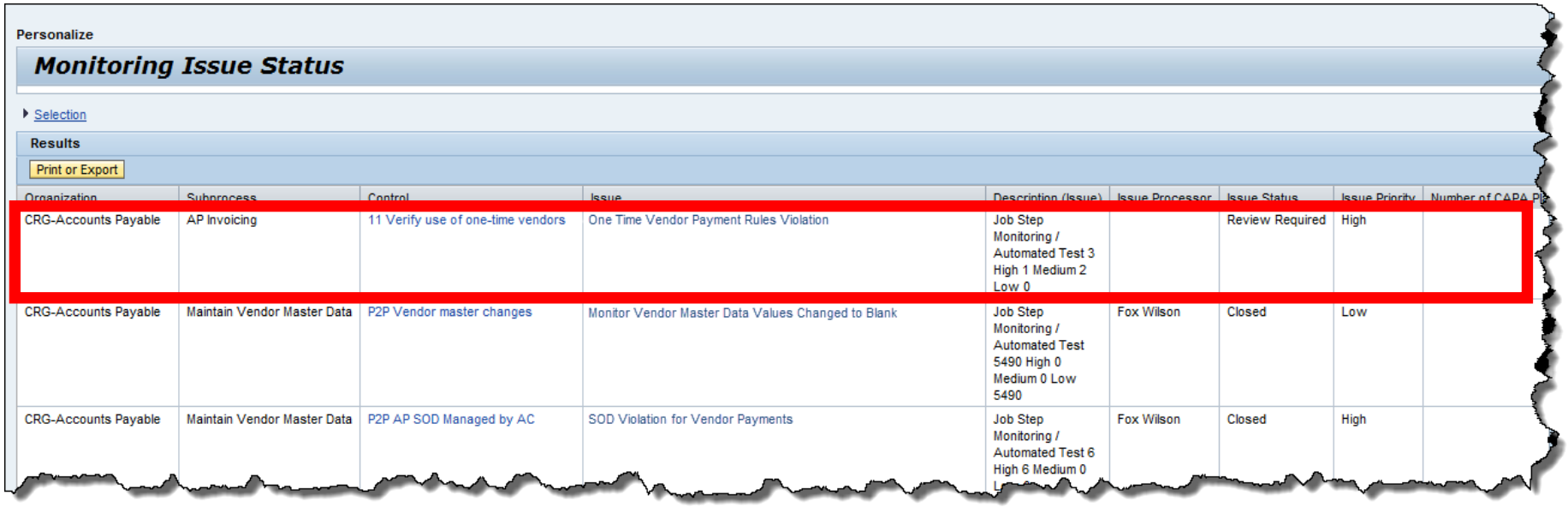
Постоянный мониторинг с помощью SAP GRC

Платежи - Отчетность по зарегистрированным инцидентам



Постоянный мониторинг пример

Платежи - Отчетность по зарегистрированным инцидентам



Personalize

Monitoring Issue Status

Selection

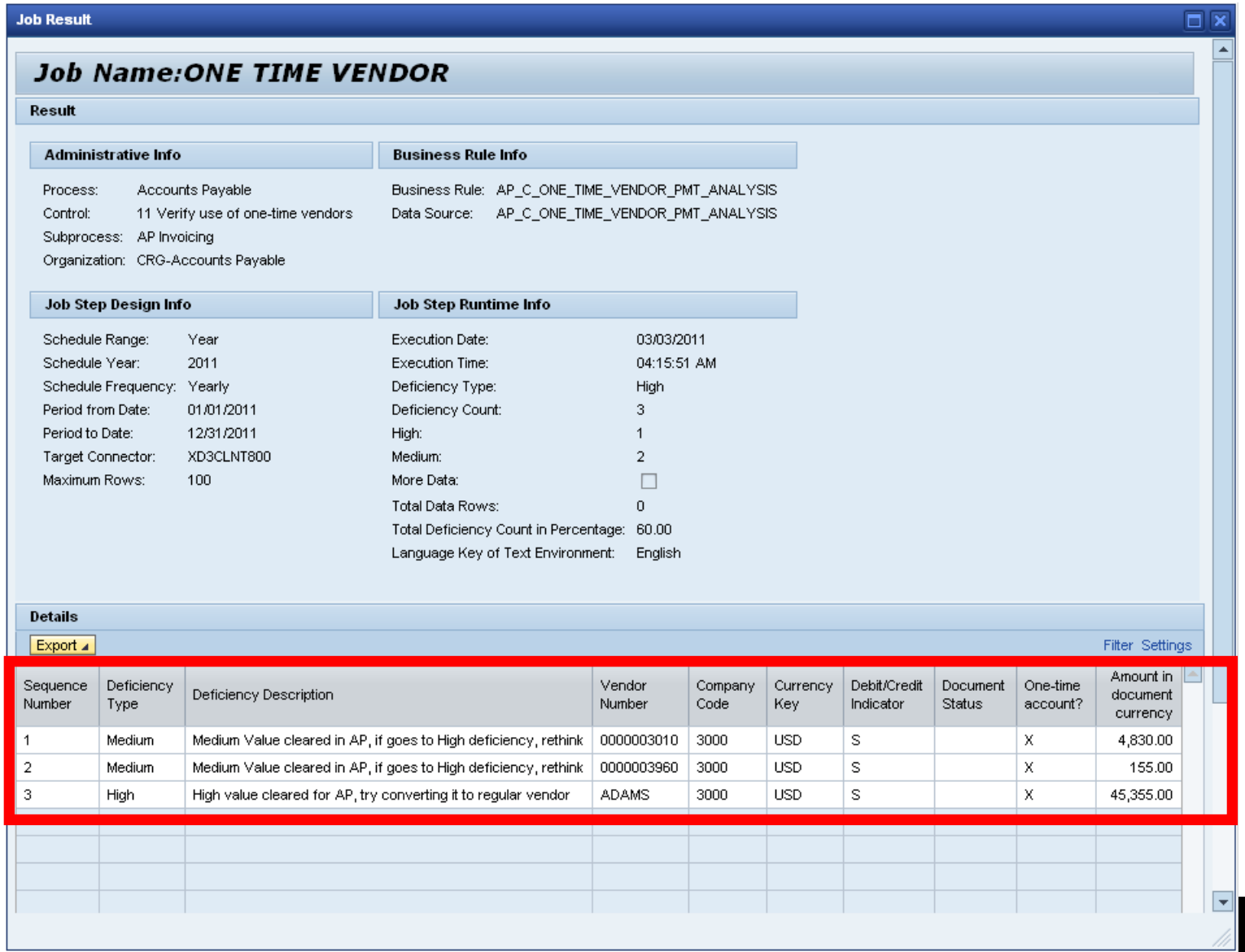
Results

Print or Export

Organization	Subprocess	Control	Issue	Description (Issue)	Issue Processor	Issue Status	Issue Priority	Number of CAPA Pl
CRG-Accounts Payable	AP Invoicing	11 Verify use of one-time vendors	One Time Vendor Payment Rules Violation	Job Step Monitoring / Automated Test 3 High 1 Medium 2 Low 0		Review Required	High	
CRG-Accounts Payable	Maintain Vendor Master Data	P2P Vendor master changes	Monitor Vendor Master Data Values Changed to Blank	Job Step Monitoring / Automated Test 5490 High 0 Medium 0 Low 5490	Fox Wilson	Closed	Low	
CRG-Accounts Payable	Maintain Vendor Master Data	P2P AP SOD Managed by AC	SOD Violation for Vendor Payments	Job Step Monitoring / Automated Test 6 High 6 Medium 0 L	Fox Wilson	Closed	High	

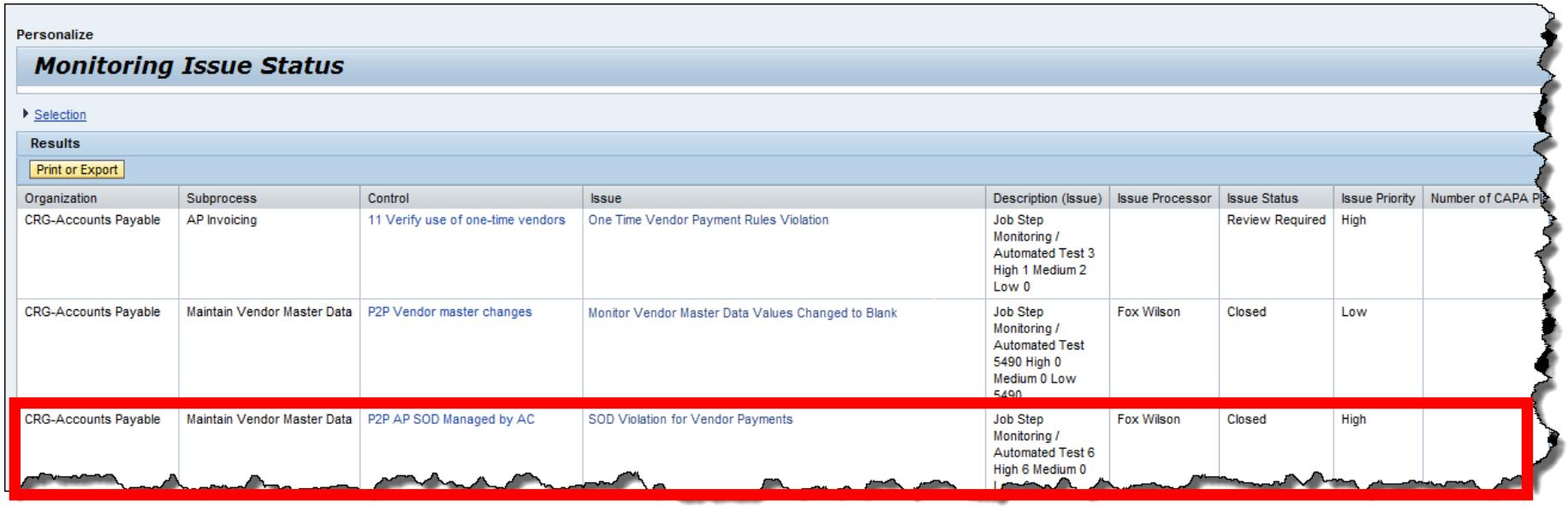
Постоянный мониторинг пример

Инцидент с разовыми поставщиками



Постоянный мониторинг пример

Платежи: Отчет по зарегистрированным инцидентам



Personalize

Monitoring Issue Status

▸ Selection

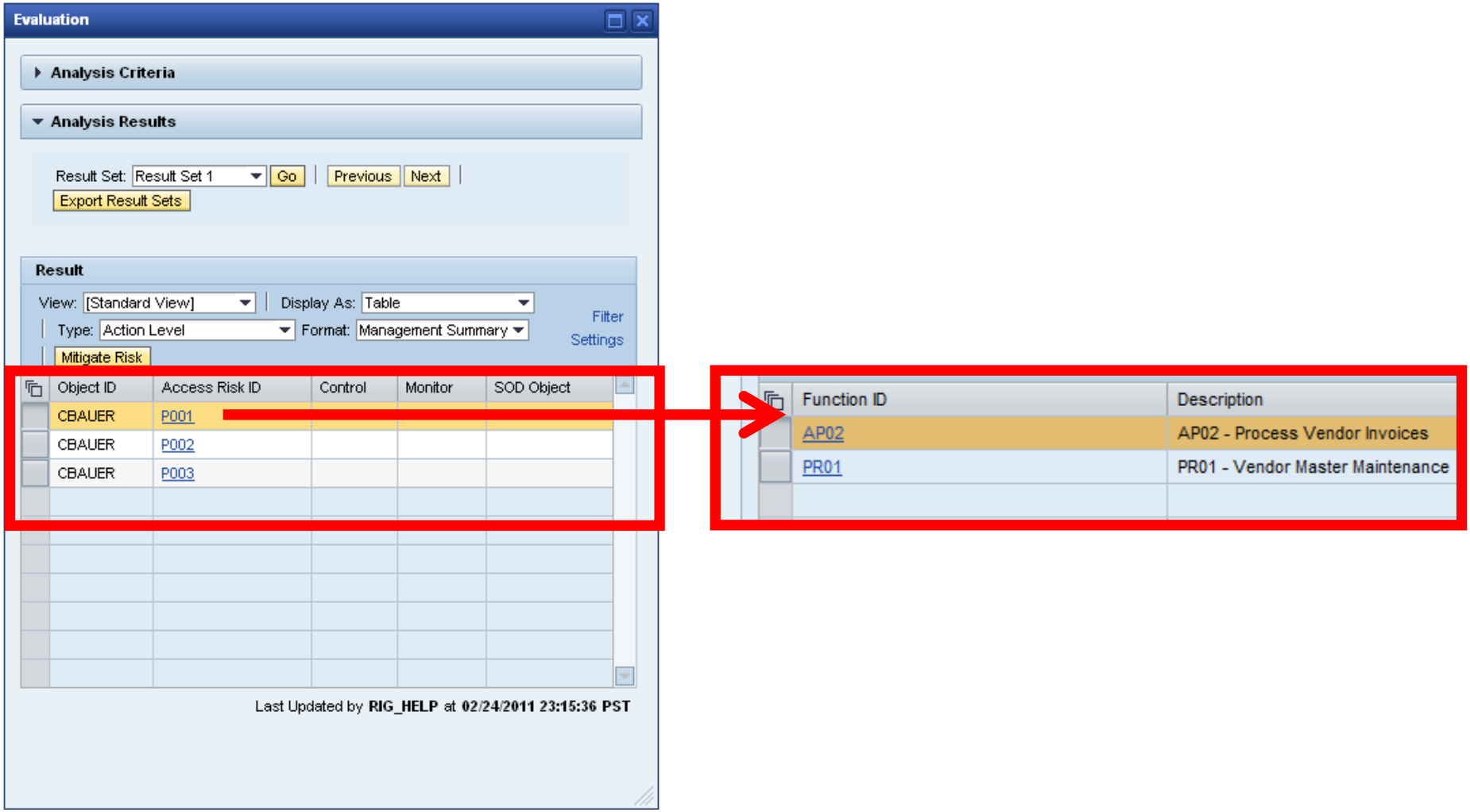
Results

Print or Export

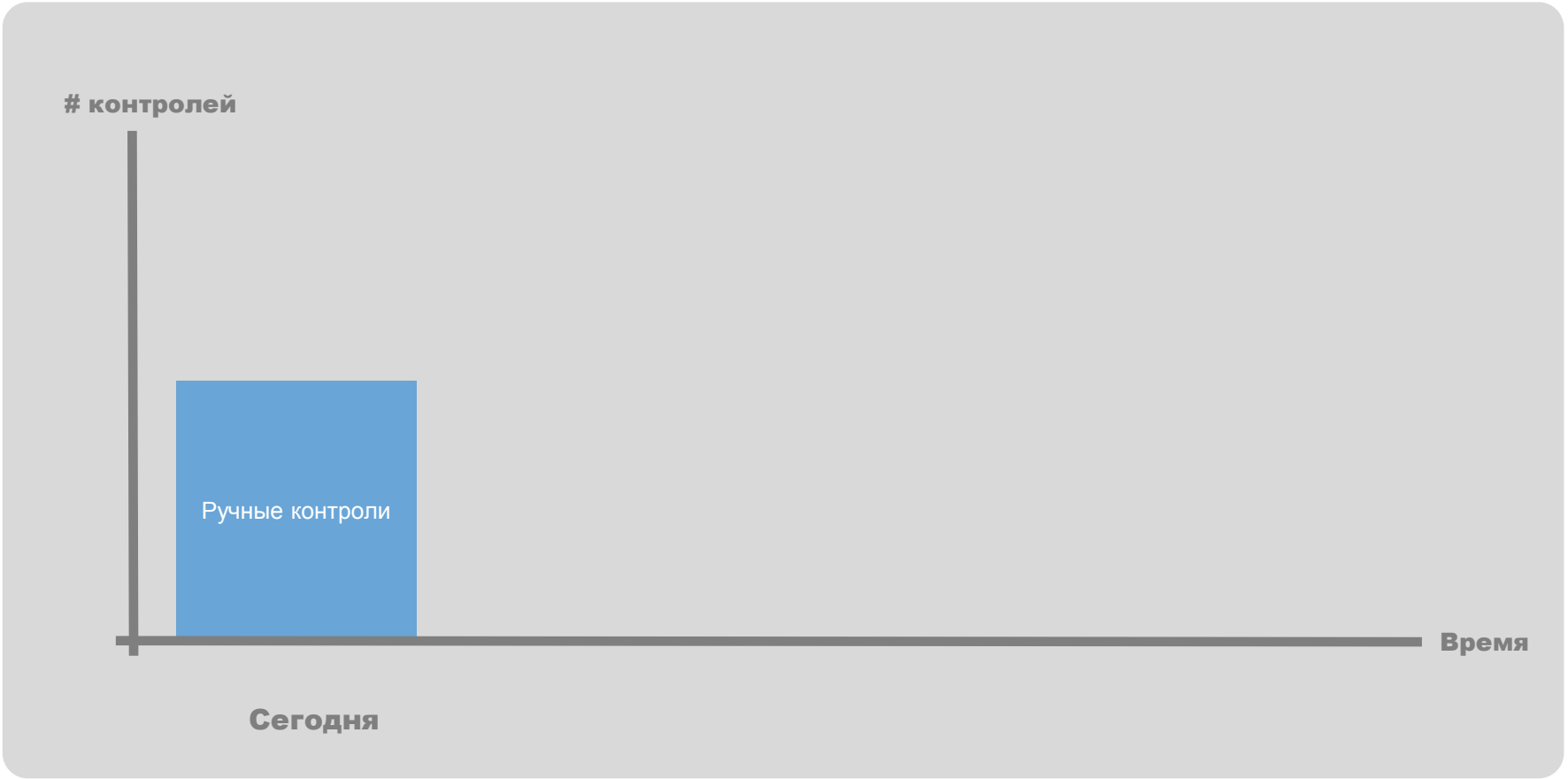
Organization	Subprocess	Control	Issue	Description (Issue)	Issue Processor	Issue Status	Issue Priority	Number of CAPA Pl
CRG-Accounts Payable	AP Invoicing	11 Verify use of one-time vendors	One Time Vendor Payment Rules Violation	Job Step Monitoring / Automated Test 3 High 1 Medium 2 Low 0		Review Required	High	
CRG-Accounts Payable	Maintain Vendor Master Data	P2P Vendor master changes	Monitor Vendor Master Data Values Changed to Blank	Job Step Monitoring / Automated Test 5490 High 0 Medium 0 Low 5490	Fox Wilson	Closed	Low	
CRG-Accounts Payable	Maintain Vendor Master Data	P2P AP SOD Managed by AC	SOD Violation for Vendor Payments	Job Step Monitoring / Automated Test 6 High 6 Medium 0	Fox Wilson	Closed	High	

Постоянный мониторинг пример

Пример конфликта разделения полномочий (SoD)

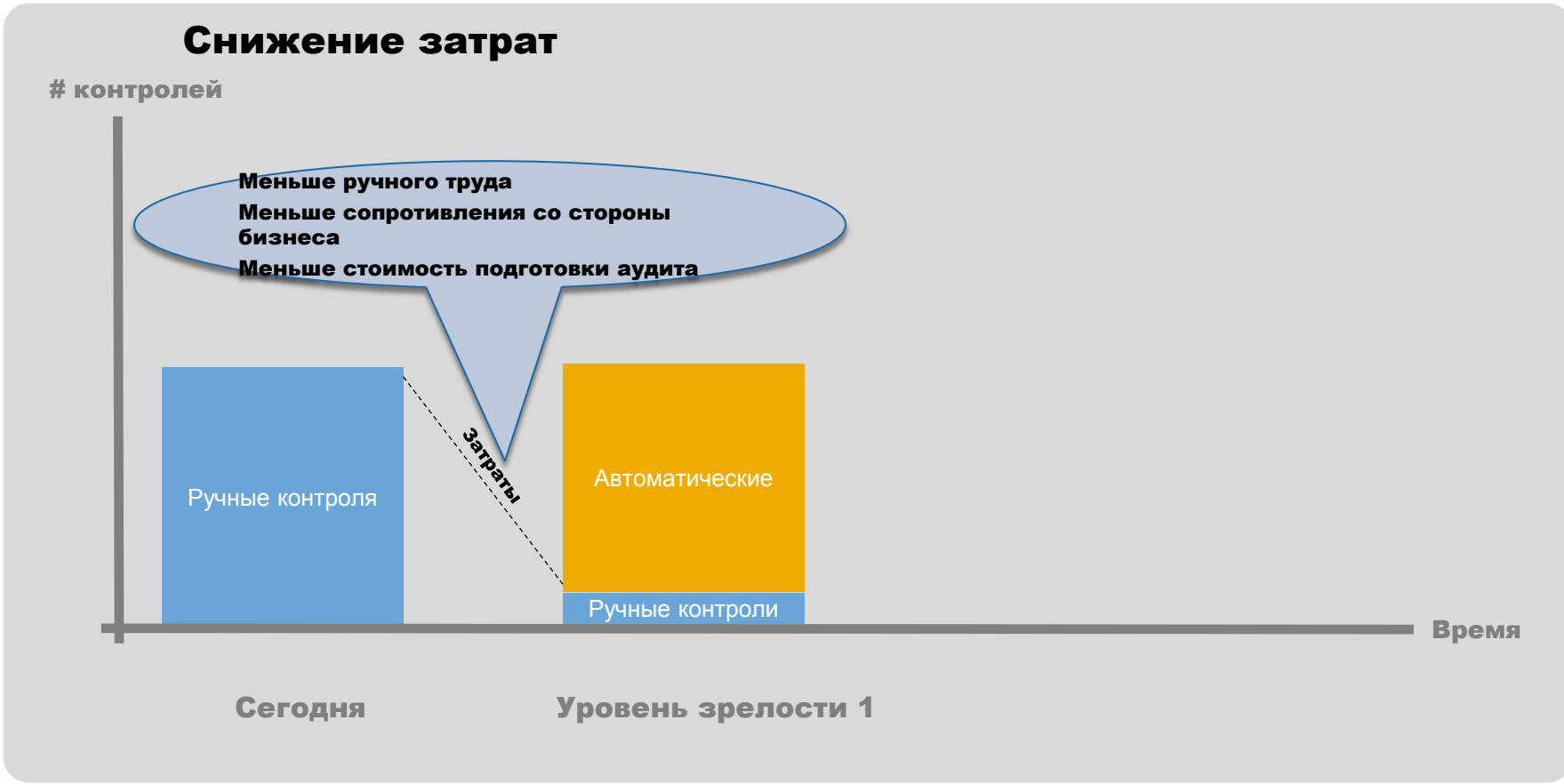


Достижение большей уверенности



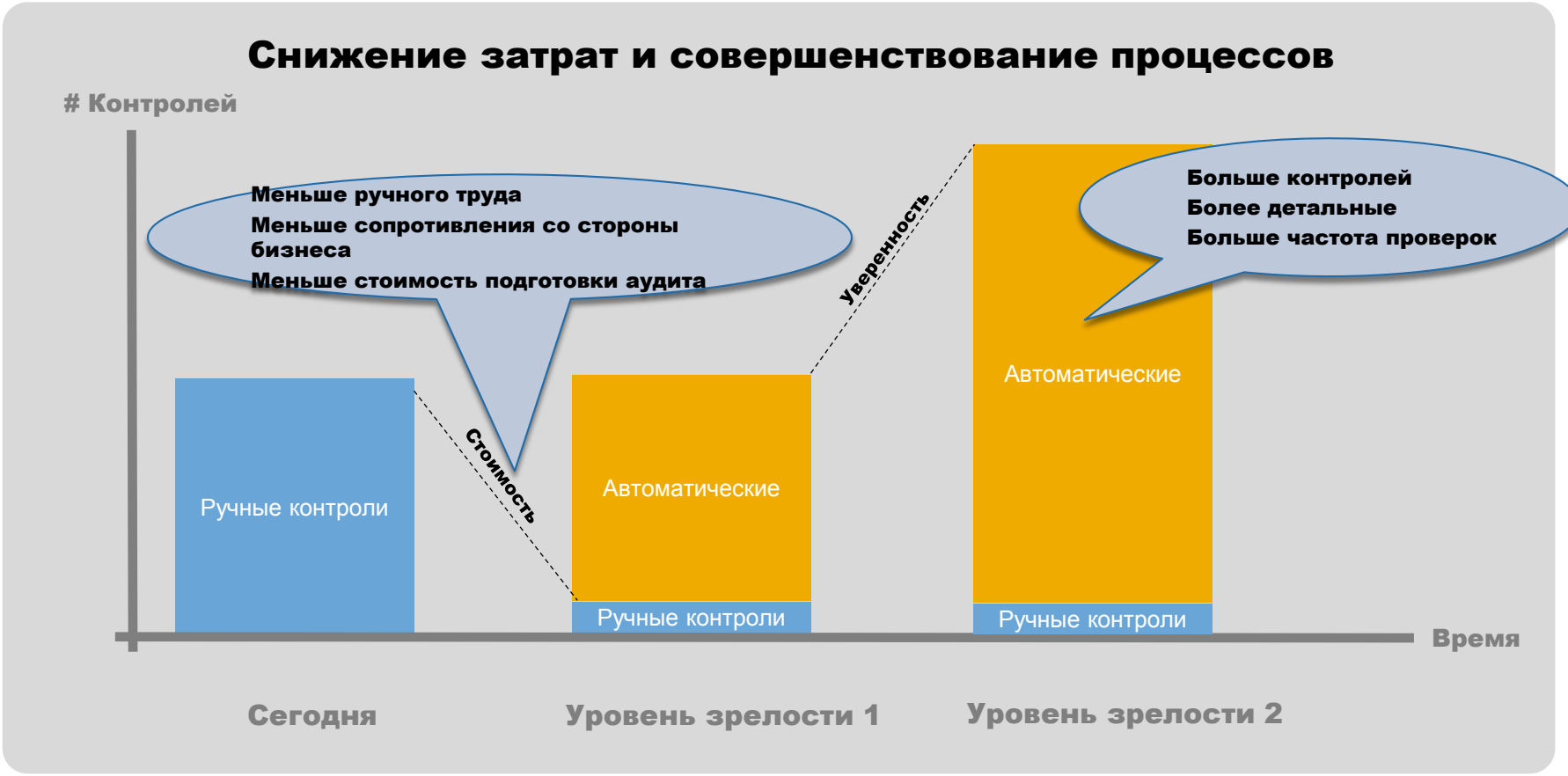
Достижение большей уверенности

Меньше затраты



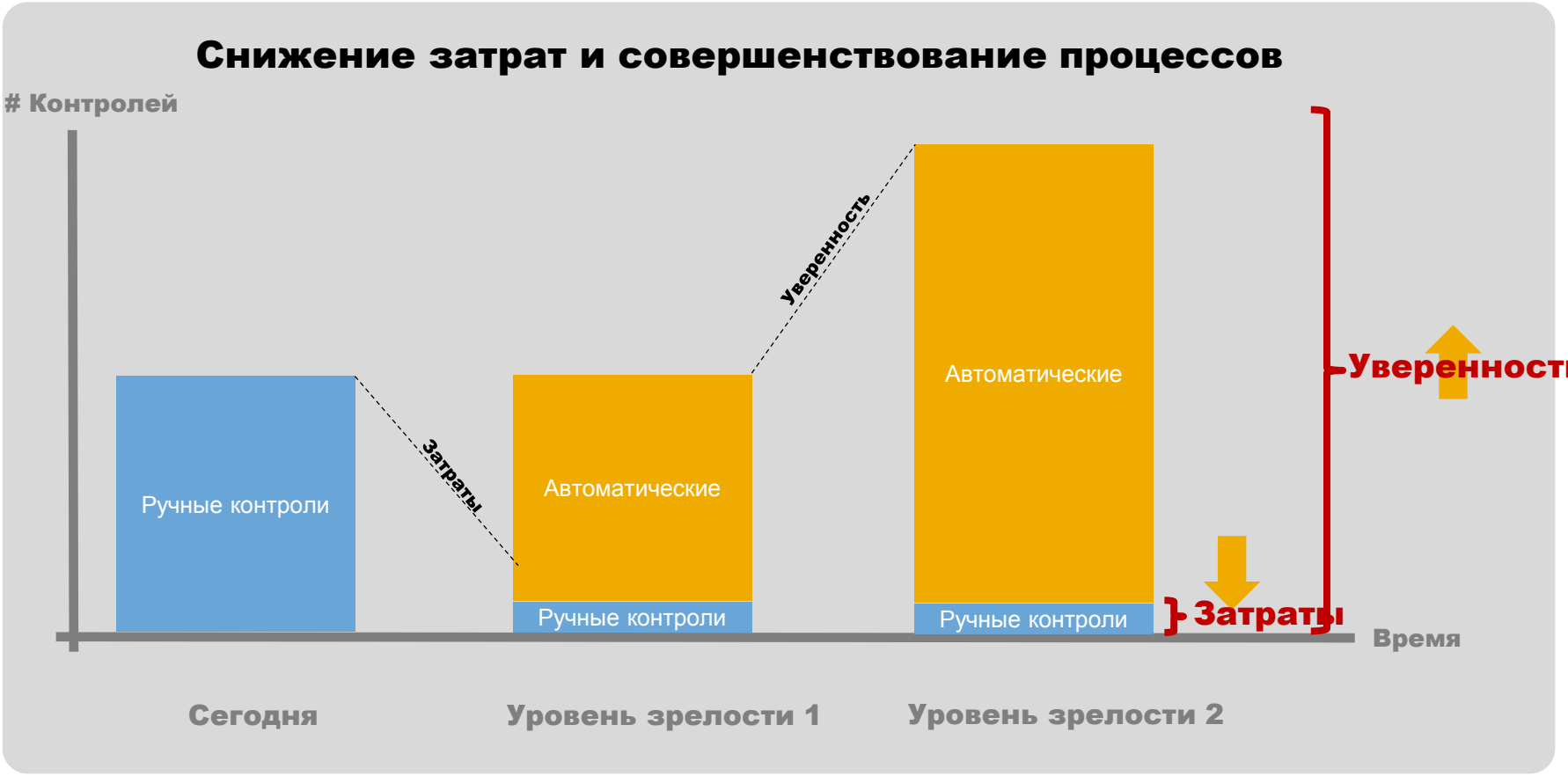
Достижение большей уверенности

Меньше затраты и совершенствование процессов

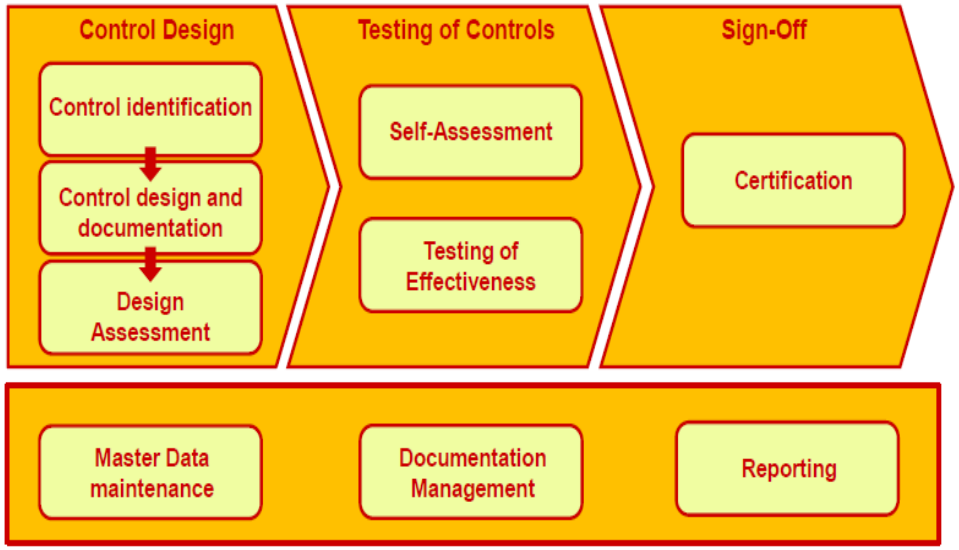


Достижение большей уверенности

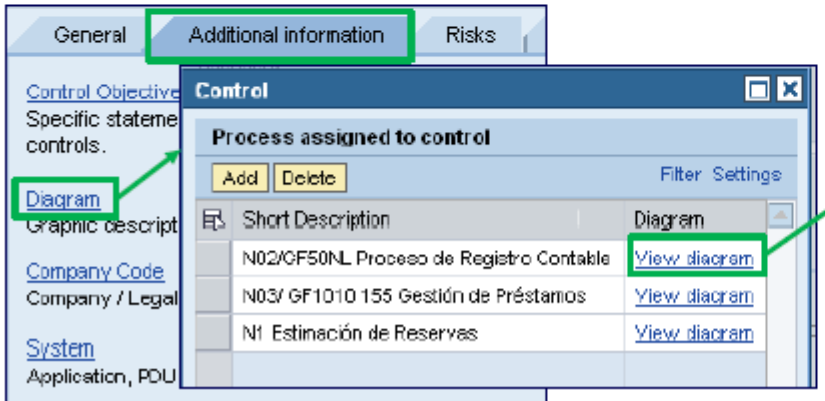
Меньше затраты и совершенствование процессов

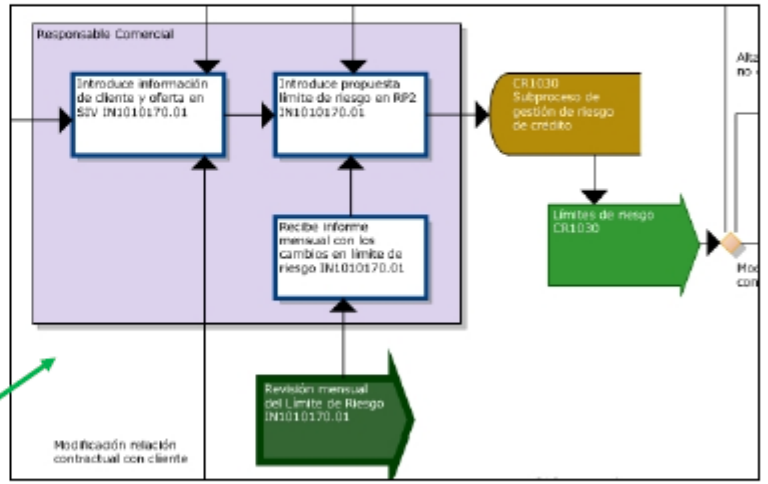


Компания REPSOL контролирует достоверность финансовой отчетности с помощью SAP GRC PC

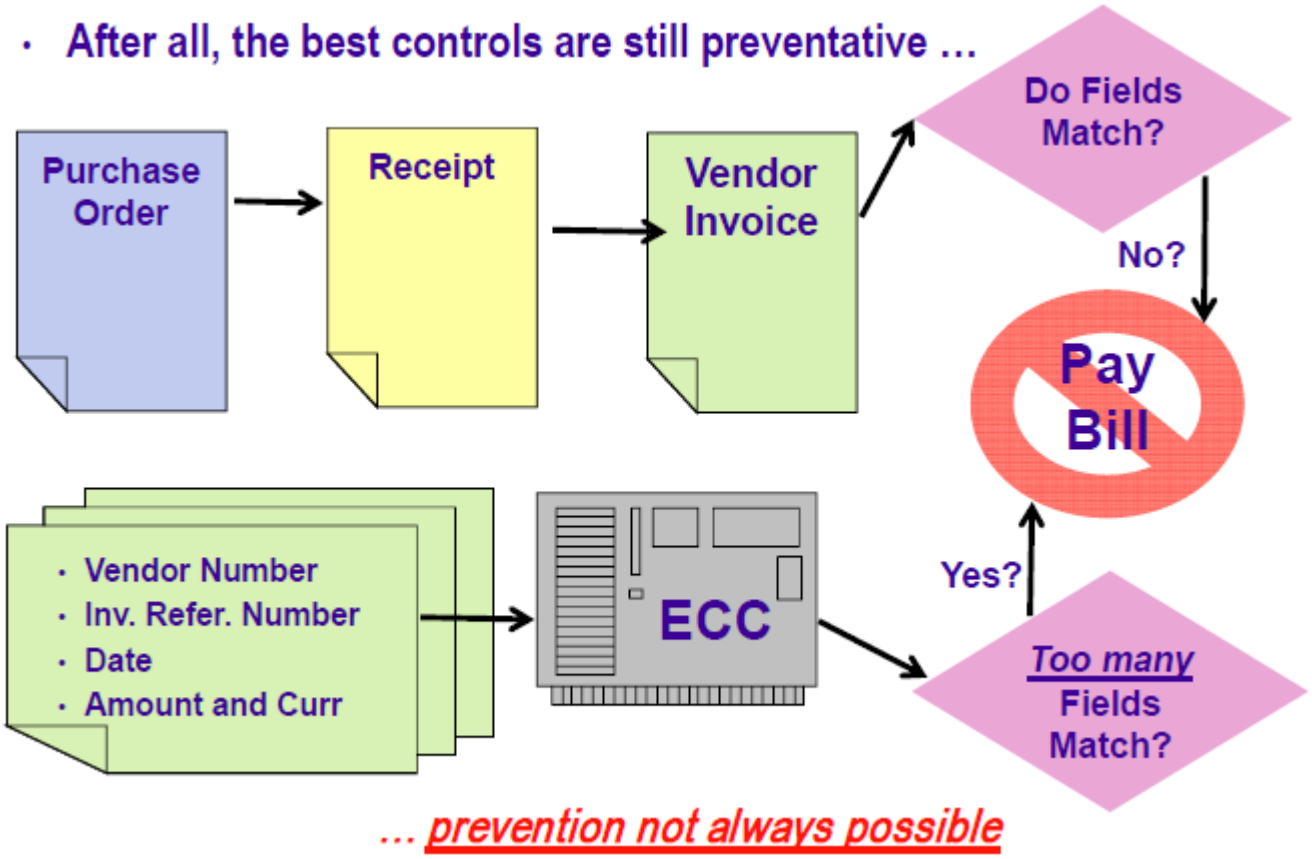


Role	Activities Performed
Auditor	• Document processes and controls • Plan control design assessment, self-assessment, test of effectiveness and sign-off workflows • Review control design assessment, self-assessment results • Enter test of effectiveness result coming from SACI • Verify and monitor life cycle for every control within regulation
Manager	• Receive and manage issue • Define remediation plan • Monitor life cycle for every control within regulation
Organization owner	• Potentially perform control design assessment and self-assessment • Perform remediation plan • Perform sign off for the organization he/she is responsible for • Monitor control life cycle within the organization(s) he/she is responsible for and below
Organization supervisor	• Monitor control life cycle within the organization(s) he/she is responsible for and below
Control recipient task	• Potentially perform control design assessment and self-assessment • Monitor life cycle for the controls he/she is assigned to



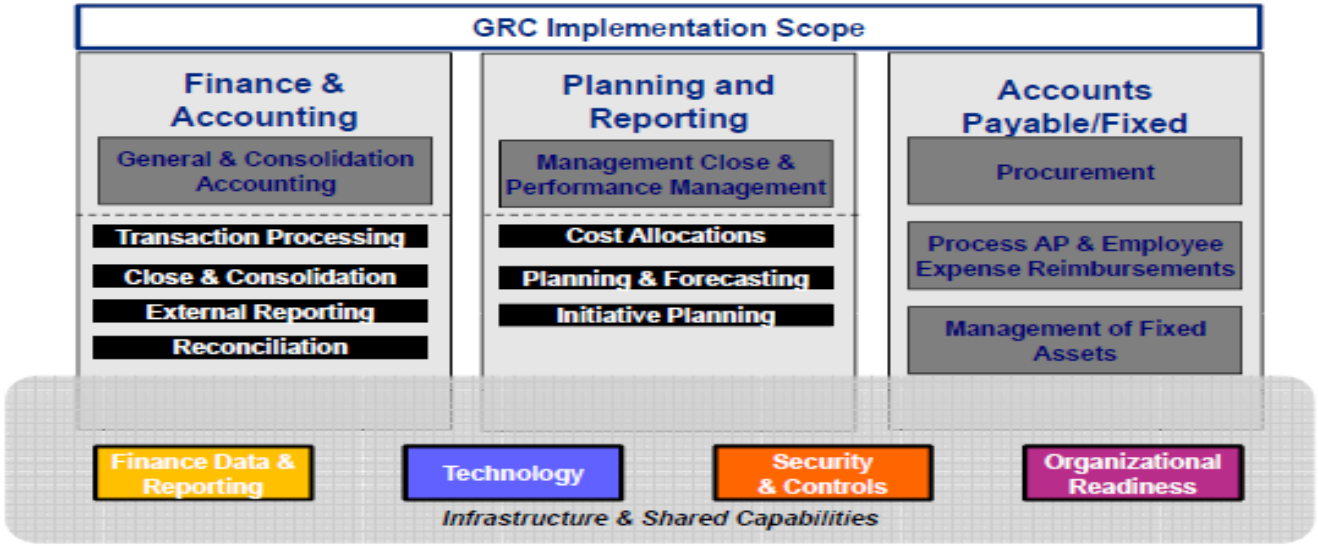


DowChemical выявляет дублирующие счета на оплату с помощью SAP GRC PC



Bank of America использует SAP GRC PC для контроля бизнес-процессов

Область автоматизации	Действия системы
Автоматизированный контроль и мониторинг	Мониторинг ключевых настроек систем, мастер данных, транзакций (связанных с функциями комплаенс, проверка работоспособности КП)
Управление инцидентами	Управление потоками операций для своевременного реагирования менеджмента
Постоянный контроль и мониторинг ИТ зависимых контролей	Контроль доступа к данным, контроль разделения полномочий
Предупреждение финансовых потерь	Автоматический контроль ключевых операционных процессов банка для снижения расходов



Решение SAP GRC

Наши клиенты использующие GRC решения

Спасибо!

Контактная информация:

Андрей Нифатов
andrey.nifatov@sap.com