Аудит управления ИТ-проектами: риски, контроли, процедуры аудита

Круглый стол Института Внутренних Аудиторов Украины.
11.06.2015, г. Киев

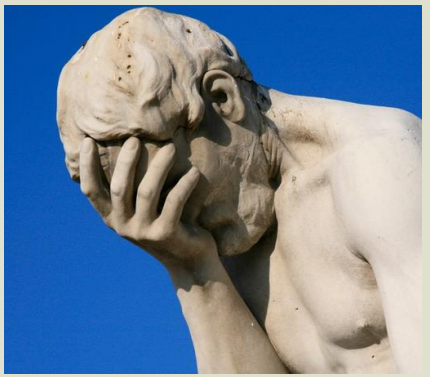
Содержание

A. Риски, факторы риска, контроли и процессы ITPM

B. Аудиторские процедуры по областям (процессам) ITPM

А. Риски, факторы риска, контроли и процессы ITPM

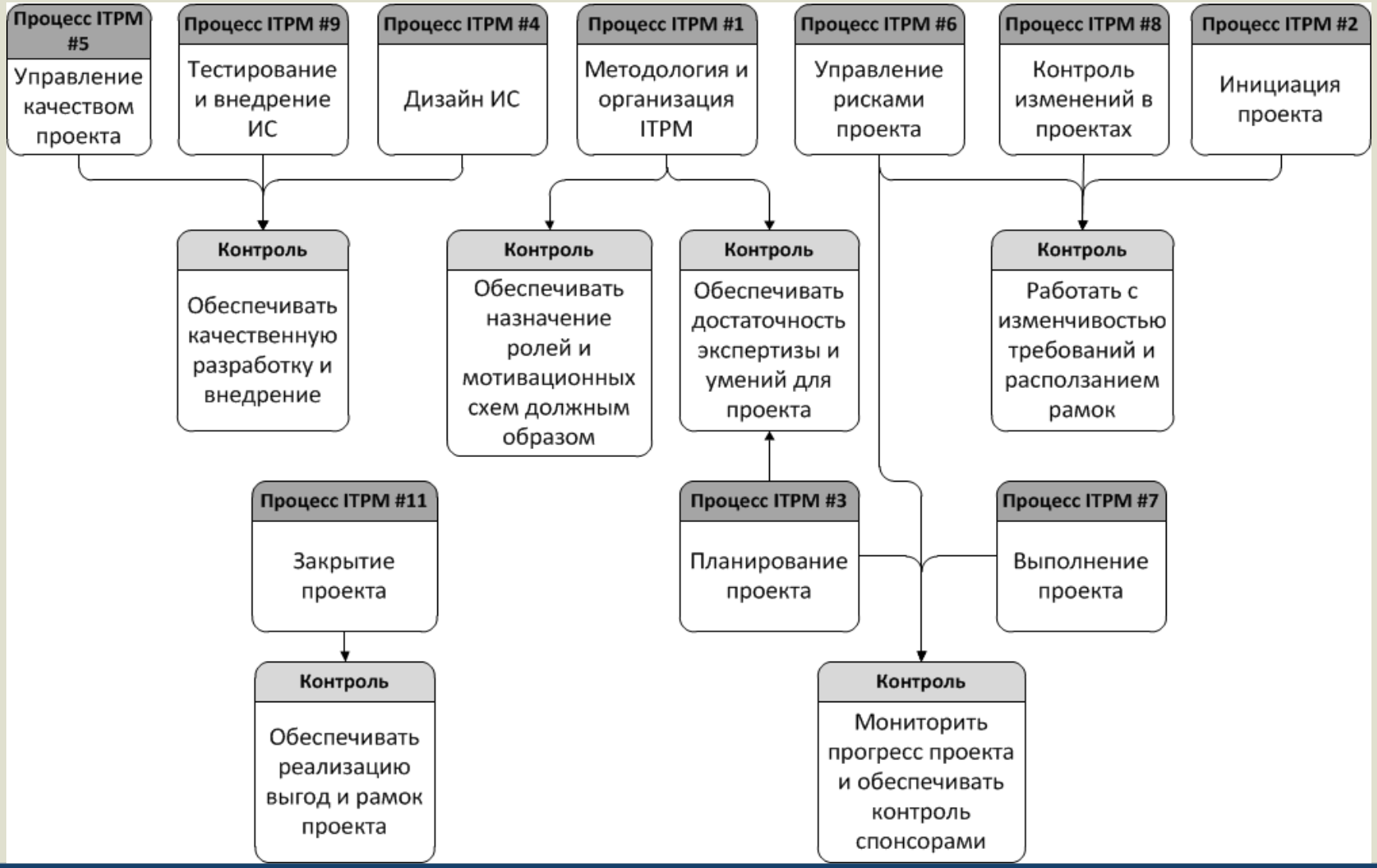
Риск I: Проекты не достигают результата и/или не выполняются в срок и/или превышают бюджет



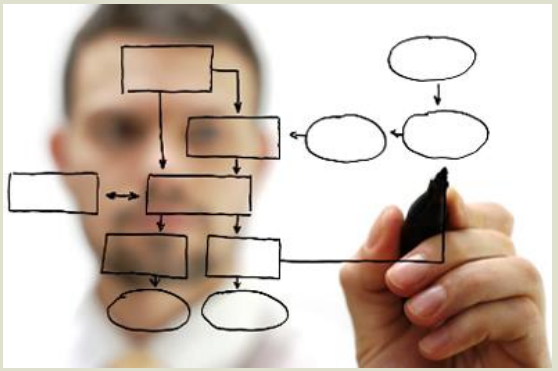
Факторы риска:

- Бизнес-владельцы не получают желаемый результат
  - Частая смена бизнес-требований и рамок проекта
    - «Расползание» рамок проекта
    - Присущая неопределенность
    - Недостаток умений команды проекта
  - Неожиданные проблемы и критические ошибки
    - Недостаток умений команды проекта
    - Искажение информации о статусе проекта менеджером проекта (намеренное или непреднамеренное)
  - Плохие коммуникации во время проекта
  - Нечеткая структура и роли участников проекта
  - Сужение рамок проекта
- Конечные пользователи не могут использовать функциональность
  - Пользователи не обучены новой функциональности
  - Плохая миграция данных

Риск I: Процессы и контроли ITPM



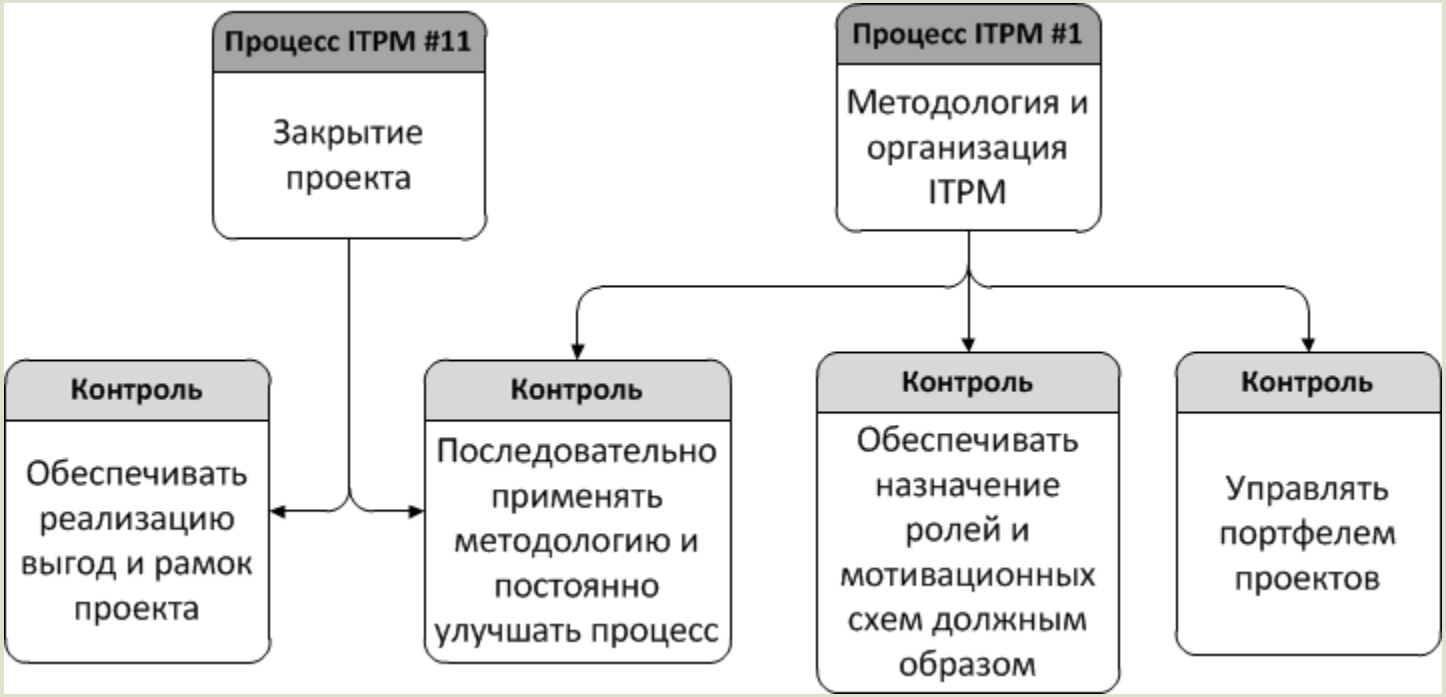
Риск II: Портфель проектов не оптимизирован с точки зрения выгод и затрат



Факторы риска:

- Одновременное использование ресурсов (плохая приоритезация)
- Несоответствующее назначение ресурсов на проекты (плохая приоритезация)
- Текущие проекты своевременно не прерываются
- Повторяющиеся проблемы в проектах (рамки, бюджет, время, качество) не устраняются
- ИТ-проекты выполняются за рамками методологии ITPM

Риск II: Процессы и контроли ITPM

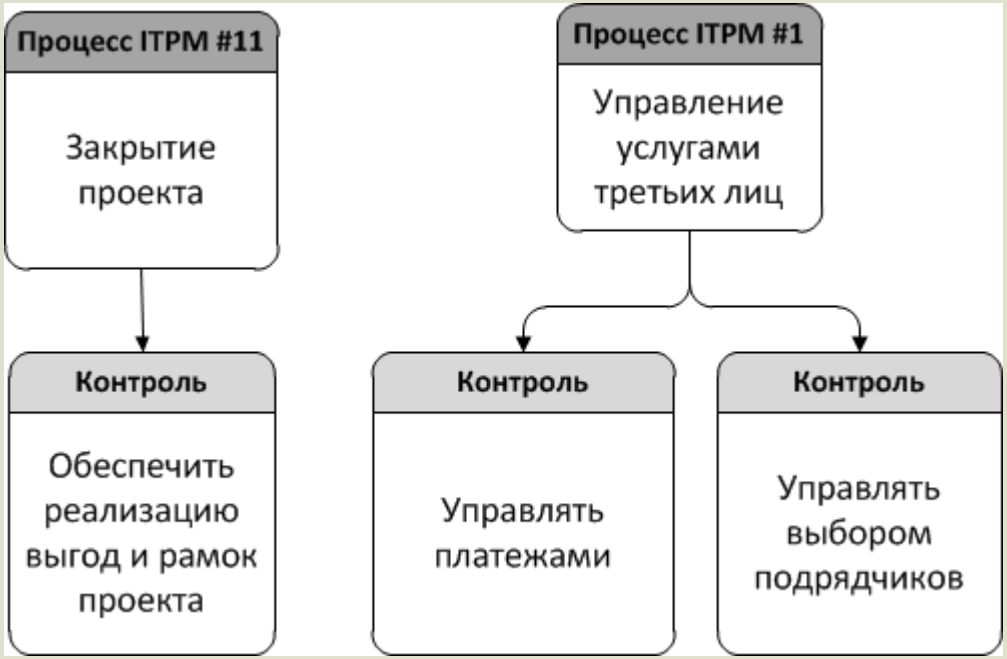


Риск III: Необоснованные затраты проекта и высокая стоимость владения ИТ-решением

Факторы риска:

- Скрытые затраты
  - Искусственный сдвиг этапов проекта за его рамки
  - Дорогостоящая поддержка
- Перерасход бюджета проекта
  - Необоснованная предварительная оплата или переплата за этап
  - Не выполнение подрядчиком своих обязательств
- Дорогой подрядчик или частое использование консультантов

Риск III: Процессы и контроли ITPM



B. Аудиторские процедуры по областям (процессам) ITPM

Область ITPM #1. Методология и организация ITPM

Аудиторские процедуры - убедиться в следующем:

- Существует стандартизированный подход к управлению проектами / портфелем проектов. Подход (методология) должен:
  - обеспечивать достижение целей проектов, управление требованиями, рисками, затратами, ресурсами, временем и качеством
  - покрывать все дисциплины проектного менеджмента (управление рамками проекта, ресурсами, рисками, затратами, качеством, временем, коммуникациями, определением участников проекта, закупками, управлением изменениями в проектах, интеграцией и реализацией выгод).
- Существует соответствующая орг.структура с достаточными полномочиями для управления проектами
- Встречи менеджмента для контроля общего статуса проектов проводятся, и соответствующие планы мероприятий и отчеты по их выполнению создаются.

Область ITPM #2. Инициация проекта

Аудиторские процедуры - убедиться в следующем:

- Существует стандартизированный подход к выбору заинтересованных лиц, владельцев (спонсоров) проектов, проектных менеджеров и управляющие комитеты:
  - Роли и ответственность определена
  - Участники наделены соответствующими полномочиями
- Утвержден бизнесом и предоставлен заинтересованным лицам документ с четким описанием целей и характера проекта, его рамок, затрат и выгод в количественном выражении (бизнес-кейс)
- Установлены ключевые показатели деятельности (KPI), критерии успеха и ожидаемые результаты, и они утверждены и приняты заинтересованными лицами и спонсорами проекта
- Проанализированы альтернативные варианты решений для достижения бизнес-целей (e.g. улучшение системы вместо покупки новой, разработка внутри или покупка «коробки»), есть соответствующий документ. Финальное решение утверждено бизнесом и ИТ.
- Вехи проекта (результаты фаз) определены на начальном этапе

Область ITPM #3. Планирование проекта

Аудиторские процедуры - убедиться в следующем:

- Определены необходимые ресурсы от бизнеса и ИТ, их роли, соответствующие умения и их использование во времени
- Определены и описаны обязанность и ответственность за закупки и управление услугами и продуктами третьих лиц.
- Определен план проекта, который должен включать:
  - Детальные результаты проекта и критерии приёмки
  - Требуемые внешние и внутренние ресурсы и обязанности
  - Четкая разбивка работ по шагам и фазам
  - Вехи проекта и фазы с промежуточными результатами
  - Ключевые зависимости
- План проекта и взаимосвязанные планы поддерживаются в актуальном состоянии
- План проекта и отчеты о статусе коммуницируются участникам должным образом
- Целевые показатели проекта (затраты, сроки, рамки, качество и результаты) установлены, проанализированы, утверждены и присутствуют в интегрированном плане проекта.

Область ITPM #4. Дизайн информационных систем (ИС)

Аудиторские процедуры - убедиться в следующем:

- Спецификации высокоуровневого дизайна (HLD) транслируют бизнес-требования согласно информационной архитектуре организации
- Квалифицированные и опытные специалисты вовлечены в процесс дизайна
- HLD утверждается и подписывается заинтересованными лицами от ИТ, которые гарантируют, что решение может быть разработано и поддерживаться.
- Спецификации детального дизайна содержат:
  - Описание входящих и исходящих данных согласно архитектуре и корпоративного словаря данных
  - Описание интеграции системы с другими системами организации
  - Требования информационной безопасности и к доступности системы, восстановлению после сбоев
  - Дизайн базы данных
  - Шаги обработки информации, включая спецификацию типов транзакций и правил обработки
- Детальный дизайн утвержден ответственными сотрудниками до перехода на следующую стадию разработки.

Область ITPM #5. Управление качеством проекта

Аудиторские процедуры - убедиться в следующем:

- Владение проектом и обязанности, контроль качества, критерии успеха и метрики выполнения (KPIs) определены
- Результаты каждой фазы утверждаются соответствующими менеджерами и пользователями вовлеченных бизнес-функций и ИТ
- Подтверждение качества внедрения системы включает:
  - Спецификацию критериев качества
  - Процесс валидации и верификации
  - Определение процесса контроля качества
  - Необходимый уровень квалификации проверяющих качество, их ролей и обязанностей

Область ITPM #6. Управление рисками проекта

Аудиторские процедуры - убедиться в следующем:

- Применяется формальный подход к управлению рисками, включающий определение, анализ, обработку и снижение рисков, их мониторинг и контроль
- Квалифицированный персонал вовлечен в процесс управления рисками
- Управление рисками осуществляется на протяжении всего жизненного цикла проекта
- Риски периодически пересматриваются, в том числе на каждой фазе проекта
- Разрабатываются и выполняются планы мероприятий по управлению рисками с указанием сроков и ответственных
- Ведется реестр всех рисков проекта, он анализируется для определения основных причин возникновения рисков

Область ITPM #7. Выполнение проектов

Аудиторские процедуры - убедиться в следующем:

- Набор критериев проекта установлен и используется (включая рамки, сроки, качество, затраты и уровни риска)
- Ход выполнения проекта измеряется согласно ключевых показателей деятельности. Отклонения анализируются на предмет их причин и влияния на проект. Разрабатываются соответствующие планы мероприятий.
- Результаты выполнения проекта докладываются заинтересованным лицам проекта

Область ITPM #8. Контроль изменений в проектах

Аудиторские процедуры - убедиться в следующем:

- Изменения в проекте управляются и документируются
- Изменения в проектах тщательно анализируются, утверждаются и включаются в обновленный план проекта
- Определены критерии и случаи, когда изменения должны быть одобрены владельцем проекта и/ или управляющим комитетом проекта
- На основе выборки проектов выбрать изменения и проверить, что
  - Соответствующее изменение задокументировано должным образом
  - Влияние изменения на проект и бизнес-кейс оценено и задокументировано
  - Проведена оценка рисков изменения
  - Получены соответствующие согласования изменения

Область ITPM #9. Тестирование и внедрение ИС

Аудиторские процедуры - убедиться в следующем:

- Определены и применяются требования для выполнения видов тестирования (модульное, интеграционное, регрессионное, пользовательское, стресс-тестирование, миграционное). Описание требований включает цель тестирования, его рамки, сроки, сценарии.
- Тестирование выполняется в выделенной тестовой среде
- Разработан набор тестовых данных, он сохраняется для последующего регрессионного тестирования
- Определены необходимые параметры и объем данных для стресс-тестирования
- Разработаны и соответствующим образом утверждены планы тестирования
- Результаты тестирования задокументированы, ошибки зарегистрированы, проанализированы и устранены
- Необходимое время для тестирования, включая пользовательское, предусмотрено в плане проекта
- План миграции с соответствующими спецификациями разработан и ему следуют
- Проводится оценка готовности системы, с фиксацией открытых вопросов и их риск-анализом, оценка утверждена ключевыми заинтересованными лицами, спонсором и управляющим комитетом
- Ключевые ИТ и бизнес-пользователи прошли обучение новой функциональности
- Разработаны руководства пользователей и администраторов

Область ITPM #10. Управление услугами третьих лиц

Аудиторские процедуры - убедиться в следующем:

- Нормативные документы организации требуют, чтобы ИТ-проекты следовали процедурам закупок и проведения тендеров согласно политик организации
- Выбор поставщиков соответствует установленным политикой закупок критериям
- Контракты с поставщиками включают необходимые условия, включая объем услуг, соглашения об уровне предоставления услуг (SLA), роли и обязанности, потенциальные риски и способы их снижения, процесс разрешения споров
- Обязательства по контрактам выполнены до закрытия проекта, все открытые вопросы с поставщиком решены
- Если контракты разорваны до получения результатов, проанализировать причины, фактические результаты и предпринятые меры для минимизации влияния на проект
- Проанализировать причины рисков, возникшие из-за вовлечения третьих лиц, предпринятые меры по их минимизации влияния на проект

Область ITPM #11. Закрытие проекта

Аудиторские процедуры - убедиться в следующем:

- Ключевые шаги по закрытию проекта определены и согласованы (включая обзор после реализации проекта (post-implementation review) для оценки достигнутых результатов)
- Обзоры после реализации проектов запланированы и выполняются
- Все открытые вопросы и незавершенные мероприятия определены, ответственность за их закрытие назначена и закрытие контролируется
- Заинтересованные лица приняли результаты проекта, владение системой передано после закрытия проекта
- Проведен анализ реализовавшихся рисков и недостатков, определены шаги по их недопущению в будущем (lessons learned)

Максим Померко, CISA, Член Правления ИВАУ, старший аудитор ИТ ЧАО «Киевстар»,
mpomerko@gmail.com