Теоретические основы компьютерной безопасности

Лекция №9. Международный стандарт COBIT

Учебные вопросы:

1. Назначение стандарта COBIT.
2. Принципы управления информационными технологиями на базе стандарта COBIT.

Литература:

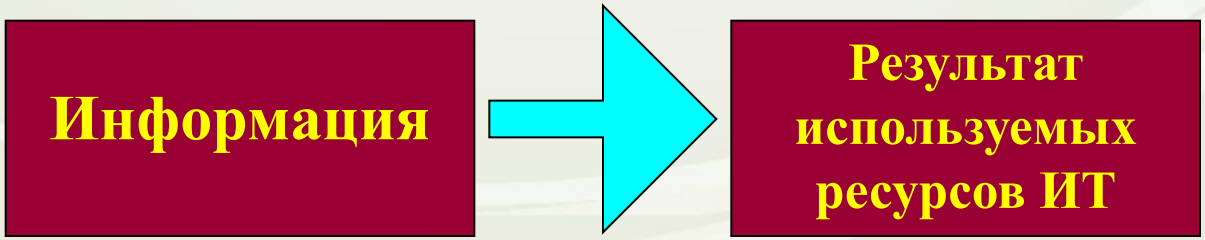
1. В.И. Аверченко «Аудит информационной безопасности». Учебное пособие. М: Издательство «Флинта», 2001.
2. В.А. Галатенко «Стандарты информационной безопасности». Учебное пособие. М: Интернет-Университет информационных технологий, 2006.
3. Jet Info. Информационный бюллетень №1 (116)/2003. Стандарт Cobit.

Вопрос №1. Назначение стандарта COBIT

Разработчики: Стандарт COBIT (Контрольные объекты для информационных и смежных технологий) разработан «Международной ассоциацией аудита и контроля за информационными системами» (ISACA) и Институтом руководства информационных технологий в 1992 г.

Издан: первая редакция стандарта была издана в 1996 г.

Назначение стандарта: Стандарт COBIT представляет менеджерам и аудиторам, а также пользователям информационных технологий набор утвержденных метрик, процессов и практик с целью помочь им в извлечении максимальной выгоды от использования информационных технологий и для разработки соответствующего руководства и контроля информационных технологий в компании.



Составляющие ресурсы информацион-ных технологий

Данные – объекты (внутренние, внешние), структурированные и неструкту-рированные, а также графики, звук и т.д.

Приложения – совокупность автомати-зированных и выполняемых в ручную процедур

Технология – аппаратное обеспечение, программное обеспечение, операционные системы, системы управления базами данных, сетью и мультимедиа

Оборудование – все ресурсы, создаю-щие и поддерживающие информационные технологии

Люди – персонал, его навыки: умение планировать и организовывать, комплек-товать, обслуживать и корректировать информационные системы и услуги

Критерии информации для достижений целей бизнеса

1. Эффективность – актуальность информации, соответствующего бизнес-процесса, гарантия своевременного и регулярного получения правильной информации;

2. Продуктивность – обеспечение доступности информации с помощью оптимального (наиболее продуктивного и экономичного) использования ресурсов;

3. Конфиденциальность – обеспечение защиты информации от неавторизованного ознакомления;

4. Целостность – точность, полнота и достоверность информации в соответствии с требованиями бизнеса;

5. Пригодность – предоставление информации по требованию бизнес-процессов;

6. Согласованность – соответствие законам, правилам и договорным обязательствам;

7. Надежность – доступ руководства организации к соответствующей информации для текущей деятельности, для создания финансовых отчетов и оценки степени соответствия.

Состав стандарта (книги ориентированные на разные аудитории)

1. Резюме для руководителя. Описание стандарта COBIT, ориентированное на топ-менеджеров организации для принятия ими решения о применимости стандарта в конкретной организации;

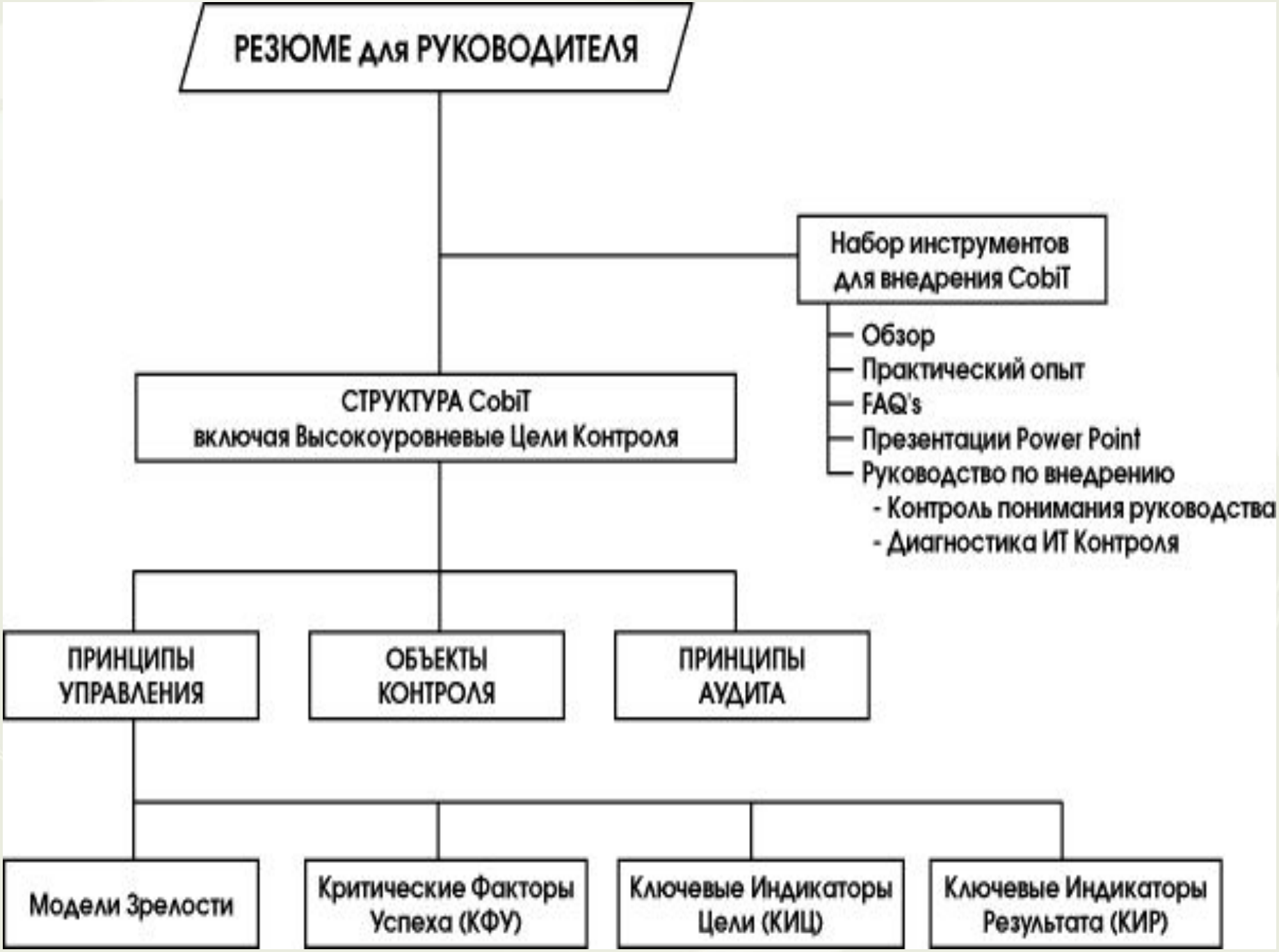
2. Описание структуры. Книга содержит развернутое описание структуры стандарта, высокоуровневых целей контроля и пояснения к ним, необходимые для эффективной навигации и результативной работы со стандартом;

3. Объекты контроля. В книгу включены детальные описания объектов контроля, содержащие расшифровку каждого из объектов;

4. Принципы управления. Книга отвечает на вопросы как управлять ИТ, как правильно поставить достижимую цель, как ее достичь и как проконтролировать полноту ее достижения. Предназначена для руководителей ИТ-служб;

5. Принципы аудита. Правила проведения ИТ-аудита. Описание того, у кого можно получить необходимую информацию, как ее проверить, какие вопросы задавать? Книга предназначена для внутренних и внешних аудиторов ИТ, а также консультантов в сфере ИТ;

6. Набор инструментов внедрения стандарта — практические советы по ежедневному использованию стандарта в управлении и аудите ИТ. Книга предназначена для внутренних и внешних аудиторов ИТ, консультантов в сфере ИТ.


РЕЗЮМЕ для РУКОВОДИТЕЛЯ
Набор инструментов для внедрения CobiT
Обзор
Практический опыт
FAQ's
Презентации Power Point
Руководство по внедрению
- Контроль понимания руководства
- Диагностика ИТ Контроля
СТРУКТУРА CobiT включая Высокоуровневые Цели Контроля
ПРИНЦИПЫ УПРАВЛЕНИЯ
ОБЪЕКТЫ КОНТРОЛЯ
ПРИНЦИПЫ АУДИТА
Модели Зрелости
Критические Факторы Успеха (КФУ)
Ключевые Индикаторы Цели (КИЦ)
Ключевые Индикаторы Результата (КИР)

Вопрос №2. Принципы управления Информационными технологиями на базе стандарта COBIT

Принципы управления информационны-ми технологиями

Стратегические вопросы:

1. Существуют ли в настоящее время в организации ИТ, при управлении которыми удовлетворяются все информационные потребности организации?
2. Как организация обеспечивает инфраструктуру и управляет рисками, насколько организация зависит от этого?
3. С какими проблемами организация сталкивается при управлении ИТ?

Тактические вопросы:

1. Что является результатом ИТ-процессов?
2. Что является решением проблем в информационных технологиях?
3. Из чего состоят эти решения?
4. Будут ли работать эти решения?
5. Как их реализовать?

Ответы на тактические вопросы

Модели зрелости

Критические факторы успеха

Ключевые индикаторы цели

Ключевые показатели результата

МОДЕЛИ ЗРЕЛОСТИ

Модели зрелости предназначены для организации эффективного управления. Они определяют ключевые действия, которые указывают, что надо сделать для достижения требуемого качества и содержат способы контроля над правильностью выполнения ключевых ИТ-процессов и методы их корректировки.

Модели зрелости

Используя «Модели зрелости» руководитель организации получает ответы на следующие вопросы:

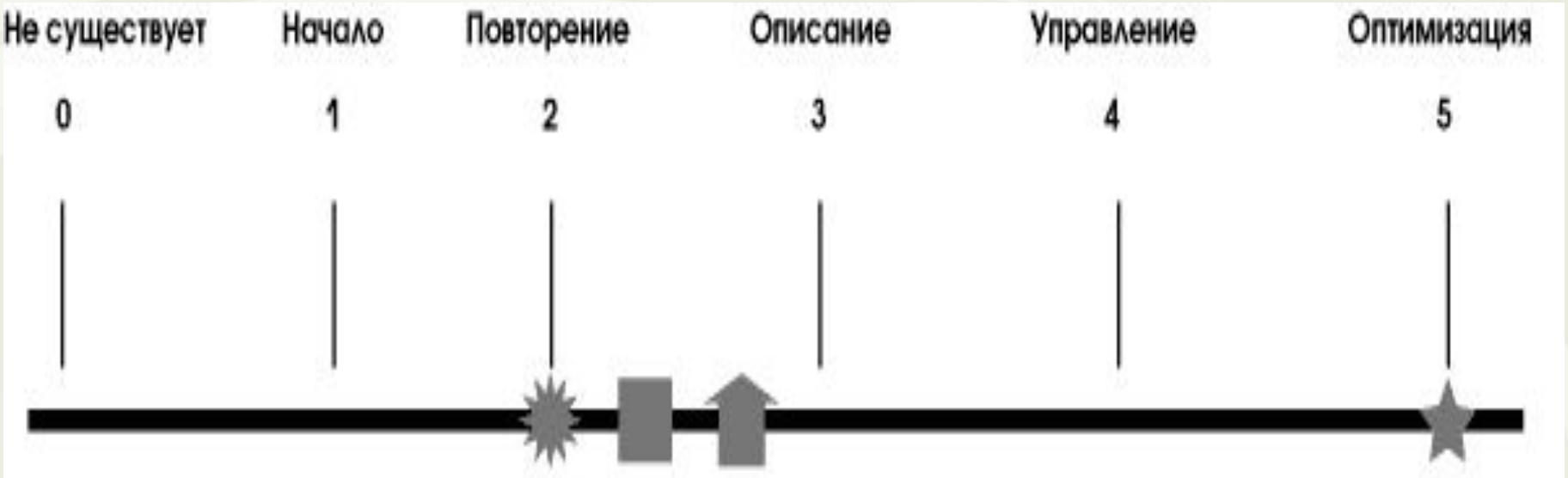
1. Текущий статус организации – оценить на какой стадии организация находится сегодня.

2. Текущий статус лучшей практики в этой отрасли – сравнить свою организацию с лучшей организацией в этой отрасли.

3. Текущий статус международных стандартов – провести дополнительное сравнение текущего статуса организации с «лучшей практикой» или международными стандартами.

4. Статус организации после усовершенствования (реализация стратегии организации) – оценить стратегию организации, каких результатов организация хочет достичь.

ШКАЛА МОДЕЛЕЙ ЗРЕЛОСТИ



Легенда для используемых символов

- Текущий статус организации
- Требования международных стандартов
- "Лучшая практика" индустрии
- Стратегия организации

Легенда для используемой шкалы

0 Не существует	- Процессы управления не применяются
1 Начало	- Процессы специализированны и неорганизованны
2 Повторение	- Процессы повторяются на регулярном основании
3 Описание	- Процессы документированы и взаимосвязаны
4 Управление	- Процессы наблюдаются и измеряются
5 Оптимизация	- Процессы соответствуют "лучшей практике" и автоматизированы

0. Не существует

Полное отсутствие каких-либо процессов управления информационными технологиями. Организация не признает существования проблем в информационных технологиях, которые нужно решать, и, таким образом, нет никаких сведений о проблемах.

1. Начало (Анархия)

Организация признает существование проблем управления информационными технологиями и необходимость их решения. При этом не существует никаких стандартизованных решений. Существуют случайные одномоментные решения, принимаемые кем-то персонально или от случая к случаю. Подход руководства к решению ИТ-проблем хаотичен, признание существования проблем случайно и непоследовательно.

2. Повторение (Фольклор)

1. Существует всеобщее осознание проблем управления ИТ;
2. Показатели деятельности и ИТ-процессов находятся в развитии, охватывая процессы планирования, функционирования и мониторинга информационных технологий;
3. Выбраны для улучшения и/или контроля те ИТ-процессы, которые влияют на основные бизнес-процессы предприятия;
4. Эффективно выполняется планирование и управление инвестициями;
5. Руководство организации регламентировало меры по управлению информационными технологиями, но процесс не был принят в организации;
6. Не существует формализованного обучения, набора взаимосвязанных стандартных процедур управления, ответственность возложена на сотрудников;
7. Сотрудники контролируют процессы управления с помощью проектов и ИТ-процессов;
8. Ограниченные инструменты управления выбираются и внедряются для сбора метрик управления, но не используются в полном объеме из-за недостатков в оценке их функциональности.

3. Описание (Стандарты)

1. Необходимость действовать в соответствии с принципами управления информационными технологиями понимается и принимается;
2. Определена связь между результатом и показателями производительности, она зафиксирована и внедрена в стратегические процессы планирования и мониторинга;
3. Процедуры стандартизованы и документированы, проводится обучение сотрудников по выполнению этих процедур;
4. Показатели производительности всех видов деятельности зафиксированы и отслеживаются, что приводит к повышению эффективности работы всей организации;
5. Ответственность за обучение, выполнение и применение стандартов возложена на сотрудников организации;
6. Анализ первопричин применяется время-от-времени;
7. Большинство процессов управляются в соответствии с некоторыми основными метриками, и, как правило, отдельными сотрудниками, поэтому ни о каких отклонениях руководители не знают;
8. Всеобщая отчетность о выполнении ключевых процессов является четкой, и руководство премирует сотрудников на основе измерения ключевых результатов.

4. Управление (Измеряемый)

1. Существует полное понимание проблем управления информационными технологиями на всех уровнях организации, постоянно происходит обучение сотрудников;

2. Четко распределена ответственность, установлен уровень владения процессами;

3. Процессы информационных технологий соответствуют бизнесу и стратегии информационных технологий;

4. Все совладельцы процесса осознают риски, важность информационных технологий и их возможности, которые они предоставляют;

5. Руководство организации определило допустимые отклонения, при которых процессы должны работать;

6. Процессы постоянно совершенствуются, их результаты соответствуют «лучшим практикам»;

7. Формализован порядок анализа первопричин. Присутствует понимание необходимости постоянного совершенствования;

8. Ограниченно применяются передовые технологии, основанные на современной инфраструктуре и модифицированных стандартных инструментах;

9. Все необходимые ИТ-специалисты вовлечены в бизнес-процессы;

10. Управление информационными технологиями превращается в процесс уровня всей организации;

11. Деятельность управления информационными технологиями интегрируется в процесс управления организацией.

5. Оптимизация (Оптимизируемый)

1. В организации существует углубленное понимание управления информационными технологиями, проблем и решений информационных технологий, а также перспектив;

2. Обучение и коммуникация поддерживаются на должном уровне, самыми современными средствами;

3. В результате непрерывного улучшения процессы соответствуют моделям зрелости, построенным на основании «лучшей практики»;

4. Первопричины всех проблем и отклонений тщательно анализируются, по результатам анализа выполняются результативные действия;

5. Информационные технологии интегрированы в бизнес-процессы, полностью их автоматизируют, предоставляя возможность повышать качество и эффективность работы организации.

КРИТИЧЕСКИЕ ФАКТОРЫ УСПЕХА

Определяют наиболее важные проблемы или действия руководителей, направленные на достижение контроля ИТ-процессами.

Примеры критических факторов успеха:

- Действия по управлению информационными технологиями интегрированы в процессы управления организации и стиль работы руководителей;
- Управление информационными технологиями сосредоточенно на целях организации: стратегических инициативах, использовании технологий для развития бизнеса, достаточности ресурсов и удовлетворения бизнес-требований;
- Действия по управлению информационными технологиями ясно определены, формализованы и осуществляются на основе потребностей предприятия с соответствующей отчетностью;
- Методы управления разработаны для увеличения продуктивности, оптимального использования ресурсов и увеличения эффективности ИТ-процессов;

- Организационные методы следят за окружающей средой и культурой управления; способствуют нормальному контролю; ведению стандартной практики управления рисками; определяют степень соответствия установленным стандартам; управляют и изучают недостатки и риски;

- Методы аудита определены таким образом, чтобы избежать сбоев и ошибок в системе внутреннего контроля;

- Наблюдается интеграция и развитие взаимодействия сложных ИТ-процессов, таких как управление проблемами, изменениями и конфигурациями;

- Учрежден контрольный комитет, назначающий и наблюдающий за независимым аудитом, уделяющий пристальное внимание ИТ при составлении планов аудита, а также принимающий во внимание результаты исследований сторонних организаций и аудиторов.

КЛЮЧЕВЫЕ ИНДИКАТОРЫ ЦЕЛИ

Описывают комплекс измерений, которые по факту сообщают руководству, что ИТ-процесс достиг предъявляемых бизнес-требований.

Ключевые Индикаторы Цели выражаются в терминах информационных критериев:

- Пригодность информации, необходимой для поддержки бизнеса;
- Риски отсутствия целостности и конфиденциальности;
- Рентабельность процессов и операций;
- Подтверждение надежности, эффективности и согласованности.

Ключевыми Индикаторами Цели, могут быть:

- Улучшение управления производительностью и стоимостью;
- Увеличение дохода от инвестиций в ИТ;

- Сокращение времени запуска в продажу нового продукта или услуги;
- Улучшение управления качеством, новшествами и рисками;
- Соответствующая интеграция и стандартизация бизнес-процессов;
- Поиск новых и удовлетворение существующих клиентов;
- Выполнение требований и ожиданий клиента по бюджету и времени;
- Соответствие законам, инструкциям, промышленным стандартам и договорным обязательствам;
- Полное осознание меры принимаемого риска, а также соответствие уровню риска, приемлемого для данной организации;
- Эталонное тестирование зрелости управления ИТ.

КЛЮЧЕВЫЕ ИНДИКАТОРЫ РЕЗУЛЬТАТА

Описывают комплекс действий, необходимых для определения, насколько ИТ-процессы достигают поставленных целей.

Ключевыми Индикаторами Результата, могут быть:

- Увеличение рентабельности ИТ-процессов;
- Улучшение работы и планирования действий по совершенствованию ИТ-процессов;
- Увеличение нагрузки на ИТ-инфраструктуру;
- Повышение степени удовлетворения пользователей (опросы пользователей и количество жалоб);
- Улучшение взаимодействия и коммуникаций между руководителями ИТ и руководством организации;
- Повышение производительности сотрудников (в том числе, повышение морального духа).

Выводы:

- Модели зрелости предназначены для стратегического выбора и эталонного сравнения;
- Критические Факторы Успеха предназначены для организации контроля ИТ-процессов;
- Ключевые Индикаторы Цели предназначены для контроля достижения целей ИТ-процессов;
- Ключевые Индикаторы Результата предназначены для контроля результатов каждого ИТ-процесса.