ОСНОВНЫЕ ПОНЯТИЯ И КОНЦЕПЦИЯ АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ.

- **Аудит —** Что такое аудит? Что под этим термином понимается? Определений как таковых много, на мой взгляд, наиболее лаконичным и верным по сути является трактовка Комитета Американской бухгалтерской ассоциации по основным концепциям учета: "Аудит — это системный процесс получения и оценки объективных данных об экономических действиях и событиях, устанавливающий уровень их соответствия определенному критерию и предоставляющий результаты заинтересованным пользователям".

- **Информационная инфраструктура -** это прежде всего отлаженная система, выполняющая функции обслуживания, контроля, учета, анализа, документирования всех процессов, протекающих в информационной системе.

- **Аудит информационной системы (ИС) -** это системный процесс получения и оценки объективных данных о текущем состоянии информационной системы, действиях и событиях, происходящих в ней, устанавливающий уровень их соответствия определенному критерию и предоставляющий результаты заказчику.

- **Стандарт аудита —** нормативно-технический документ (или эталон, модель, которая является отправной точкой), устанавливающий комплекс требований и правил к объекту аудита, квалификации исполнителей, организации аудита, методическим приемам анализа документации и представлению аудиторского заключения в предметной области и т.д.
- **Методика аудита —** совокупность теоретических и практических способов проведения аудита, разработанные аудитором на базе стандартизированных правил и норм проведения аудита в предметной области, в определенной степени, на основе личного профессионального опыта.

- **Информационно-коммуникационные технологии —** совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей.
- **Информационные системы—** организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

ISACA

Information Systems Audit and Control Association или Ассоциация Аудита и Контроля Информационных Систем (**ISACA**) была основана в 1969 году для финансовых аудиторов в контроле ИТ. Ассоциация Аудита и Контроля Информационных Систем является ведущей мировой профессиональной организацией с представительствами в более чем 100 странах мира и охватывает все уровни ИТ:

- Организации;
- Управления;
- Практического применения.

COBIT

- **Control Objectives for Information and Related Technologies** или же Контрольные Объекты для Информационных и смежных Технологий. За этой аббревиатурой скрывается набор документов, в которых изложены принципы управления и аудита информационных технологий. **CobiT** позиционируется как открытый стандарт "де-факто", в настоящее время переживающий свое третье издание.

В состав стандарта входят шесть книг, ориентированных 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. С переводом этой книги на русский язык Вы можете ознакомиться: **http://www.isaca.ru**
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.

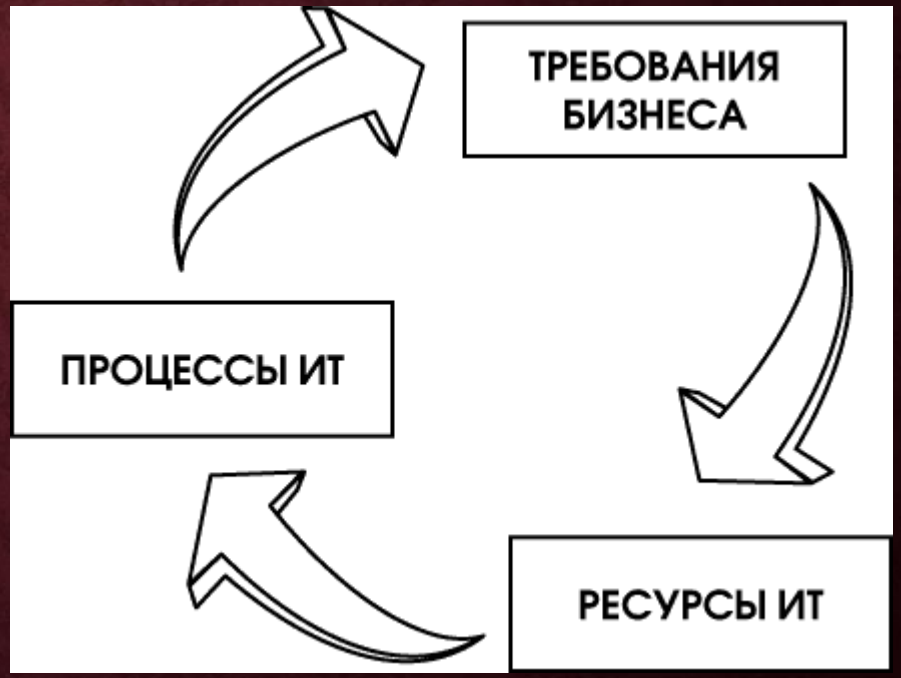

РЕЗЮМЕ для РУКОВОДИТЕЛЯ
Набор инструментов для внедрения CobiT
Обзор
Практический опыт
FAQ's
Презентации Power Point
Руководство по внедрению
- Контроль понимания руководства
- Диагностика ИТ Контроля
СТРУКТУРА CobiT включая Высокоуровневые Цели Контроля
ПРИНЦИПЫ УПРАВЛЕНИЯ
ОБЪЕКТЫ КОНТРОЛЯ
ПРИНЦИПЫ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

Модель процессов, выстраиваемая на базе **CobiT**, предпочтительней других подходов, в основе которых не лежат бизнес-процессы организации (методики и стандарты аудита производителей программно-аппаратных средств), по нескольким причинам:

1. По определению: процесс — это действие, направленное на достижение результата, при оптимальном использовании ресурсов, и которое может корректироваться при его выполнении. При выполнении процесса все задействованные ресурсы структурируются и выстраиваются таким образом, чтобы максимально эффективно выполнять этот процесс.
2. Во-вторых, процессы в подавляющем большинстве организаций, а особенно их цели не так часто изменяются, по сравнению с организационными объектами (организационно-штатная структура: сотрудники, отделы, департаменты и т.д.).
3. В-третьих, развертывание информационной системы или внедрение информационных технологий не может быть ограничено спецификой одного отдела или департамента, а затрагивает руководителей, пользователей из других подразделений и ИТ-специалистов.

ОСНОВА COBIT. РАЗДЕЛЕНИЕ COBIT НА УПРАВЛЕНИЕ И АУДИТ

В основу стандарта CobiT положено следующее утверждение: **для предоставления информации, необходимой организации для достижения ее целей, ресурсы ИТ должны управляться набором естественно сгруппированных процессов.**



Для этого CobiT выделяет 34 высокоуровневые цели контроля, по одной на каждый ИТ- процесс, которые сгруппированы в 4 домена: Планирование и Организация; Проектирование и Внедрение; Эксплуатация и Сопровождение; Мониторинг. Предлагаемая структура объединяет все аспекты информации и технологий, поддерживающих ее. Применяя 34 высокоуровневые цели контроля, руководитель может быть уверен, что ему будет предоставлена адекватная система контроля над ИТ-средой, которая учитывает задействованные ресурсы ИТ, дающая возможность оценить ИТ по предлагаемым CobiT семи критериям оценки информации.

Ресурсы ИТ в **CobiT** описаны пятью составляющими:

1. Данные — объекты в широком смысле (то есть внутренние и внешние), структурированные и неструктурированные, а также графика, звук и т.д.
2. Приложения — совокупность автоматизированных и выполняемых вручную процедур.
3. Технология — аппаратное обеспечение, программное обеспечение, операционные системы, системы управления базами данных, сетью и мультимедиа.
4. Оборудование — все ресурсы, создающие и поддерживающие информационные технологии.
5. Люди — персонал, его навыки: умение планировать и организовывать, комплектовать, обслуживать и контролировать информационные системы и услуги.

Критерии оценки информации:

- **Эффективность —** актуальность информации, соответствующего бизнес-процесса, гарантия своевременного и регулярного получения правильной информации.
- **Продуктивность —** обеспечение доступности информации с помощью оптимального (наиболее продуктивного и экономичного) использования ресурсов.
- **Конфиденциальность —** обеспечение защиты информации от неавторизованного ознакомления.
- **Целостность —** точность, полнота и достоверность информации в соответствии с требованиями бизнеса.
- **Пригодность —** предоставление информации по требованию бизнес-процессов.
- **Согласованность —** соответствие законам, правилам и договорным обязательствам.
- **Надежность —** доступ руководства организации к соответствующей информации для текущей деятельности, для создания финансовых отчетов и оценки степени соответствия.

Для достижения целей организации в сфере ИТ, **CobiT** включает в себя две основные книги, которые отражают Принципы управления и Принципы аудита.

Как следует из названия — это две части одного целого (оказание воздействия и контроль результатов). Управляем — воздействуем на ИТ для достижения поставленных целей. Аудит — контролируем достижение цели.

УПРАВЛЕНИЕ ИТ ПО COBIT

1. Управление ИТ осуществляется с учетом бизнес-потребностей.
2. Для управления ИТ определены информационные критерии.

Потребности бизнеса определяются Ключевыми Индикаторами Цели, чему способствует организация постоянного контроля над всеми ресурсами ИТ. Достижение необходимого уровня контроля измеряется Ключевыми Показателями Результата, которые учитывают Критические Факторы Успеха.

Модель Зрелости используется для оценки уровня управления ИТ в данной организации — от несуществующего (самый низкий уровень) до оптимизированного (самый высокий уровень).

Для достижения пятого, "оптимизированного" уровня зрелости в управлении ИТ организация должна быть, по крайней мере, на пятом уровне в домене мониторинг и как минимум на четвертом уровне моделей зрелости для всех других доменов.

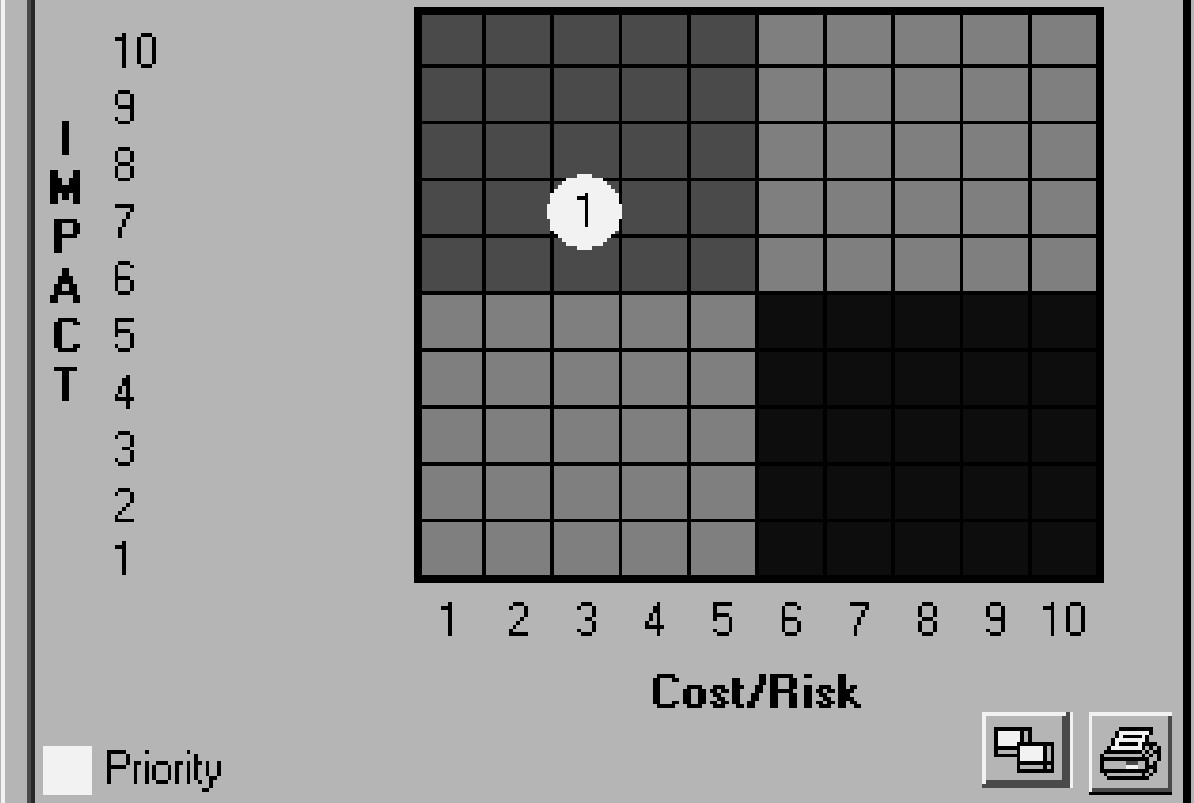
ПРИНЦИПЫ АУДИТА ИТ, СТАНДАРТ COBIT

Принципы аудита CobiT — книга стандарта, которая в большей степени ориентирована на аудит ИТ-процессов, чем на аудит конкретных функций или приложений. **CobiT** состоит из высокоуровневых целей контроля (определенных для ИТ-процессов организации), которые охватывают все параметры информационных систем и применяемых информационных технологий, учитывают цикл жизни и специфические задачи, решаемые ИТ.

COBIT ADVISOR 3RD EDITION (AUDIT)

Navigation | Reports | Sub-Domains | Projects | Actions | CSFs | KGIs | KPIs | Graphs | Outline

Maturity Assessment | Maturity Gap Assessment | KPI Gap | CSF Gap | KGI Gap | Project Priority | Actions Priority



Rank	Name	Risk	Impact	Priority
1	Strategic Plan Update	3	7	High

High Priority Moderate Priority Low Priority

ЭТИЧЕСКИЙ КОДЕКС АУДИТОРА (АССОЦИАЦИЯ ISACA)

1. Содействовать приведению информационных систем в соответствие с принятыми стандартами и руководствами;
2. Осуществлять свою деятельность в соответствии со стандартами в области аудита информационных систем, принятыми THE INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA);
3. Действовать в интересах работодателей, акционеров, клиентов и общества в старательной, лояльной и честной манере;
4. Сознательно не принимать участия в незаконной, либо недобросовестной деятельности;
5. Сохранять конфиденциальность информации, полученной при выполнении своих должностных обязанностей;
6. Не использовать конфиденциальную информацию для получения личной выгоды и не передавать ее третьим лицам без разрешения ее владельца;
7. Выполнять свои должностные обязанности, оставаясь независимым и объективным;

8. Избегать деятельности, которая ставит под угрозу независимость аудитора;
9. Поддерживать на должном уровне свою компетентность в областях знаний, связанных с проведением аудита информационных систем, принимать участие в профессиональных мероприятиях;
10. Проявлять добросовестность при получении и документировании фактографических материалов, на которых базируются выводы и рекомендации аудитора;
11. Информировать все заинтересованные стороны о результатах проведения аудита;
12. Способствовать повышению осведомленности руководства организаций, клиентов и общества в вопросах, связанных с проведением аудита информационных систем;
13. Соответствовать высоким этическим стандартам в профессиональной и личной деятельности;
14. Совершенствовать свои личные качества.

СТРУКТУРА ПРИНЦИПОВ АУДИТА COBIT

Для каждого ИТ-процесса, определенного **CobiT**, в **Принципах аудита** представлена следующая информация.

Секция высокого уровня принципов аудита **CobiT** отражает:

1. Название бизнес-процесса;
2. Требования бизнеса (Объекты контроля высокого уровня);
3. Как осуществлять контроль;
4. Что учитывать.

Для перехода на уровень детального аудита ИТ-процесса:

1. Детальные объекты контроля;
2. Как понять ИТ-процесс (кому задавать вопросы);
3. Как оценить контроль ИТ-процесса;
4. Как оценить соответствие этого контроля — управлению;
5. Как доказать риск не выполнения целей управления.

На практике при проведении аудита для каждого ИТ-процесса ИТ-аудитору, как минимум необходимо выполнить следующую работу:

1. Определить высокоуровневый объект контроля;
2. Определить ИТ-процесс;
3. Проанализировать границы аудита;
4. Определить детальные объекты контроля;
5. Провести интервью с сотрудниками (ориентировочные названия должностей для каждого объекта контроля приведены в принципах управления);
6. Назначить задания на оценку средств контроля (Принято ли во внимание ...);
7. Оценить соответствие;
8. Проверить доказательства.