

Принципы проведения аудита информационных технологий

Принципы проведения аудита информационных технологий

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.

Секция высокого уровня принципов аудита CoBIT отражает:

- ▶ Название бизнес-процесса;
- ▶ Требования бизнеса (Объекты контроля высокого уровня);
- ▶ Как осуществлять контроль;
- ▶ Что учитывать.

Для перехода на уровень детального аудита ИТ-процесса:

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

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

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

Структура и содержание типового проекта аудита информационных технологий.

В обобщенном виде ИТ-аудит проводится в два этапа:

- ▶ этап "Планирование ИТ-аудита".
- ▶ этап "Проведение ИТ-аудита".

На этапе "Планирования ИТ-аудита":

Анализируются:

- ▶ структура бизнес-процессов;
- ▶ платформы и структура информационных систем, поддерживающих бизнес-процессы;
- ▶ структура ролей и распределения ответственности, включая аутсорсинг;
- ▶ бизнес-риски и бизнес-стратегия.

Определяются информационные критерии, наиболее значимые для существующих бизнес-процессов.

Идентифицируются ИТ-риски.

Оценивается общий уровень контроля рассматриваемых бизнес-процессов.

На основе полученной информации осуществляется выбор границ и объектов исследования: ИТ-процессов и связанных с ними ИТ-ресурсов.

На этапе "Проведения ИТ-аудита" выполняются следующие виды работ:

- ▶ Идентификация существующих механизмов управления и документирование процедур (сбор и первичный анализ информации);
- ▶ Оценка эффективности существующих механизмов управления при выполнении задач управления, их целесообразность и пригодность;
- ▶ Тест соответствия (получение гарантий пригодности существующих механизмов управления для решения задач управления);
- ▶ Детальное тестирование с целью выполнения корректирующих действий для улучшения состояния системы управления ИТ.

Принципы проведения аудита.

- ▶ 1) Целостность. Является основой профессионализма. Аудиторам и лицу, осуществляющему управление программой аудита, следует: осуществлять свою работу честно, старательно и ответственно; выявлять все применимые правовые требования и действовать в соответствии с ними; демонстрировать свою компетентность при выполнении своей работы; осуществлять свою работу беспристрастно, т.е. сохранять справедливость и объективность в отношении всего, с чем приходится иметь дело; быть чувствительными к любым воздействиям, которые, как можно ожидать, окажут давление на выработку суждений при проведении аудита.

- ▶ 2) **Беспристрастное представление результатов.** Является обязательством представлять правдивые и точные отчеты. Результатам аудита, заключениям по аудиту и отчетам об аудитах следует правдиво и точно отражать деятельность по проведению аудитов. Существенные препятствия, встретившиеся в ходе аудита, а также неразрешенные расходящиеся мнения и разногласия между командой по аудиту и аудируемой организацией следует отражать в отчете. Коммуникации следует быть честной, точной, объективной, своевременной, понятной и полной.

- ▶ 3) Надлежащая профессиональная тщательность. Означает приложение усердия (прилежания) и проявление рассудительности при проведении аудита. Аудиторам следует проявлять заботу о тщательности, которая должна соответствовать важности выполняемого ими задания и доверию, оказываемому им заказчиком аудита и другими заинтересованными сторонами. Важным фактором осуществления их деятельности с надлежащей профессиональной тщательностью является наличие способности вырабатывать здравые суждения во всех ситуациях, возникающих во время аудита,

- ▶ 4) Конфиденциальность. Означает обеспечение безопасности полученной информации. Аудиторам следует проявлять осторожность в использовании информации, запрашиваемой в связи с осуществляемой ими деятельностью, и защищать ее. Информацию, полученную в ходе аудита, не следует использовать в целях получения выгоды для аудиторов или заказчика аудита или таким образом, который наносит ущерб законным интересам аудируемой организации. Данный подход включает в себя должное обращение с «чувствительной» или конфиденциальной информацией.


- ▶ 5) Независимость. Это основа беспристрастности при проведении аудита и объективности заключений по аудиту. Аудиторам, где это только возможно, следует быть независимыми от деятельности, которая будет подвергаться аудиту, и во всех случаях действовать таким образом, чтобы быть свободными от предвзятости и конфликта интересов. При проведении внутренних аудитов аудиторам следует быть независимыми от руководителей функциональных структур, подлежащих аудиту. Аудиторам следует сохранять объективность во время всего процесса аудита для обеспечения того, чтобы результаты аудита и заключения по аудиту были основаны только на свидетельствах аудита. Для малых организаций, возможно, будет достаточно того, чтобы внутренние аудиторы были полностью независимыми от деятельности, подвергаемой аудиту, но при этом следует приложить все усилия, чтобы исключить предвзятость и обеспечить объективность.

- ▶ 6) Подход, основанный на свидетельствах. Является разумным способом получения надежных и воспроизводимых заключений по аудиту в процессе систематически проводимых аудитов. Свидетельствам аудита следует быть верифицируемыми. Они в общем случае будут базироваться на выборках доступной (полученной в распоряжение) информации, поскольку аудит проводится в ограниченный период времени и с ограниченными ресурсами. Следует использовать соответствующие (уместные, подходящие) выборки примеров, поскольку это сильно влияет на доверие к заключениям по аудиту.

Инициирование, формирование информационной базы аудита.

Информационной базой аудита могут быть:

- ▶ · Первичные документы субъекта хозяйствования и третьих лиц;
- ▶ · Регистры бухгалтерского учета;
- ▶ · Результаты анализа финансово-хозяйственной деятельности компании;
- ▶ · Результаты анализа на основе сопоставления одних документов или данных компании с другими, а также сопоставление документов или данных компании с документами и данными третьих лиц;
- ▶ · Результаты инвентаризации имущества компании;
- ▶ · Финансовая отчетность;
- ▶ · Материалы арбитражных или судебных дел;
- ▶ · Устные пояснения сотрудников компании и третьих лиц.

- 
- ▶ Согласно п.13 МСА 230 «аудитор должен принять соответствующие процедуры для соблюдения конфиденциальности и обеспечения сохранности рабочих документов и их хранения в течение необходимого периода времени, достаточного для удовлетворения потребностей практики, а также в соответствии с правовыми и профессиональными требованиями, предъявляемыми к хранению записей».

Данный стандарт дает минимальный перечень сведений, который необходим для отражения в рабочих документах аудитора. Рабочие документы должны содержать:

- ▶ Информацию, касающуюся юридической и организационной структуры субъекта;
- ▶ Извлечения из важных юридических документов, договоров и протоколов или копии таких документов;
- ▶ Информацию от отрасли, экономической конъюнктуры и правовой базе, в условиях которых субъект осуществляет свою деятельность;
- ▶ Положения о бухгалтерской службе, системе внутреннего контроля на предприятии;
- ▶ Доказательства, подтверждающие оценку неотъемлемого риска, риска контроля и любых изменений этих оценок;
- ▶ Доказательства, подтверждающие факт рассмотрения аудитором работы службы внутреннего аудита и сделанных выводов;
- ▶ Анализ операций и сальдо счетов;
- ▶ Анализ значимости коэффициентов и тенденций;
- ▶ Описание характера, сроков и объема выполненных аудиторских процедур и результатов таких процедур;
- ▶ Копии корреспонденции с другими аудиторами, экспертами и третьими сторонами;
- ▶ Письма-представления, полученные от субъекта;
- ▶ Копии финансовой отчетности и аудиторского отчета.

При возможности аудитор может использовать комплекты документов, подготовленные клиентом.

Для удобства в последующей работе (при повторных проверках) архивные документы целесообразно разделять на два типа:

- ▶ · Документы постоянного архива;
- ▶ · Документы текущего архива.

В постоянный архив могут включаться следующие материалы (по разделам):

- ▶ Данные об организации;
- ▶ Протоколы и материалы общих собраний и заседаний Совета директоров, правления;
- ▶ Юридические документы постоянного характера;
- ▶ Заключение по предшествующему аудиту;
- ▶ Материалы по организации учета и внутреннего контроля;
- ▶ Отчеты по ценным бумагам;
- ▶ Анализы.

Постоянные архивы должны все время обновляться и не иметь бесполезных и устаревших материалов.

Текущая аудиторская папка заводится для отражения данных запланированной работы, а также проделанной работе, включая: осуществляемые процедуры, проведенные тесты, собранную информацию, полученные выводы.

В текущих архивах хранятся все рабочие документы, разрабатываемые, составляемые или копируемые в ходе аудита.

В текущий архив включаются по разделам:

- ▶ План проведения аудита;
- ▶ Проверяемая финансовая (налоговая и иная) отчетность;
- ▶ Все рабочие документы, подшиваемые по счетам, в соответствии с планом счетов.

Все документы должны быть надежно закреплены в папках текущего и постоянного архива, на папках казано название аудиторской организации.

Оценка соответствия требованиям стандартов.

- ▶ В случае проведения аудита безопасности на соответствие требованиям стандарта, аудитор, полагаясь на свой опыт, оценивает применимость требований стандарта к обследуемой ИС и ее соответствие этим требованиям. Данные о соответствии различных областей функционирования ИС требованиям стандарта, обычно, представляются в табличной форме. Из таблицы видно, какие требования безопасности в системе не реализованы. Исходя из этого, делаются выводы о соответствии обследуемой ИС требованиям стандарта и даются рекомендации по реализации в системе механизмов безопасности, позволяющих обеспечить такое соответствие.

Выработка рекомендаций.

- ▶ Рекомендации, выдаваемые аудитором по результатам анализа состояния ИС, определяются используемым подходом, особенностями обследуемой ИС, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита.
- ▶ В любом случае, рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности. При этом мероприятия по обеспечению защиты организационного уровня практически всегда имеют приоритет над конкретными программно-техническими методами защиты.
- ▶ В то же время, наивно ожидать от аудитора, в качестве результата проведения аудита, выдачи технического проекта подсистемы информационной безопасности, либо детальных рекомендаций по внедрению конкретных программно-технических средств защиты информации. Это требует более детальной проработки конкретных вопросов организации защиты, хотя, внутренние аудиторы могут принимать в этих работах самое активное участие.

Структура отчета по результатам аудита и анализу рисков.

1. Вводная часть

1.1. Введение

1.2. Цели и задачи проведения аудита

1.3. Описание ИС

1.3.1. Назначение и основные функции системы

1.3.2. Группы задач, решаемых в системе

1.3.3. Классификация пользователей ИС

1.3.4. Организационная структура обслуживающего персонала ИС

1.3.5. Структура и состав комплекса программно-технических средств ИС

1.3.6. Виды информационных ресурсов, хранимых и обрабатываемых в системе

1.3.7. Структура информационных потоков

1.3.8. Характеристика каналов взаимодействия с другими системами и точек входа

1.4. Границы проведения аудита

1.4.1. Компоненты и подсистемы ИС, попадающие в границы проведения аудита

1.4.2. Размещение комплекса программно-технических средств ИС по площадкам (помещениям)

1.4.3. Основные классы угроз безопасности, рассматриваемых в ходе проведения аудита

1.5. Методика проведения аудита

1.5.1. Методика анализа рисков

1.5.2. Исходные данные

1.5.3. Этапность работ

1.6. Структура документа

2. Оценка критичности ресурсов ИС

2.1. Критерии оценки величины возможного ущерба, связанного с осуществлением угроз безопасности

2.2. Оценка критичности информационных ресурсов

2.2.1. Классификация информационных ресурсов

2.2.2. Оценка критичности по группам информационных ресурсов

2.3. Оценка критичности технических средств

2.4. Оценка критичности программных средств

2.5. Модель ресурсов ИС, описывающая распределение ресурсов по группам задач

- 3. Анализ рисков, связанных с осуществлением угроз безопасности в отношении ресурсов ИС
 - 3.1. Модель нарушителя информационной безопасности
 - 3.1.1. Модель внутреннего нарушителя
 - 3.1.2. Модель внешнего нарушителя
 - 3.2. Модель угроз безопасности и уязвимостей информационных ресурсов
 - 3.2.1. Угрозы безопасности, направленные против информационных ресурсов
 - 3.2.1.1. Угрозы несанкционированного доступа к информации при помощи программных средств
 - 3.2.1.2. Угрозы, осуществляемые с использованием штатных технических средств
 - 3.2.1.3. Угрозы, связанные с утечкой информации по техническим каналам
 - 3.2.2. Угрозы безопасности, направленные против программных средств
 - 3.2.3. Угрозы безопасности направленные против технических средств
 - 3.3. Оценка серьезности угроз безопасности и величины уязвимостей
 - 3.3.1. Критерии оценки серьезности угроз безопасности и величины уязвимостей
 - 3.3.2. Оценка серьезности угроз
 - 3.3.3. Оценка величины уязвимостей
 - 3.4. Оценка рисков для каждого класса угроз и группы ресурсов

4. Выводы по результатам обследования

5. Рекомендации

5.1. Рекомендуемые контрмеры
организационного уровня

5.2. Рекомендуемые контрмеры программно-
технического уровня