ПРОВЕДЕНИЕ АУДИТА
информационных технологий

В КАКИХ СЛУЧАЯХ НЕОБХОДИМ АУДИТ ИТ

Несколько аргументов в пользу целесообразности привлечения внешнего консультанта.

Независимый внешний взгляд

Внешняя объективность, непредвзятость.

Уникальные знания

Знание предметной области, отраслевой специфики и российского законодательства.

Уникальный опыт

Опыт реализации проектов различного масштаба с использованием апробированной методики, основанной на лучших мировых и российских практиках.

Наличие компетенций

Наличие специалистов, сертифицированных в области аудита ИТ, управления проектами.

Ведение проектов в соответствии с рекомендациями COBIT, PMBoK.

Оперативность

Выполнение проекта в сжатые сроки с требуемым качеством.

Как правило, аудит ИТ проводится в следующих случаях:

- при подготовке к масштабным преобразованиям и структурным изменениям бизнеса (сделки слияния/поглощения, смена собственников, реинжиниринг бизнес-процессов, региональная экспансия);
- перед крупной реструктуризацией ИТ-службы (централизация/децентрализация, реорганизация, внедрение процессного подхода, модернизация, аутсорсинг ИТ, внедрение корпоративной ИС);
- перед формированием/актуализацией стратегии развития ИТ;
- при необходимости оценить деятельность ИТ-службы на предмет соответствия стандартам и лучшим мировым практикам (ITIL/ITSM, COBIT, ISO 20000);
- при подготовке к сертификации (например, ISO 9000, ISO 27000, SOX).

Исходя из вышеперечисленных случаев необходимости проведения аудита ИТ, в качестве потребителей данной услуги могут выступать:

- собственники бизнеса;
- вышестоящие структуры (ведомства, управляющие компании);
- высшее руководство компании (Совет директоров, Правление, курирующие руководители);
- руководство ИТ-службы компании.

Форматы проведения аудита ИТ

Аудит ИТ в зависимости от требований Заказчика может проводиться в различных форматах.

Инвентаризация ИТ

Проводится, когда требуется оперативная оценка имеющихся ресурсов по следующим направлениям:

- Анализ ИТ-инфраструктуры.
- Анализ используемого программного обеспечения.

Обследование (экспресс-анализ) ИТ

Обычно предшествует структурным преобразованиям бизнеса или ИТ и проводится по отдельным областям:

- Анализ эффективности используемых прикладных ИС на предмет покрытия требуемой функциональности.
- Анализ текущей организационно-функциональной структуры ИТ-службы с точки зрения ее оптимальности и соответствия возложенным на нее задачам.
- Анализ эффективности управления ИТ-процессами на предмет соответствия лучшим практикам.
- Анализ текущих ИТ-проектов на предмет соответствия стратегии развития бизнеса.
- Анализ системы внутреннего контроля ИТ и системы управления рисками, связанными с ИТ.
- Анализ эффективности инвестиций в ИТ с точки зрения оптимизации затрат.

Комплексный аудит ИТ

Проводится в целях всестороннего анализа текущего состояния ИТ и в случае необходимости принятия стратегических решений относительно дальнейшего развития ИТ. Затрагивает в той или иной степени все аспекты, перечисленные выше.

Целевая аудитория – компании, организации и предприятия крупного и среднего масштаба.

Финансовый сектор

- *Банки с государственным участием.*
- *Коммерческие банки.*
- *Страховые компании.*
- *Инвестиционные фонды.*

Государственные структуры

- *Государственные корпорации.*
- *Федеральные органы законодательной и исполнительной власти.*
- *Муниципальные органы.*
- *Государственные унитарные предприятия.*
- *Государственные организации и учреждения.*

Промышленный сектор

- *Промышленные холдинги.*
- *Предприятия ТЭК.*
- *Транспортные компании/корпорации.*
- *Строительные корпорации.*

При планировании инвестиционных сделок (приобретение/продажа/слияние/поглощение) или при масштабной передаче ИТ-сервисов на аутсорсинг, ИТ рассматриваются в качестве одного из важных компонентов, определяющих стоимость бизнеса. В таких случаях востребована специальная форма аудита – **IT Due Diligence**, позволяющая получить информацию об ИТ для принятия решений в сфере управления инвестиционными рисками.

В рамках этой услуги выполняются следующие работы: оценка ИТ-активов (включая лицензии на ПО), ИТ-инфраструктуры; анализ внешних поставщиков услуг и контрактов, ИТ-процессов и ИТ-сервисов, политик и регламентов ИТ-службы, структуры управления и квалификации сотрудников ИТ-службы, текущих ИТ-проектов, технологической поддержки непрерывности бизнеса и бизнес-стратегии; оценка бизнес- и ИТ-рисков.

IT Due Diligence позволяет оценить текущее состояние ИТ, провести анализ потенциального объединения/передачи/развития ИТ, определить зоны рисков и предоставить объективную оценку инвестору, покупателю или аутсорсинговой компании о состоянии ИТ.

СТАНДАРТЫ И ЛУЧШИЕ ПРАКТИКИ

Международные стандарты и лучшие практики адаптируются и используются с учетом отраслевой специфики и в соответствии с требованиями российского законодательства.

Управление и внутренний контроль

COBIT (Control Objectives for Information and related Technology) – Методология управления, контроля и аудита ИТ.

COSO (The Committee of Sponsoring Organizations of the Treadway Commission) – Концептуальные основы внутреннего контроля организаций.

SOX 404 (Sarbanes-Oxley Act) – Статья 404 акта Сарбейнса-Оксли, определяющая требования к внутреннему контролю.

Управление проектами

PMBoK (The Project Management Body of Knowledge) – Свод знаний по управлению проектами.

PRINCE2 (Projects IN Controlled Environments v.2) – Методология управления проектами.

Управление информационной безопасностью

СТО БР ИББС – Стандарт Банка России “Обеспечение ИБ организаций банковской системы Российской Федерации”.

ISO 27000 – ИТ. Методы обеспечения безопасности. Системы управления информационной безопасностью.

Управление рисками

BS 25999 – Управление непрерывностью бизнеса.

BS 25777 – Управление непрерывностью информационных и коммуникационных технологий.

COSO ERM (COSO Enterprise Risk Management) – Концептуальные основы управления рисками организаций.

Управление сервисами

ITIL/ITSM (IT Infrastructure Library/IT Service Management) – Библиотека передового опыта управления ИТ, основанная на процессном подходе и сервисной организации.

ISO 20000 – Управление ИТ-сервисами.

ЭТАПЫ РАБОТ

Состав и продолжительность работ могут варьироваться в зависимости от формата проведения аудита ИТ, целей и ограничений проекта, масштаба обследуемой компании.

Ниже приводится базовый состав работ.

1. Организация и планирование

Осуществляется:

- Разработка плана управления проектом.
- Разработка и согласование шаблонов результатов проекта.
- Формирование проектных команд со стороны Заказчика и Консультанта.
- Проведение общего установочного совещания.

2. Обследование и анализ

Осуществляется:

- Формирование, получение и обработка запросов на предоставление информации.
- Планирование и проведение интервью с руководством компании, руководством ИТ-службы, представителями ключевых ИТ- и бизнес-подразделений.
- Анализ, оценка и документирование собранных свидетельств аудита.
- Согласование документированных свидетельств аудита с руководителями обследуемых подразделений.
- Уточнение необходимой информации с помощью дополнительных запросов.

3. Подготовка итогового отчета

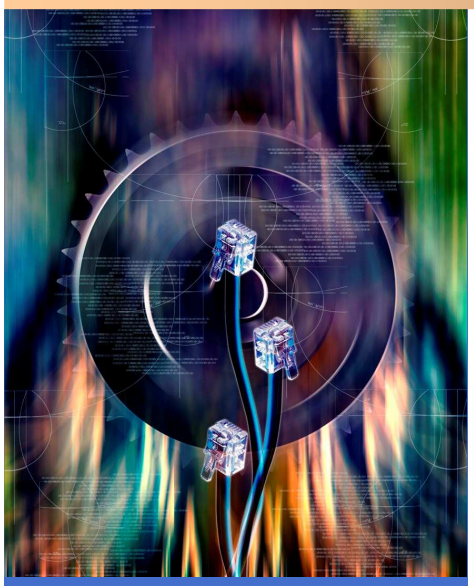
Осуществляется:

- Подготовка разделов итогового отчета.
- Формирование выводов по результатам анализа.
- Формирование рекомендаций.
- Согласование разделов итогового отчета с Заказчиком.
- Предоставление и презентация итогового отчета руководству Заказчика.

Как правило, запросы на предоставление исходной информации включают следующие темы:

- *Стратегия развития бизнеса.*
- *Специфика и объемные показатели бизнеса.*
- *Существующие регламенты в соответствии с корпоративными политиками и стандартами в области управления качеством, управления рисками, внутреннего контроля.*
- *Существующие и целевые клиентские сегменты.*
- *Региональная сеть.*
- *Структура управления компании.*
- *Прикладные системы.*
- *ИТ-инфраструктура.*
- *Реестр текущих и планируемых в краткосрочной перспективе ИТ-проектов.*
- *Структура управления ИТ-службы.*
- *Политики, процедуры и регламенты ИТ-службы.*

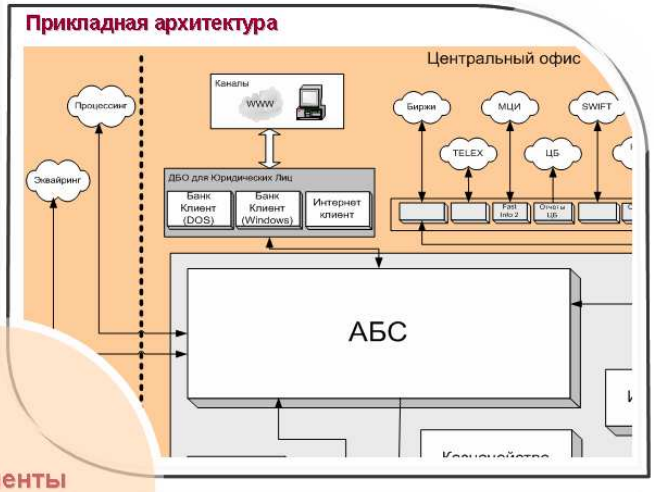
РЕЗУЛЬТАТЫ РАБОТ



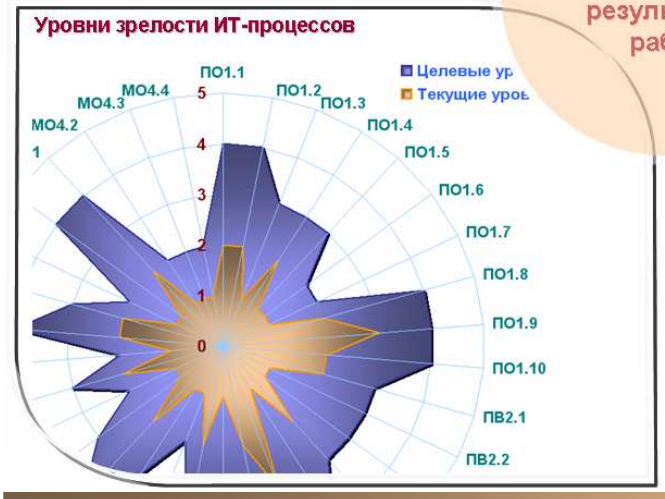
По результатам аудита формируется “Отчет о состоянии ИТ”, содержащий результаты анализа всех свидетельств аудита, выводы и рекомендации.

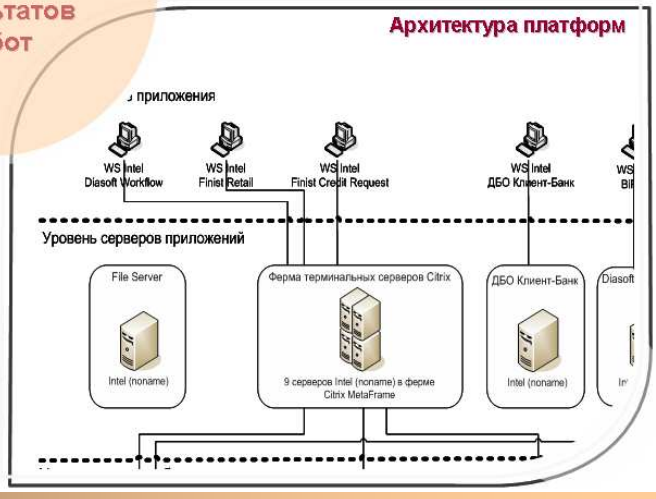
Основные разделы “Отчета о состоянии ИТ”

- **Бизнес-архитектура** – отражает уровни зрелости информационных систем (степень покрытия потребностей бизнес-направлений функциональностью ИС).
- **Системная архитектура** – включает описание прикладной архитектуры ИС (схемы взаимодействия прикладных систем), архитектуру данных ИС, техническую архитектуру ИС.
- **ИТ-инфраструктура** – отражает уровни соответствия ИТ-инфраструктуры требованиям производительности, надежности, безопасности, отказоустойчивости, катастрофоустойчивости.
- **Управление ИТ** – включает описание текущей структуры управления ИТ-службы, уровней зрелости ИТ-процессов, степени удовлетворенности бизнеса качеством ИТ-сервисов.
- **ИТ-проекты** – содержит описание уровней зрелости организации проектного управления, соответствия целей ИТ-проектов стратегии развития компании.
- **Анализ рисков и факторов успеха** – содержит выводы о выявленных проблемах и причинах их возникновения, выводы о положительных решениях и тенденциях.
- **Рекомендации** – включает рекомендации по основным объектам аудита (структура управления ИТ-службы, управление ИТ-процессами, политики и стандарты ИТ, ИТ-инфраструктура, системная архитектура, аутсорсинг ИТ).



Фрагменты результатов работ





ДОСТИГАЕМЫЕ ПРЕИМУЩЕСТВА

Проведение аудита ИТ способствует достижению конкурентных преимуществ по основным аспектам деятельности.

Стратегическое управление

- Получение независимой экспертной оценки состояния ИТ, учитывающей мнение как ИТ-, так и бизнес-подразделений, и позволяющей принимать адекватные управленческие решения.
- Получение оценки соответствия ИТ стратегическим целям компании, возможности технологической поддержки предстоящих масштабных изменений структуры бизнеса.

Управление рисками

- Выявление проблемных областей и бизнес-рисков, связанных с ИТ, получение рекомендаций по их устранению и минимизации.
- Получение рекомендаций по обеспечению непрерывного функционирования ИТ.

Внутренний контроль

- Получение оценки степени адекватности средств контроля ИТ, системы информационной безопасности.
- Получение рекомендаций по совершенствованию системы внутреннего контроля на основе лучших практик.

Управление ИТ

- Получение рекомендаций по построению эффективной системы управления ИТ, оптимизации структуры управления ИТ-службы.
- Понимание текущих и целевых уровней зрелости ИТ-процессов, получение рекомендаций по мероприятиям для достижения целевых уровней зрелости ИТ-процессов.

Управление ИС

- Выявление проблем, связанных с разрывами в ИТ-поддержке бизнеса, отсутствием/недостаточностью автоматизации бизнес-процессов, дублированием функциональности ИС.

Управление ИТ-инфраструктурой

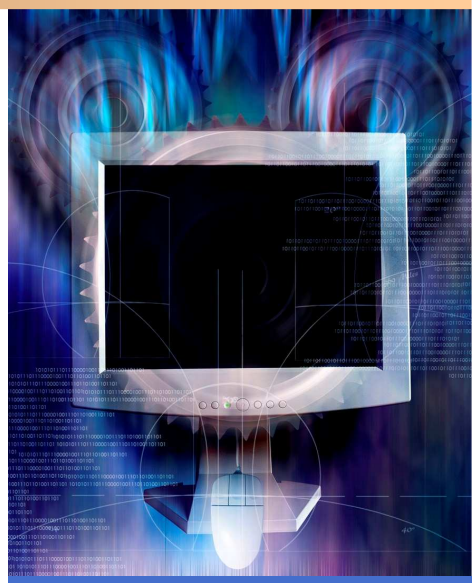
- Выявление дополнительных возможностей по эффективному использованию имеющихся ИТ-ресурсов.
- Получение рекомендаций по оптимальной модернизации элементов ИТ-инфраструктуры исходя из перспектив бизнеса.

Управление ИТ-проектами

- Получение оценки эффективности проектного управления и рекомендаций по совершенствованию.

Управление затратами на ИТ

- Оценка эффективности и целевого использования ИТ-ресурсов компании, сохранение инвестиций в ИТ.
- Получение возможности долгосрочного планирования и прогнозирования затрат и отдачи от ИТ.



В ходе обследования проводится ряд интервью как с представителями ИТ-подразделений, так и с представителями бизнес-подразделений.

В частности, в ходе обследования осуществляется анализ бизнес-архитектуры, включая основные и обеспечивающие бизнес-процессы.

Проблемы анализируются как по характеру возникновения (организационные, отсутствие функциональности, отсутствие интеграции компонент ИС, технические), так и по характеру влияния (сдерживание бизнеса, уровень качества обслуживания клиентов, зависимость от персонала, риск рекламаций и штрафов со стороны надзорных органов, потеря управления бизнесом).

Такой подход позволяет собрать больший объем свидетельств аудита, получить объективную оценку состояния ИТ, выявить бизнес-риски, связанные с ИТ.

О КОМПАНИИ ОТР

Кто мы

ОТР (ООО "Организационно-технологические решения 2000") – ведущая российская консалтинговая компания в сфере информационных технологий и системной интеграции, специализирующаяся на предоставлении комплексных ИТ-решений для финансовых организаций, государственных структур и промышленных предприятий.

Компания ОТР имеет лицензии, необходимые для выполнения работ лицензии ФСБ России.

В ОТР существует система адаптации международных отраслевых стандартов (PMBoK, ITIL, COBIT, ISO 9001) для их успешного использования в работе с отечественными заказчиками.

Система менеджмента качества компании ОТР соответствует требованиям международного стандарта ISO 9001:2000.

ISO 9001:2000 CERTIFIED

Наш опыт проведения аудита ИТ

Банк России

АК БАРС БАНК

ТрансКредитБанк

НОМОС БАНК

СКБ-БАНК

Еврофинанс Моснарбанк

БАНК СОЮЗ

МЕТКОМБАНК
МЕТАЛЛУРГИЧЕСКИЙ КОММЕРЧЕСКИЙ БАНК

РосЕвроБанк
АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК

МИБ
МЕЖРЕГИОНАЛЬНЫЙ ИНВЕСТИЦИОННЫЙ

АВТОБАНК-НИКОЙЛ
комплексный финансовый сервис

ГУТА БАНК

IRKUT
ИРКУТ

MOSTRO

Контактная информация по услуге

Руководитель практики ИТ-консалтинга
Правильщиков Максим Павлович

Тел: +7 (495) 222-59-05
E-mail: itc@otr.ru
Сайт: www@otr.ru