

Новое в международных стандартах информационной безопасности. Проблемы внедрения стандартов и аудита ИБ в России

ADVISORY

Андрей Дроздов, CISM, CISA,
вице-президент ISACA в России

Старший менеджер KPMG
Москва

30 ноября 2005

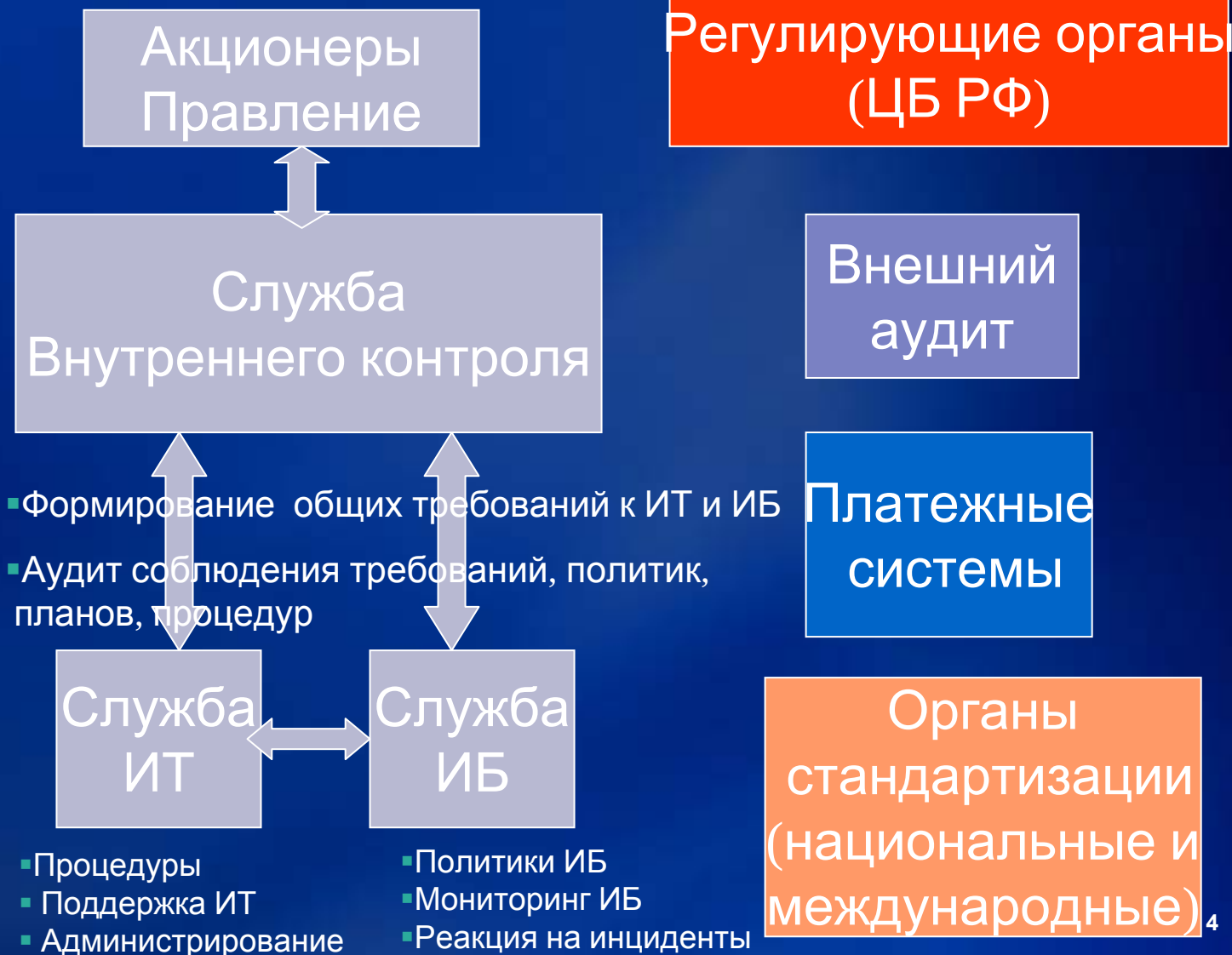
Краткое содержание

- ◆ Цели аудита ИБ
- ◆ Основные стандарты ISO17799, BS 7799, Cobit, Стандарт ИБ Банка России
- ◆ Преимущества для Компании
- ◆ Требования к аудиторам ИБ (ЕА 7/03)
- ◆ Сертификационный аудит ИБ по BS 7799
- ◆ Развитие ISO 17799 и BS 7799 (ISO 27001:2005)
- ◆ Проблемы внедрения ISO 17799/ISO 27001 в России
- ◆ Стандарт Банка России vs. ISO 17799/ISO 27001
- ◆ Вопросы?

Цели аудита ИБ

- ◆ Соответствие бизнес-целям компании
- ◆ Совершенствование ISMS
- ◆ Требования законодательства и регулирующих органов (242-п, SOX, Basel II)
- ◆ Требования клиентов и деловых партнеров

Кто проводит мониторинг и аудит ИБ?



Стандарты и методологии

- ◆ Стандарт Банка России
- ◆ ISO 17799, BS 7799 (ISO 27001)
- ◆ Cobit (в особенности DS4, DS5)
- ◆ EA 7/03

Что такое информационная безопасность?



Что такое информационная безопасность?

◆ Ключевые аспекты программы ИБ:

- Люди – организация, права, обязанности, руководство
- Процесс – политики, процедуры и практика
- Технология – масштабируемая поддержка технических решений автоматизации, включающая возможности обеспечения безопасности.

◆ **Важно:** Безопасность – не только и не столько техническая проблема.

Что такое информационная безопасность?

- ◆ ИБ- метод, посредством которого организация обеспечивает *контроль* над данными и системами, обеспечивая защиту ИТ и поддержку бизнес-процессов.

Предыстория ISO 17799

◆ Стандарт лучшей практики.

UK Department of Trade and Industry (DTI)



- Британский стандарт (BS7799)
- утвержден Британским институтом стандартов



- KPMG один из со-авторов стандарта, обладает правами сертификации



◆ Принят как ISO 17799 (часть 1 BS 7799) в декабре 2000, 15 июня 2005; ISO 27001 (часть 2 BS7799) 15 октября 2005

Что такое ISO 17799?

- ◆ Набор контролей лучшей практики ИБ
- ◆ Политики и процедуры, основанные на контролях
- ◆ Измеримость
- ◆ Возможность сертификации
- ◆ Основан на анализе рисками
- ◆ Международное признание

Новое в ISO 17799:2005

◆ 11 Областей стандарта

- Управление непрерывностью бизнеса
- Контроль доступа
- **Закупка**, разработка и сопровождение систем
- Физическая безопасность и защита от воздействий окружающей среды
- Соответствие требованиям
- Вопросы ИБ, относящиеся к персоналу
- Организация безопасности

Новое в ISO 17799:2005

◆ 11 областей стандарта (продолжение)

- Управление операционными процессами и коммуникациями
- Управление активами
- Политика безопасности
- Управление инцидентами ИБ

Новое в ISO 17799:2005

- ◆ 9 мер контроля модифицировано
- ◆ 116 мер контроля сохранено
- ◆ 17 новых мер контроля добавлено. Фокус на оценке рисков
- ◆ Формат текста (контроль, руководство по внедрению, другая информация)
- ◆ Стилль изложения

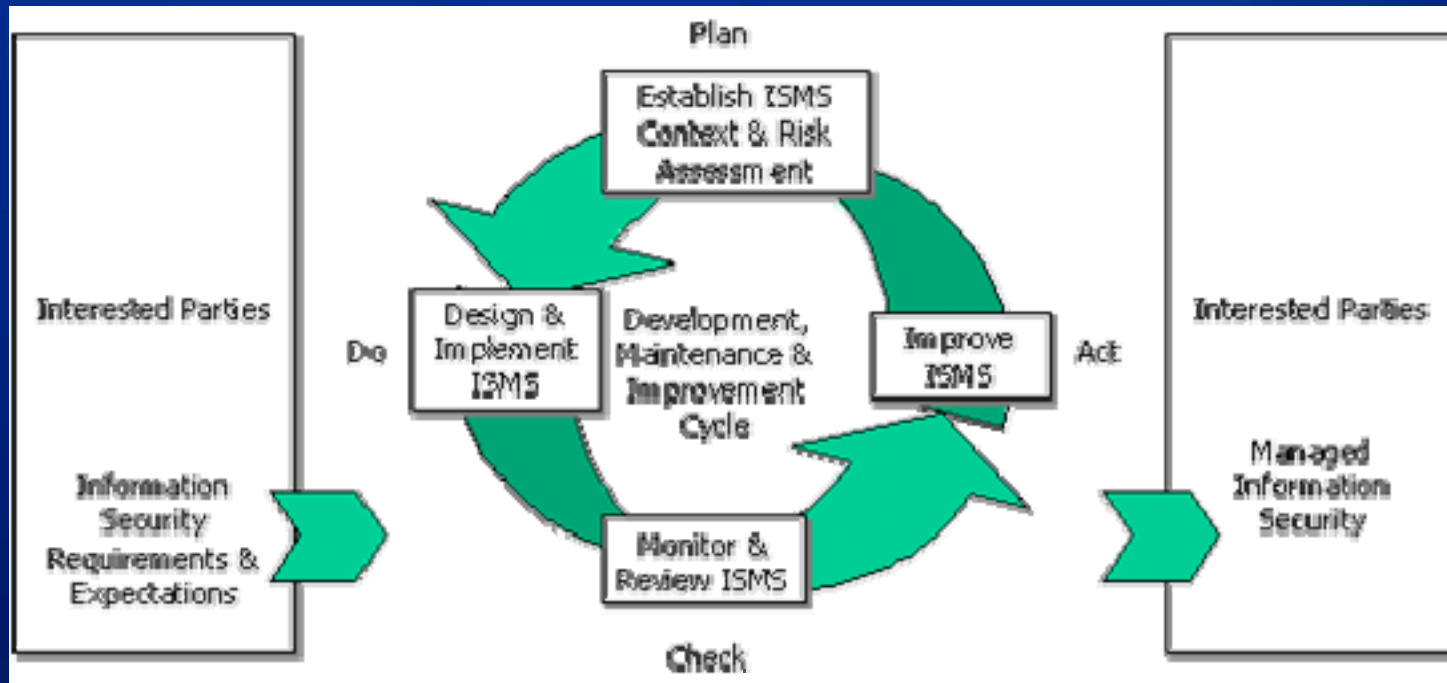
Внедрение стандарта ISO 17799



Модель КПМГ

BS 7799 Part 2-2002 (ISO 27001:2005)

Внедрение, мониторинг и аудит СУИБ



Новое в BS 7799 (ISO 27001:2005)

- ◆ Соответствует ISO 17799:2005
- ◆ Приложение “B” удалено
- ◆ Фокус на оценке рисков при выборе и оценке эффективности мер контроля
- ◆ Стилль изложения

Преимущества для компании

- ◆ Стандартизация, лучшая практика
- ◆ Управление рисками
- ◆ Эффективность затрат
- ◆ Превентивный подход
- ◆ Утвержденная корпоративная политика ИБ
- ◆ Участие и поддержка высшего руководства

Преимущества для компании

- ◆ Совершенствование процессов
- ◆ Соблюдение требований клиентов и партнеров
- ◆ Соответствие законодательству
- ◆ Способ оценки эффективности ИБ (ROI!)
- ◆ Маркетинговые и конкурентные преимущества
 - клиенты
 - партнеры
 - инвесторы
 - страховщики

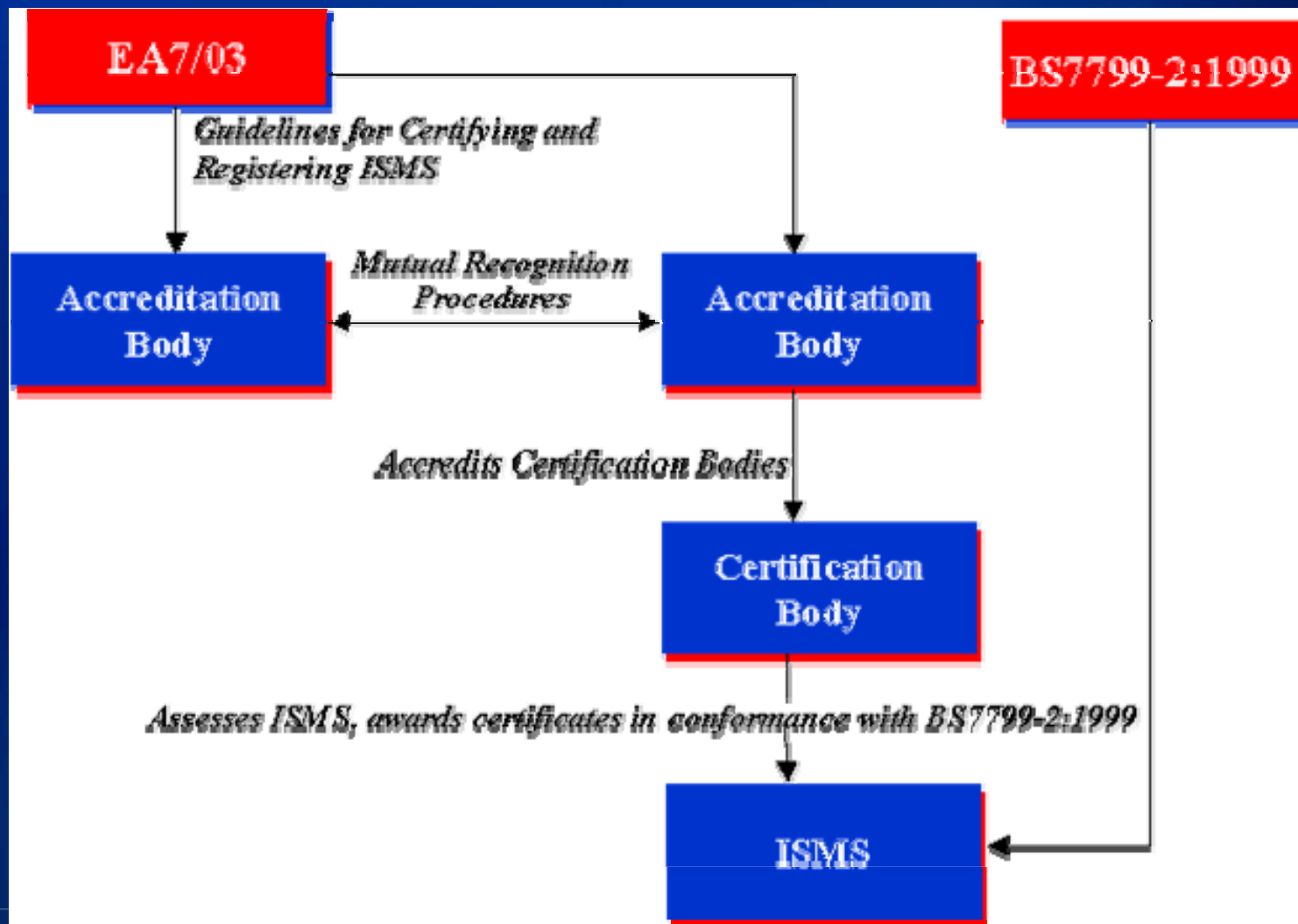
Внедрение международных стандартов ИБ

- ◆ Идентификация имеющихся недостатков по требованиям ISO 17799/27001
- ◆ Определение необходимых приоритетов и мероприятий с целью внедрения требований ISO17799/27001
- ◆ Разработка плана внедрения стандарта
- ◆ Реализация плана
- ◆ Достижение соответствия требованиям ISO 17799/27001 !
- ◆ Постоянные усовершенствования с целью минимизации рисков

Сертификация по BS 7799 (ISO 27001)

- ◆ Что сертифицируем?
- ◆ Сертификация по BS 7799/ ISO 27001
- ◆ Кто уполномочен проводить “настоящую” сертификацию и выдавать сертификат?
- ◆ Возможна ли официальная сертификация в России и странах СНГ?
- ◆ Как организован процесс сертификации?
- ◆ Сколько ресурсов потребуется?

Общая схема сертификации по международным стандартам



Требования к аудиторской организации (ЕА-7/03)

- Аккредитация в соответствующем государственном органе (в UK – UKAS)
- Юридическое лицо
- Компетентность
- Независимость и беспристрастность
- Наличие системы контроля качества
- Наличие политик и процедур

Требования к аудиторам (ЕА-7/03)

- ◆ Высшее образование
- ◆ 4 года опыта в ИТ, из них 2 в ИБ
- ◆ Трейнинги
- ◆ Опыт в 4 проектах
- ◆ Личные профессиональные качества

Процесс сертификации



KPMG - Услуги по сертификации

- ◆ **Услуги по сертификации предлагаются....**
В Великобритании с 2000 года, Теперь в России и СНГ!
- ◆ **Оценка и сертификация СУИБ для компаний, заинтересованных в получении независимого заключения о соответствии международным стандартам**
- ◆ **Цель ?.....**
Предоставления комплексного решения
- ◆ **Ресурсы ?.....**
квалифицированные сотрудники KPMG в Москве и Великобритании.
- ◆ **Уникальность услуг в Большой Четверке.**

Преимущества KPMG

- ◆ В отношении BS 7799:Часть 2 уже существует процедура и аккредитация при UKAS в соответствие с документами ISO (ISO Guide 62 and EA7/03), которые включают Euro Norm Standard (EN 45012).
- ◆ Со-редакторы стандарта – своевременный учет всех изменений
- ◆ Поддержка действия сертификата (включая переоформления на ISO 27001)
- ◆ Присутствие KPMG во всем мире (включая Россию и страны СНГ). Гарантия, что высокий уровень сервиса предоставляется всем клиентам, независимо от географического положения.
- ◆ Ориентация на бизнес

Преимущества KPMG

◆ Максимально широкие рамки проекта

- KPMG обладает уникальной возможностью обеспечить полное решение по BS 7799, включая консультации, сертификацию и последующую поддержку сертификата при обеспечении надлежащего уровня независимости.

◆ Брэнд

- Существенно, что сертификат, полученный через KPMG имеет дополнительную ценность как полученный через всемирно признанного лидера. Сертификат на соответствие с BS 7799/ISO 27001 поможет Вам получить большее доверие со стороны инвесторов и бизнес-партнеров.

Опыт сертификации по BS 7799

◆ Примеры проектов KPMG

- Link Interchange Network – Сеть банкоматов Великобритании.
- Britannic Money Plc – Провайдер услуг по ипотечным кредитам через Интернет.
- NUL Unisys (Japan) – Центр обработки данных для Финансовых институтов.
- Siemens Financial Services – UK
- DTI IMPE – Министерство промышленности и торговли Великобритании
- Symantec Security Services-UK, USA
- Обучение – курсы по подготовке аудиторов BS 7799

Проблемы внедрения ISO 17799/ISO 27001 в России

- ◆ Недостаточное внимание руководства к ИБ
- ◆ Культура ИБ в начальной стадии
- ◆ Низкий уровень зрелости СУИБ
- ◆ Стандарт универсальный, а не отраслевой
- ◆ Предполагает использование/разработку вспомогательных методик (оценка рисков), не описанных в стандарте
- ◆ Необязательный характер стандарта (обязательность только в Японии- 50% сертификаций в мире)
- ◆ Сертификационный аудит по принципу зачет/незачет
- ◆ Высокая стоимость внедрения и сертификации
- ◆ Дискредитация стандарта в России появлением технократических предложений по внедрению/аудиту/сертификации “a la BS7799”

Кому реально внедрить ISO 17799/ISO 27001 и быть сертифицированными в России

- ◆ Крупные организации, особенно с иностранными инвесторами и партнерами
- ◆ Достаточно высокий уровень зрелости СУИБ
- ◆ Наличие высококвалифицированных сотрудников ИБ, желательно со знанием английского языка и обладающими профессиональными сертификатами
- ◆ Выбор относительно небольшой области для сертификации

Стандарт ИБ Банка России. Достоинства

- ◆ Инициирован регулятором – ЦБ РФ
- ◆ Учитывает специфику банковской сферы РФ
- ◆ Дополняется методиками и примерами
- ◆ Аудит на соответствие на балльной основе (модель зрелости)

Стандарт ИБ Банка России. Проблемы

- ◆ “Болезни роста”
- ◆ Наследие терминологии ГОСТов
- ◆ Излишняя сложность и детерминированность методик внедрения и оценки
- ◆ Отсутствие аккредитованных аудиторских компаний
- ◆ Недостаточные стимулы для внедрения и аудита

Стандарт Банка России vs. ISO 17799/ISO 27001

- ◆ Внедрение и аудит по стандартам ISO и Банка России не противоречивы, а взаимодополняемы
- ◆ Для большинства кредитных организаций РФ – стандарт Банка РФ – реалистичный подход к построению СУИБ
- ◆ Для “продвинутых” кредитных организаций при непосредственном внедрении оригинальных стандартов ISO следует учитывать требования стандарта Банка России
- ◆ Внедрение и аудит соответствия по стандарту Банка России может дополняться сертификацией по ISO наиболее продвинутых областей.

Что делать?

- ◆ Пропаганда внедрения стандарта Банка России и международных стандартов
- ◆ Сообщество пользователей стандарта Банка России
- ◆ Стимулирование внедрения и подтверждения соответствия стандартам со стороны регулирующих органов и рынка

Вопросы





Контактная информация

Андрей Дроздов

KPMG

+7 (095) 937 4477

adrozdov@kpmg.ru

www.kpmg.ru

Информация, содержащаяся в настоящей презентации, носит общий характер и подготовлена без учета конкретных обстоятельств того или иного лица или организации. Хотя мы неизменно стремимся представлять своевременную и точную информацию, мы не можем гарантировать того, что данная информация окажется столь же точной на момент получения или будет оставаться столь же точной в будущем. Предпринимать какие-либо действия на основании такой информации можно только после консультаций с соответствующими специалистами и подробного анализа конкретной ситуации.