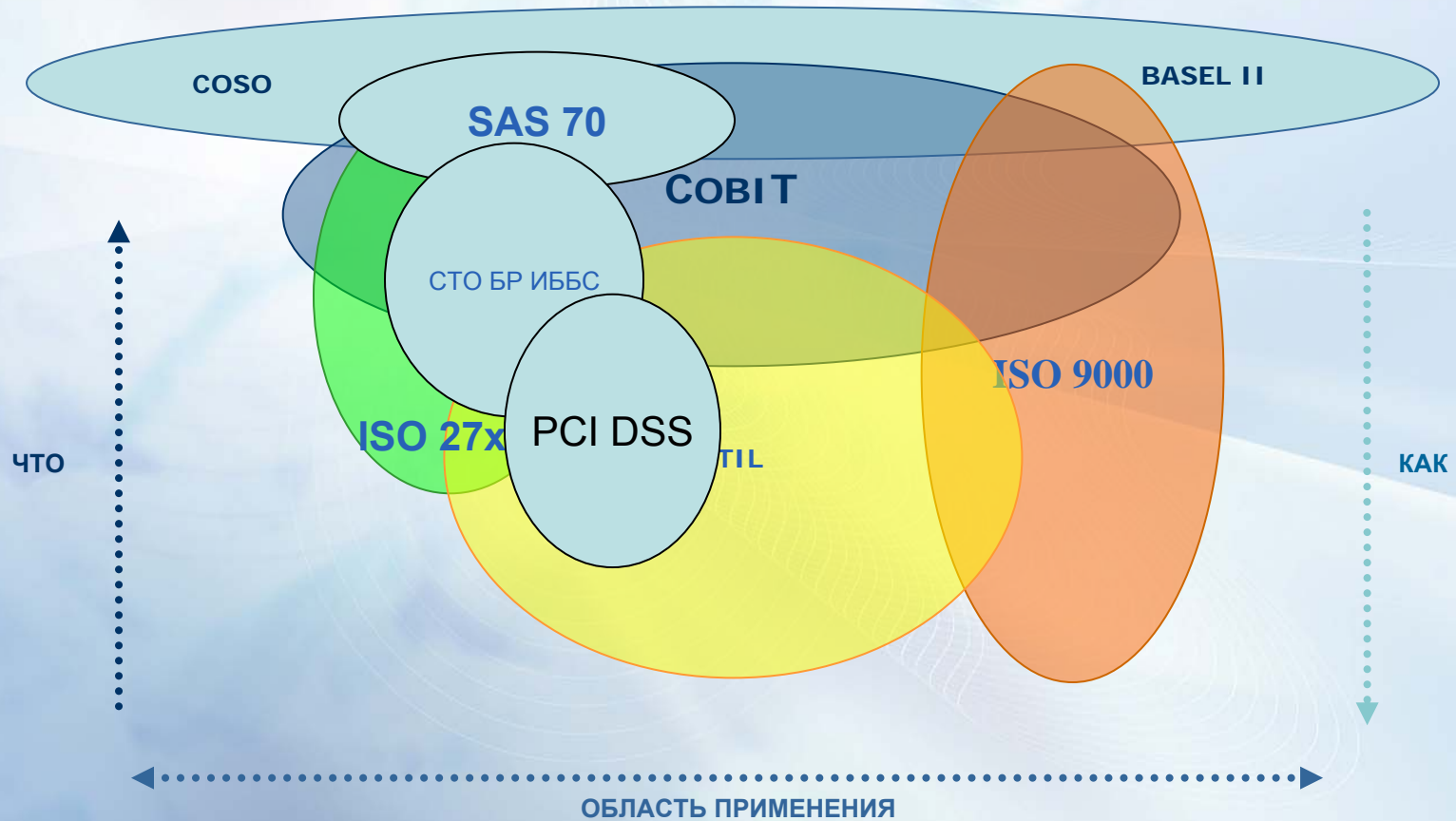


**Coso, Cobit, ISO 27001, SAS 70, ITIL,
Стандарт Банка России - интеграция и
признание международных и
национальных практик**

Андрей Дроздов, CISM, CISA, CGEIT
Старший менеджер КПМГ

Основные стандарты систем управления, связанные с ИТи ИБ



Общий подход к оценке системы управления и контроля



Свойства мер контроля

- **Дизайн**
Оценивается против стандартов и лучших практик
- **Эффективность**
Оценивается правильное срабатывание контрольных мер на выборке за период времени

Требования к системе управления и контроля и оценке

- Система соответствует стандарту
- Аудиторская организация соответствует стандарту
- Аудиторы соответствуют стандарту

Меры ИТ контроля разных уровней

Меры контроля уровня организации

Меры контроля уровня организации определяют общие политики. :

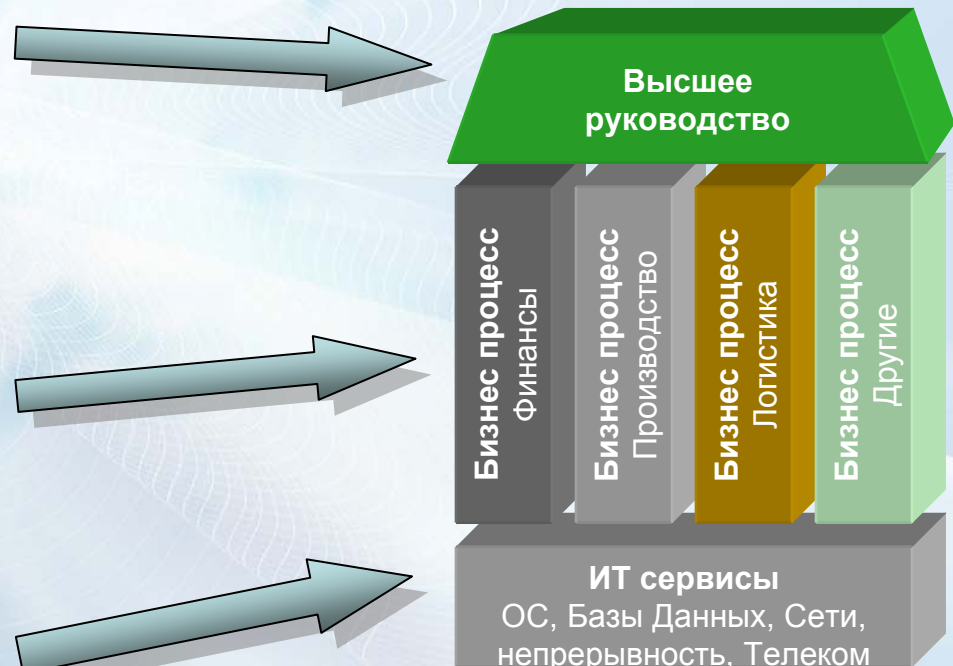
- Планирование развития систем
- Стиль операционной деятельности
- Корпоративные политики
- Корпоративное управление
- Обмен знаниями
- Кодекс корпоративной этики
- Предотвращение мошенничества

Средства контроля уровня приложений

- Разделение полномочий по транзакциям
- Пороговые лимиты значений
- Отчеты по сверкам
- Контроль при вводе данных

Общие меры контроля ИТ

- Поддержка систем
- Восстановление в случаях аварий и катастроф
- Физическая и логическая безопасность
- Управление данными
- Разрешение инцидентов



Размытые границы контролей

Закон Сарбейнса-Оксли, COSO и CobIT

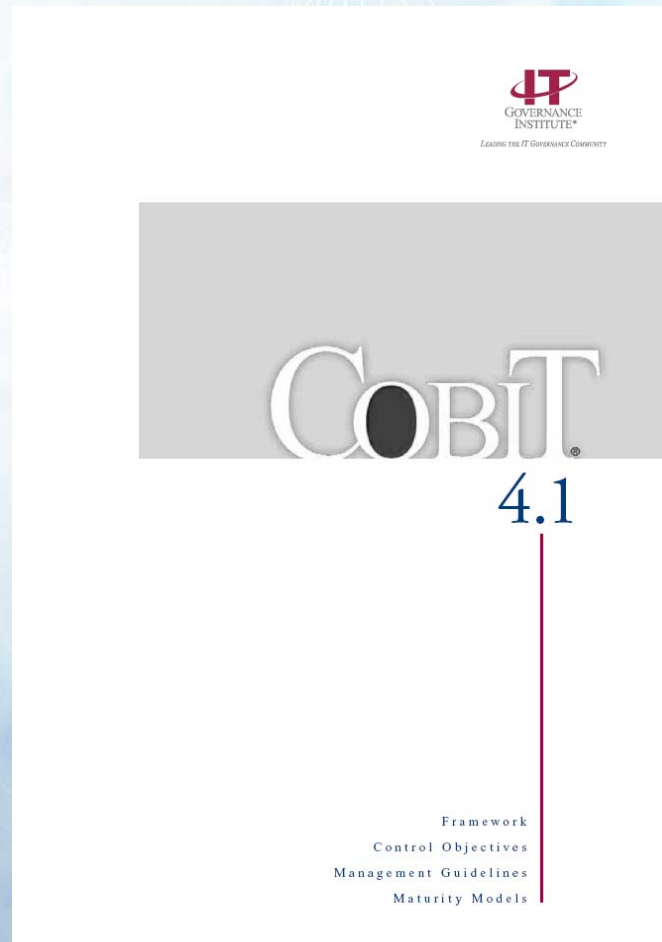


Меры контроля ИТ должны рассматривать основы Корпоративного управления для поддержки качества и целостности информации

Меры контроля ИТ относятся как к формированию финансовой отчетности, так и к требованиям раскрытия информации по закону Сарбейнса-Оксли

Компетентность во всех 5 областях COSO является необходимой для достижения интегрированной среды контроля

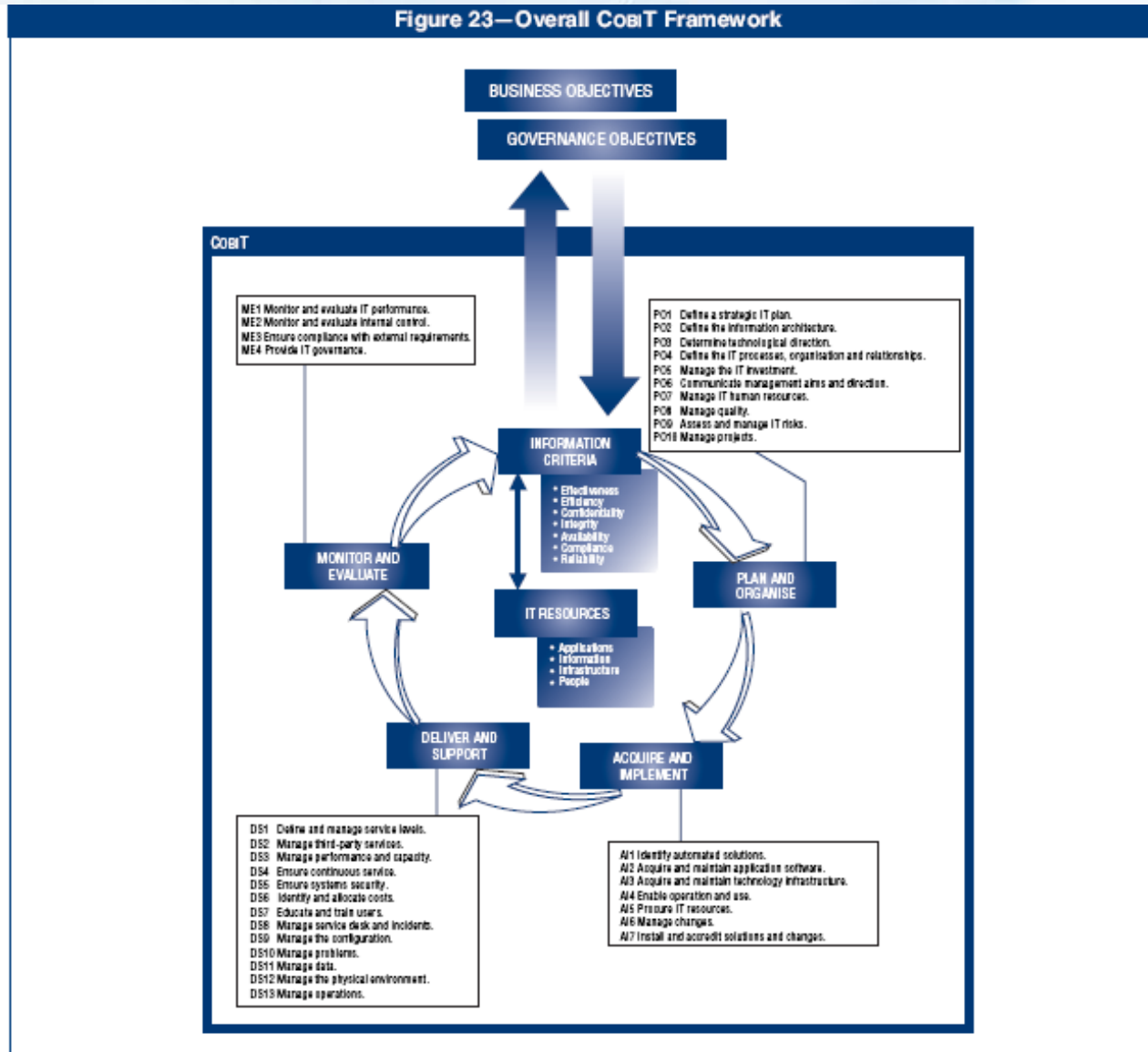
Cobit 4.1



Русский перевод – ссылка на www.isaca-russia.ru

Cobit 4.1

Figure 23—Overall CobIT Framework



ISO 27001

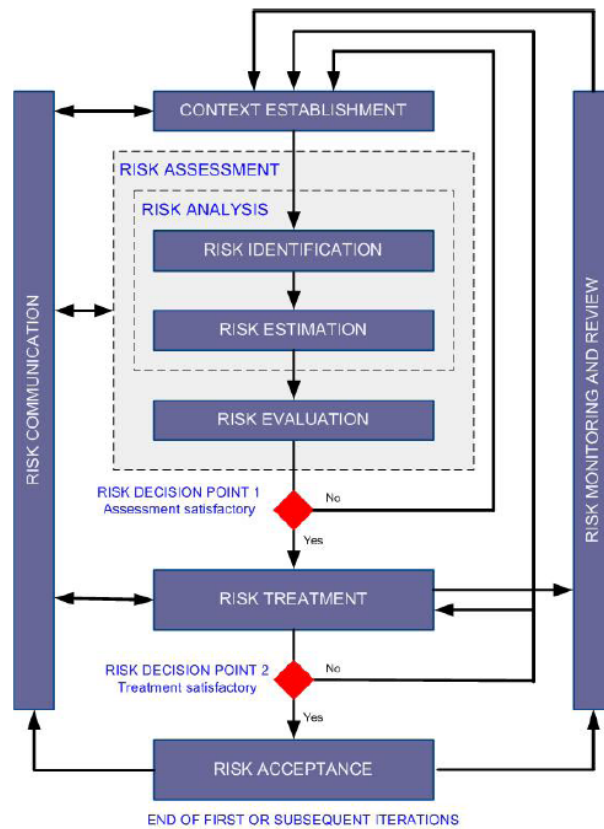


Взаимное сосуществование стандартов

- Стандарты должны применяться согласованно, особенно в пересекающихся областях
- Из соответствия стандартам низшего уровня не следует соответствие стандартам более высокого уровня
- Из соответствия стандартам верхнего уровня, как правило, следует соответствие стандартам более низкого уровня

ISO 27005

ISO/IEC FCD 27005



1

2

3

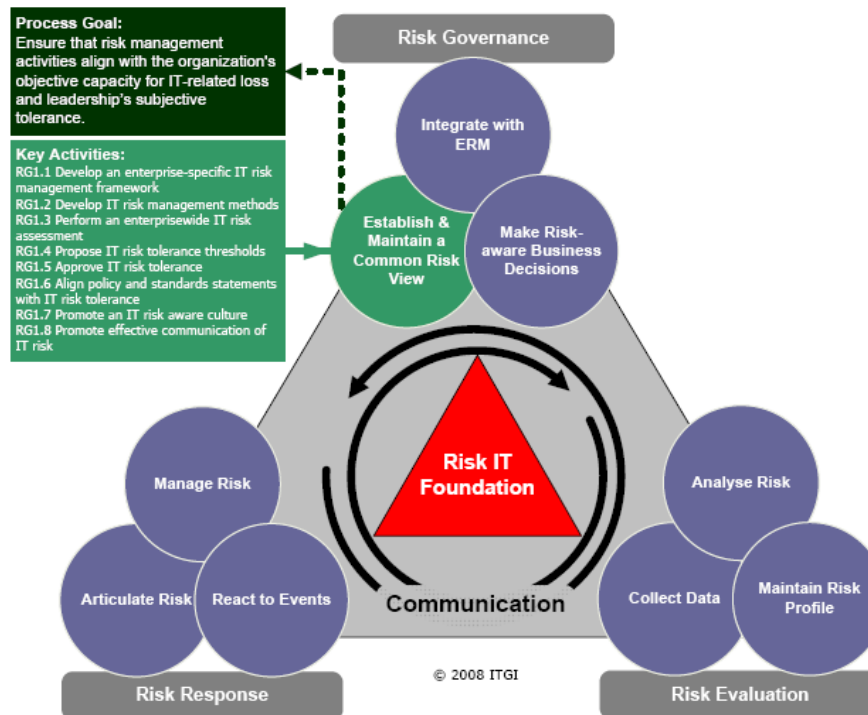
Figure 1 Information security risk management process

Модель управления ИТ рисками COBIT – интеграция с корпоративным рисками

**Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft
RG1 Establish and Maintain a Common Risk View Risk Governance**

PROCESS OVERVIEW

Figure 21—Process RG1 Establish and Maintain a Common Risk View



Ближайшие мероприятия по ИБ и ИТ

- *Круглый стол «Корпоративные ИТ в финансовой сфере: ценность для бизнеса и ключевые факторы успеха»
25 ноября 2009 года, Radisson SAS Славянская
Москва, Бережковская наб., 2
<http://www.in4media.ru>*

*Вторая межбанковская конференция
“Информационная безопасность банков”
15-20 февраля 2010 года
Республика Башкортостан
<http://www.ib-bank.ru/>*

Контакты докладчика

Андрей Дроздов

KPMG

+7 (495) 937 44 77

+7 (916) 104 15 77

adrozdov@kpmg.ru

www.kpmg.ru

The information contained herein [or insert the title of the presentation, report, or talkbook] is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.