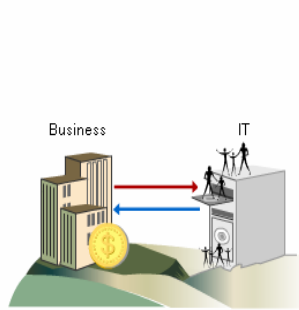


Обзор принципов Корпоративного управления ИТ на основе Cobit и других методологий ITGI

Андрей Дроздов, CISA, CISM, CGEIT
Вице-президент Московского отделения ISACA
Старший менеджер KPMG



Strategic Alignment



Poor Security Assurances



I can't access my account status.

Server

Безопасность

Непрерывность ИТ сервисов



Suppliers
Handling External Relationship

Управление комплексной средой



Project Execution Time

Цена/Качество

Соответствие ИТ целям бизнеса



Strategy

Соответствие регуляторным требованиям

Организациям необходим структурированный подход для управления этими и другими проблемами.

Такой подход позволит гарантировать согласованность целей бизнеса и ИТ, внедрение мер контроля в соответствии с лучшей практикой а также мониторинга эффективности ИТ.



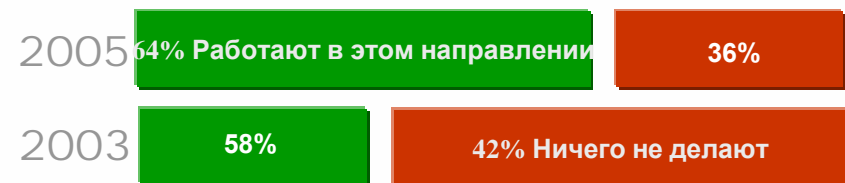
Корпоративное управление – комплекс управленческих решений и практик, применяемых высшим руководством, с целью:

- Определения **стратегического направления**
- Обеспечения достижения **целей**
- Адекватного управления **рисками**
- Надлежащего использования **корпоративных ресурсов**



Корпоративное управление ИТ:

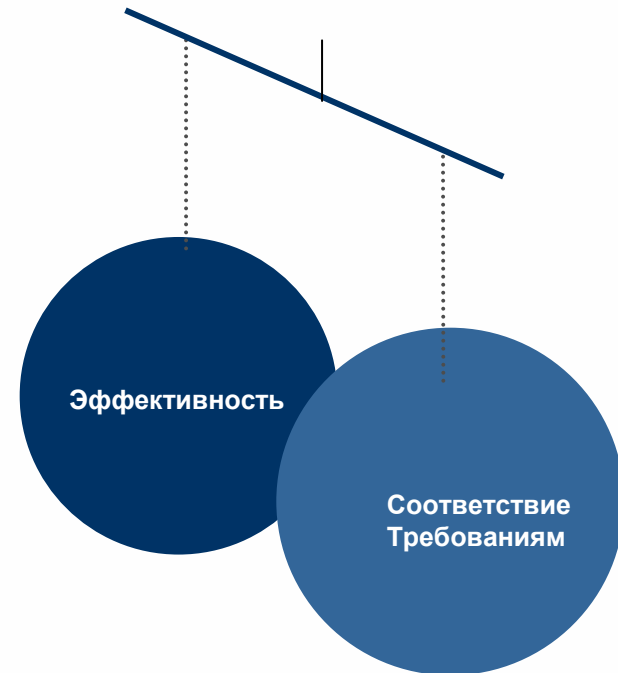
- Ответственность Совета Директоров и высшего руководства
- **Неотъемлемая часть** корпоративного управления, состоящая из руководства, организационных структур и процессов, обеспечивающих **соответствие ИТ** текущим и стратегическим целям организации



Source: Surveys by PwC for the IT Governance Institute Sep-Oct 2003 and Sep-Oct 2005

Корпоративное управление:

- ⊙ **Соответствие требованиям**
 - законодательства, внутренним политикам, требованиям аудита, и.т.д.
- ⊙ **Эффективность**
 - Повышение прибыльности, результативности, эффективности, динамики роста, и.т.д.



Корпоративное управление и управление ИТ требуют баланса между целями, связанными с необходимостью соответствия требованиям и повышения эффективности, установленными высшим руководством.

Strategic alignment

Направлено на обеспечение **соответствия бизнес и ИТ планов**; определение, поддержание и оценку **привносимой ИТ пользы**; а также **взаимосвязи ИТ операций и бизнес-операций**

Value delivery

Рассматривает **привносимую ИТ пользу** как цикл, обеспечивающий **достижение декларируемых преимуществ от ИТ в соответствии со стратегией**, с учетом оптимизации затрат

Resource management

Рассматривает оптимизацию инвестиций в ИТ и надлежащее управление **критичными ИТ ресурсами**: приложениями, информацией, инфраструктурой и персоналом. Ключевые проблемы относящиеся к **оптимизации знаний и инфраструктуры**.

Risk management

Необходимость осведомленности высшего руководства в области рисков, четкого понимания **корпоративного подхода в отношении рисков**, представления о **требованиях законодательства**, прозрачности в отношении существенных рисков, а также **включение функции управления рисками** в практику организации

Performance measurement

Мониторинг реализации стратегии, осуществления проектов, использования ресурсов, эффективности процессов и сервисов, с использованием, например, системы сбалансированных показателей, которые **транслируют стратегию в действия** направленные на достижение **измеримости достижения целей кроме традиционной отчетности**

Для успешного внедрения корпоративного управления ИТ необходимо:

- ⊙ Добиться, чтобы управление ИТ работало—реагирование на проблемы ИТ.
- ⊙ Максимальный фокус на повышение эффективности и достижение конкурентных преимуществ путем предотвращения проблем.
- ⊙ Достижение того, чтобы корпоративное управление ИТ стало совместной областью ответственности бизнеса (потребителя услуг) и поставщика ИТ услуг, при **полной поддержке и направлении со стороны Совета Директоров**.
- ⊙ Достижение согласованности управленческой модели ИТ и общего корпоративного управления организации.
- ⊙ Совет Директоров и высшее руководство должно расширить принципы общего корпоративное управление путем включения аспектов ИТ, обеспечив необходимое лидерство и организационные структуры, а также требовать внедрения должным образом управляемых и контролируемых процессов.

Совет Директоров и высшее руководство

Определение направлений развития ИТ, оценка результатов и требования по исправлению недостатков

Руководители бизнес- подразделений

Определение бизнес-требований к ИТ, обеспечение достижения пользы от ИТ и управление рисками

Руководство ИТ Служб

Обеспечение и совершенствование ИТ сервисов в соответствие с требованиями бизнеса

ИТ Аудит

Обеспечение независимой оценки, что ИТ предоставляет требуемые сервисы

Управление Рисками и Compliance

Оценка соответствия нормативным документам с учетом новых рисков

COBIT помогает заполнить разрывы между бизнес-рисками, требуемыми мерами контроля и техническими проблемами. Он приводит лучшие практики в различных областях и процессах, а также перечень требуемых задач для ИТ в стройной логической системе.

COBIT:

- ⊙ Основывается на требованиях бизнеса
- ⊙ Процессно-ориентированный, структурирующий задачи ИТ в общепринятую процессную модель
- ⊙ Идентифицирует основные необходимые ИТ ресурсы
- ⊙ Определяет необходимые цели контроля
- ⊙ Инкорпорирует основные международные стандарты
- ⊙ Стал *де факто* стандартом в области управления и контроля ИТ



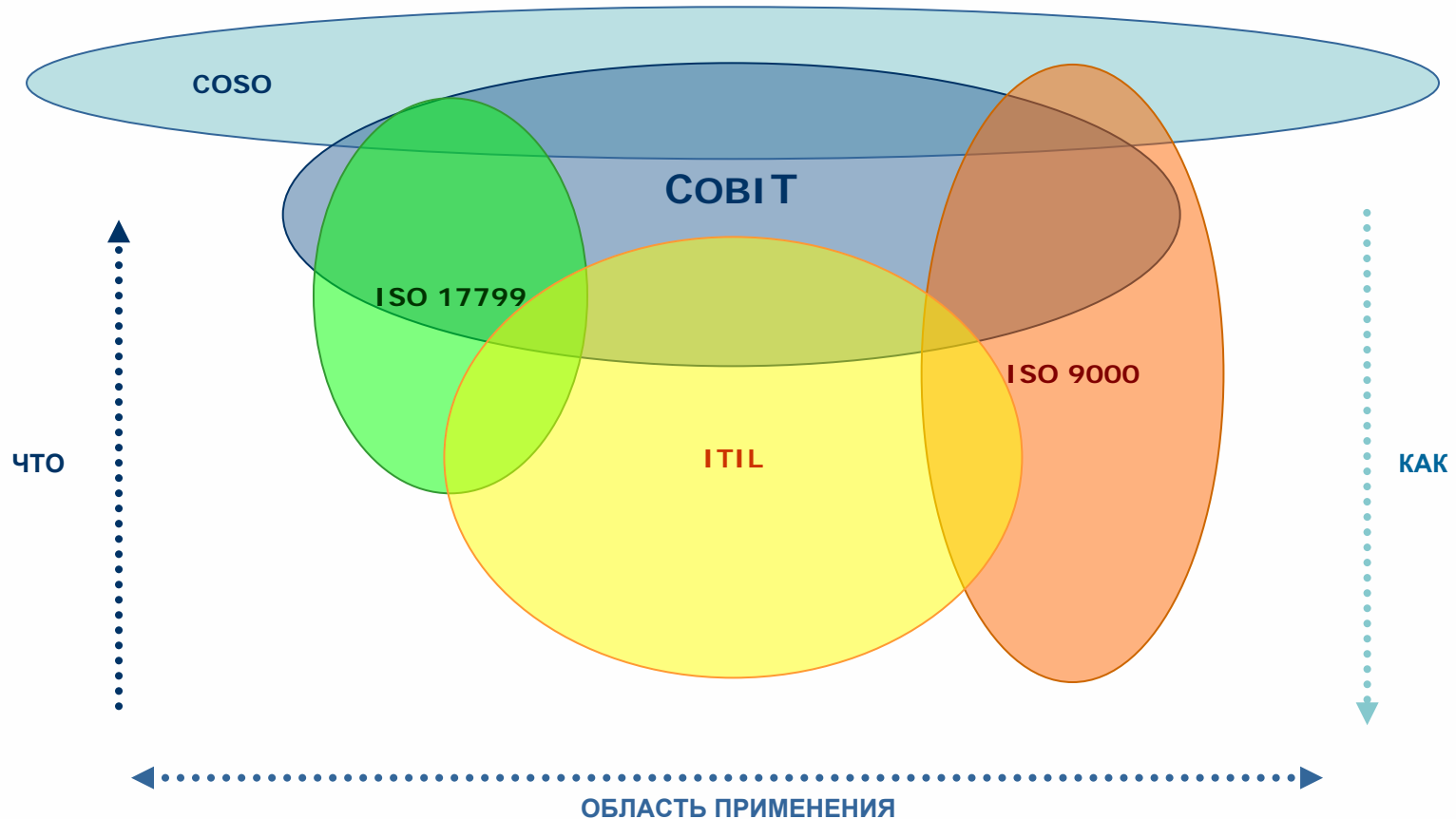
ИТ ресурсы должны управляться в рамках естественным образом сгруппированных процессов. COBIT предоставляет методiku для достижения этой цели.

COBIT предоставляет следующие преимущества при внедрении корпоративного управления ИТ:

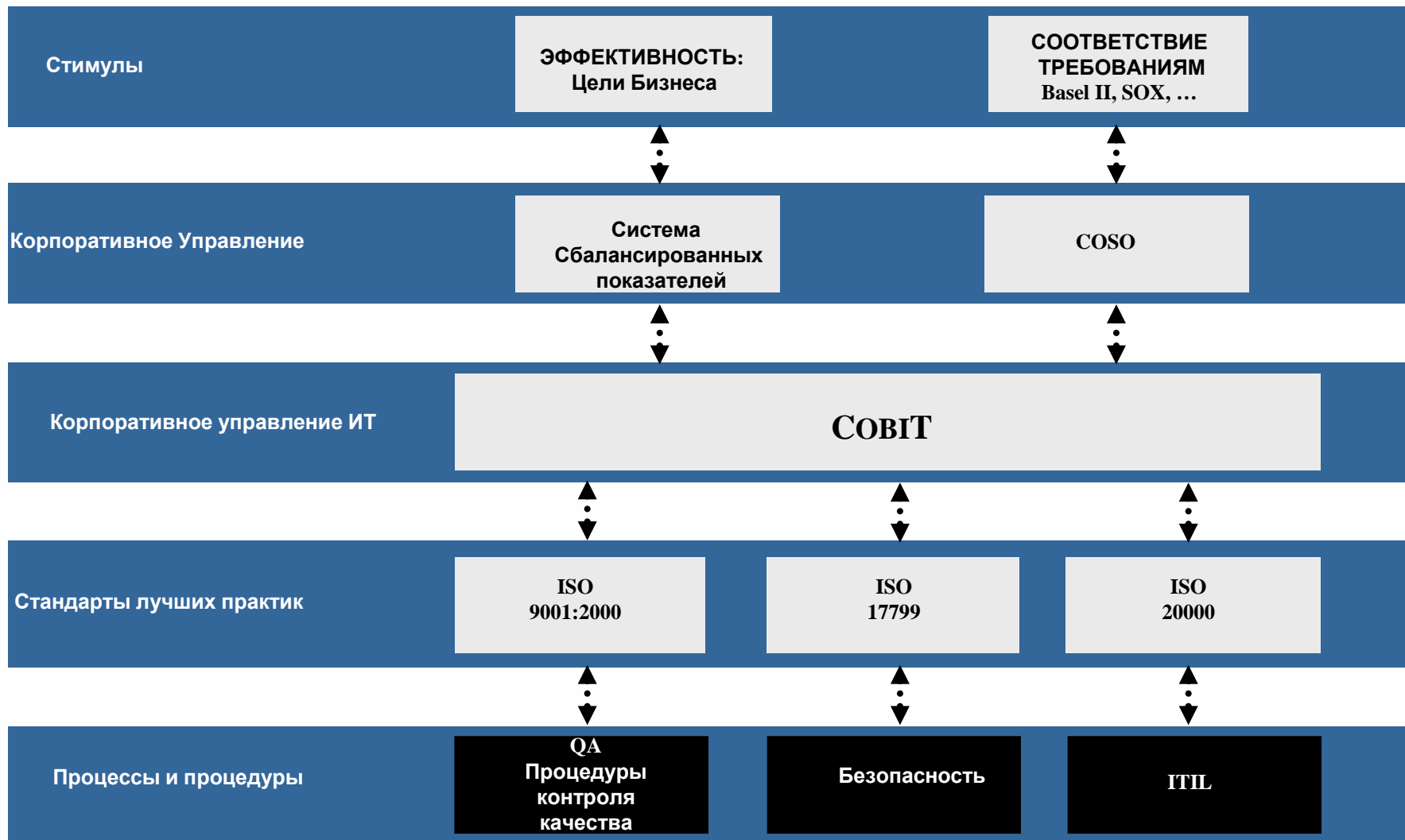
- ⊙ Позволяет построить соответствие целей ИТ целям бизнеса и *наоборот*
- ⊙ Лучшее взаимодействие ИТ и бизнеса, основывающаяся на целях бизнеса
- ⊙ Представление деятельности ИТ служб на понятном бизнесу языке
- ⊙ Четкое определение владельцев и ответственных, основанное на процессном подходе
- ⊙ Признаваемый третьими сторонами и регуляторными органами стандарт
- ⊙ Взаимопонимание между всеми заинтересованными лицами, основанное на общем языке
- ⊙ Соответствие требованиям COSO в отношении среды контроля ИТ



Организации используют различные модели ИТ, стандарты и лучшие практики. Данный слайд демонстрирует возможное совместное использование различных стандартов, при этом COBIT выступает в качестве консолидирующего ('зонтичного') стандарта.



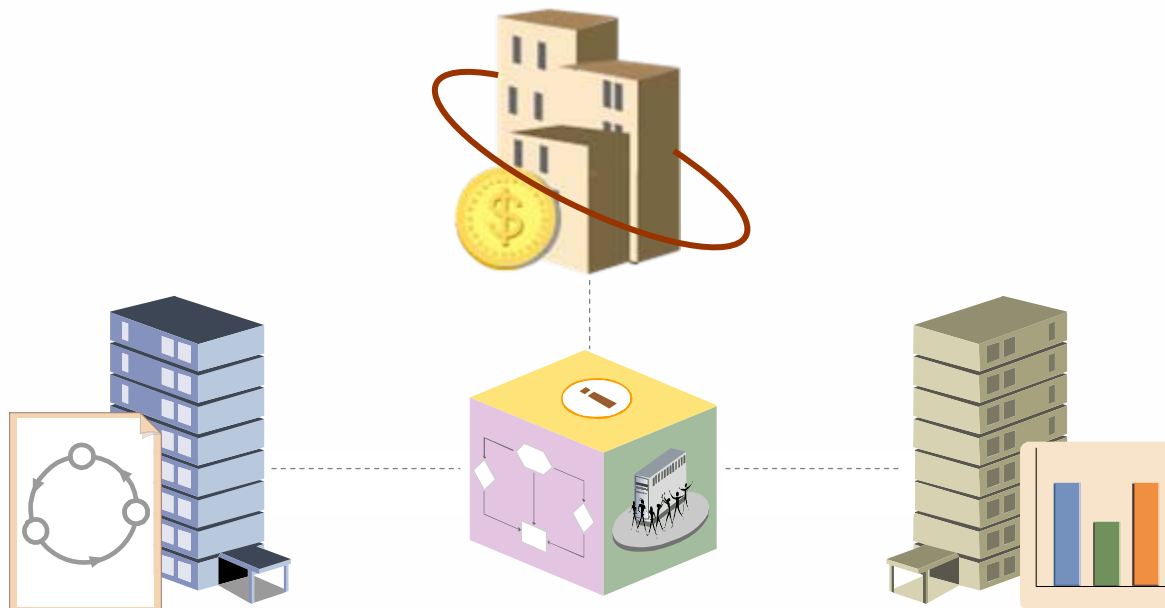
Что покрывает COBIT?



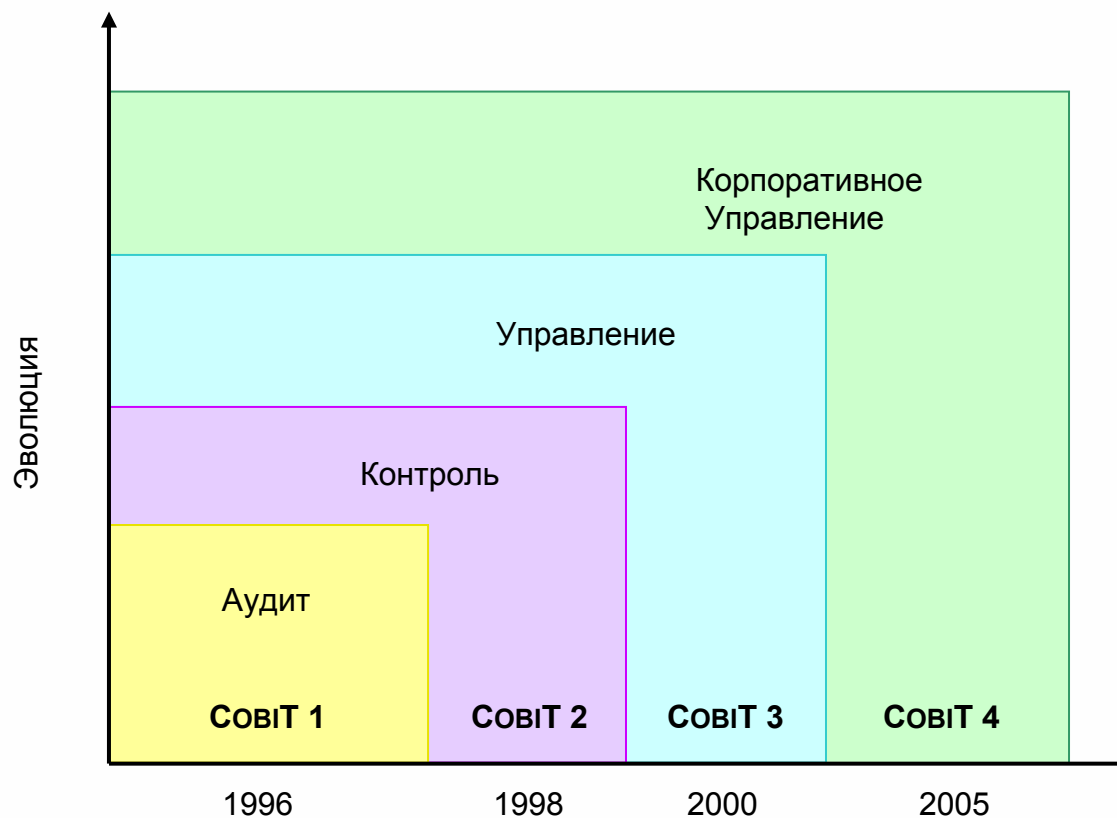
► Методология COBIT характеризуется:

- Ориентация на бизнес
- Процессный подход
- Требования к мерам контроля
- Измеримость

► Аббревиатура COBIT – *Цели Контроля в области Информационных и смежных Технологий.*



Основные характеристики COBIT



Последняя информация по COBIT на сайте www.isaca.org



4.1

Framework
Control Objectives
Management Guidelines
Maturity Models

Информация о переводе COBIT 4.1 на сайте www.isaca-russia.ru

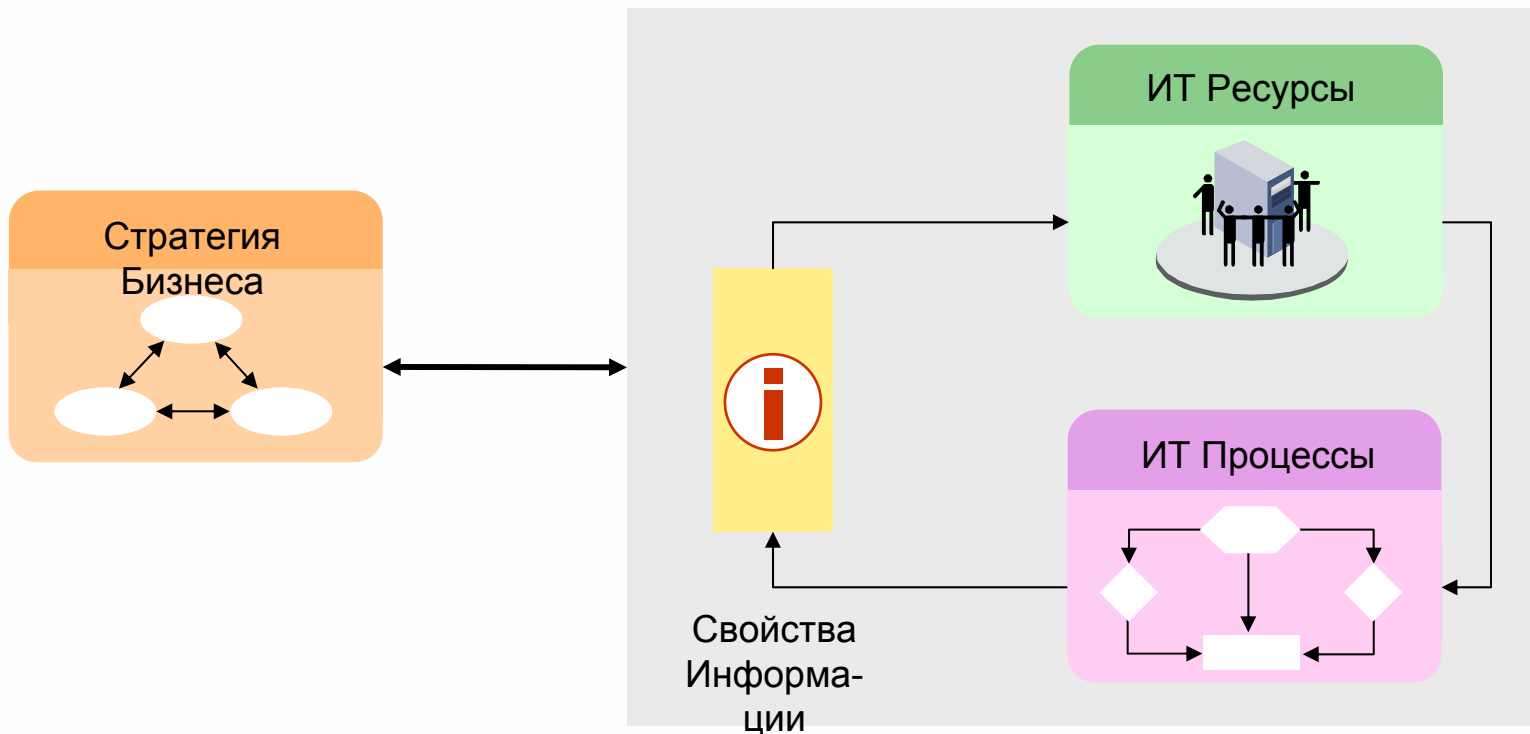
СОВИТ:

- ▶ Общепризнанная мировая лучшая практика
- ▶ Ориентация на высшее руководство
- ▶ Подкреплена инструментариями и учебными курсами
- ▶ Общедоступна, включая возможность загрузки Is freely downloadable
- ▶ Предусматривает совместное использование экспертных знаний
- ▶ Постоянно совершенствуется
- ▶ Поддерживается признанным институтом (ISACA, ITGI)
- ▶ 100 % соответствие COSO
- ▶ Соответствует основным международным стандартам в данной области
- ▶ Представляет собой руководство, а не готовое лекарство

Организациям необходимо провести анализ целей и кастомизировать СОВИТс учетом:

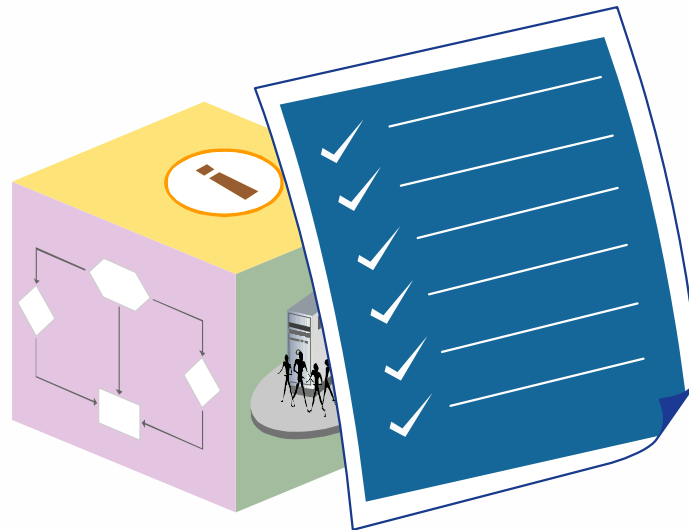
- ▶ Стимулов
- ▶ Профиля рисков
- ▶ Организации, проектов и инфраструктуры ИТ

Организации зависят от надежной с своевременной информации. Компоненты COBIT предоставляют комплексную методику для достижения целей организации на основе управления рисками и мер контроля информации.



Основные преимущества использования СОВІТ:

- ▶ СОВІТ связан с другими стандартами и лучшими практиками и должен использоваться вместе с ними.
- ▶ Методика СОВІТ и соответствующие лучшие практики позволяют внедрить хорошо управляемую и гибкую ИТ среду в организации.
- ▶ СОВІТ позволяет построить среду контроля, отвечающую потребностям бизнеса, а также помогающую руководству и аудиторам осуществлять свои контрольные функции.
- ▶ СОВІТ предоставляет инструментарий для управления задачами ИТ.

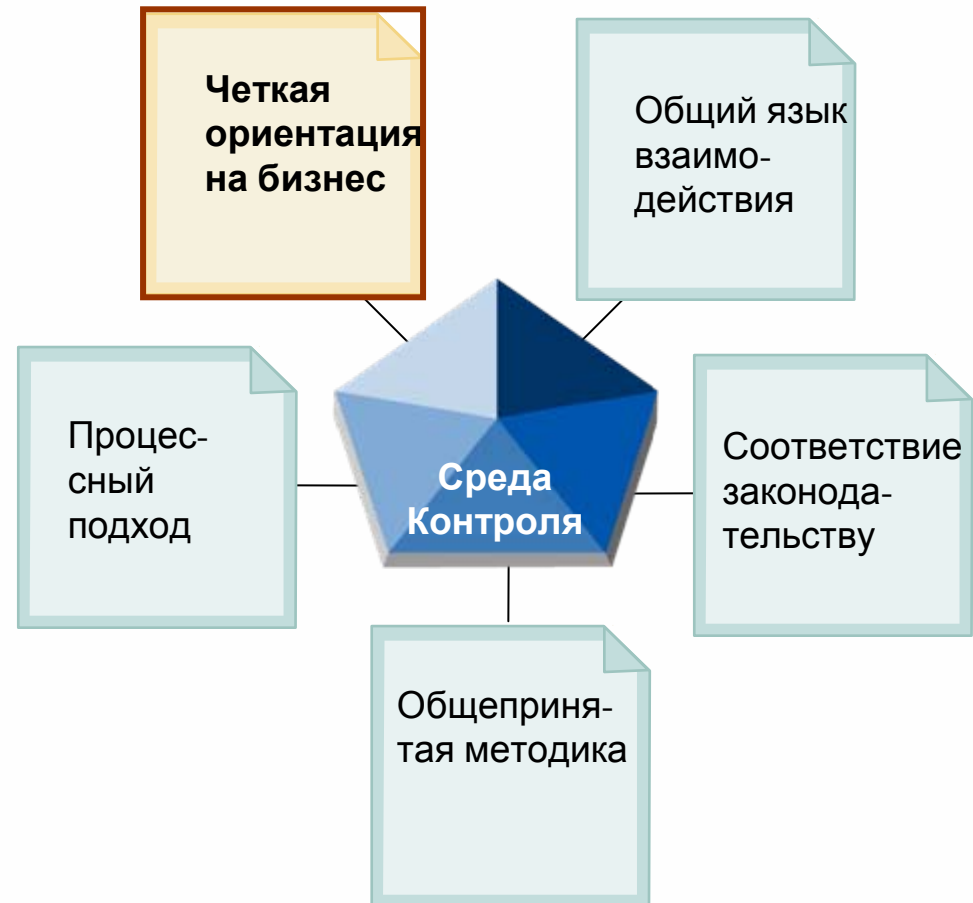


- ▶ СОВИТ направлен на совершенствование корпоративного управления ИТ в организации.
- ▶ СОВИТ предоставляет методiku для управления и контроля задачами ИТ и поддерживает пять требований к среде контроля.

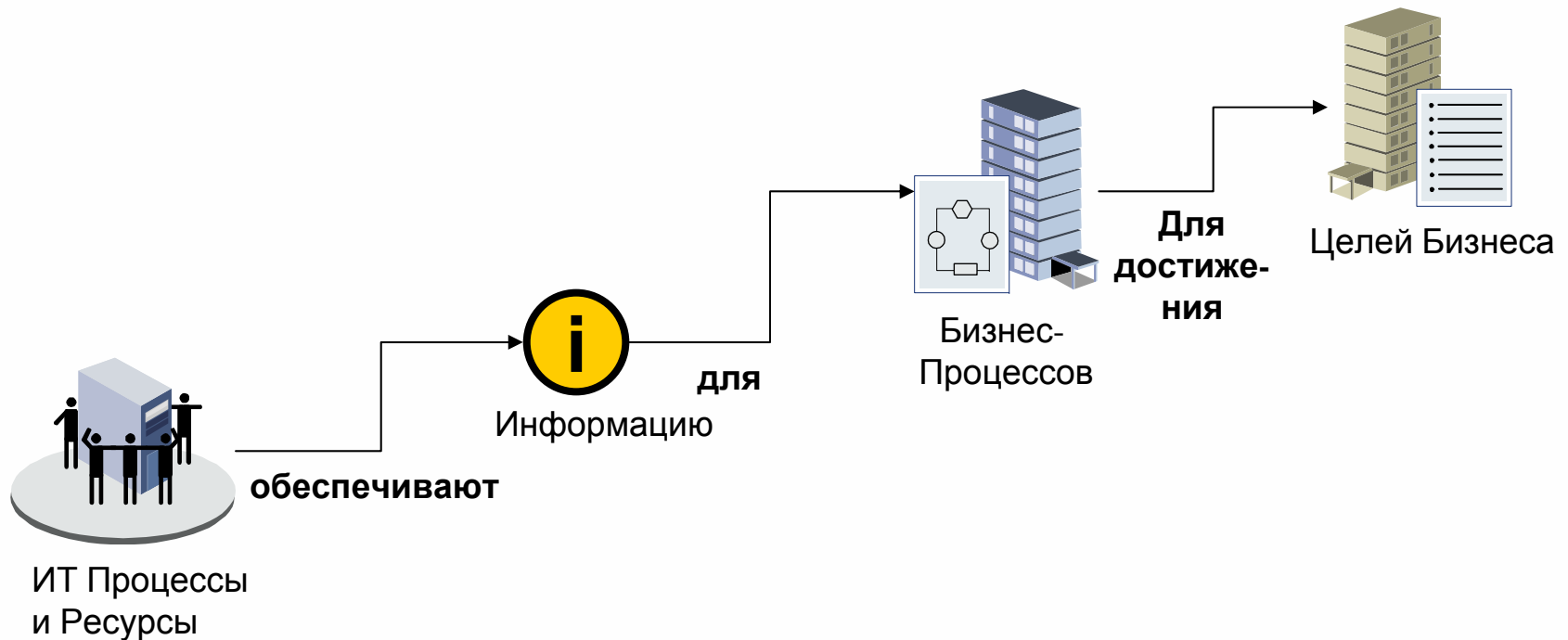


Ориентация на бизнес

- ▶ СОВИТ позволяет достичь четкой ориентации на бизнес благодаря связыванию бизнес и ИТ целей.
- ▶ Измерение эффективности ИТ должно исходить из вклада ИТ в реализацию стратегии бизнеса.
- ▶ СОВИТ, при поддержке надлежащих бизнес-ориентированных метрик, позволят получить уверенность в том, что основной фокус ИТ направлен на предоставление пользы бизнесу, а не технологические достижения сами по себе.

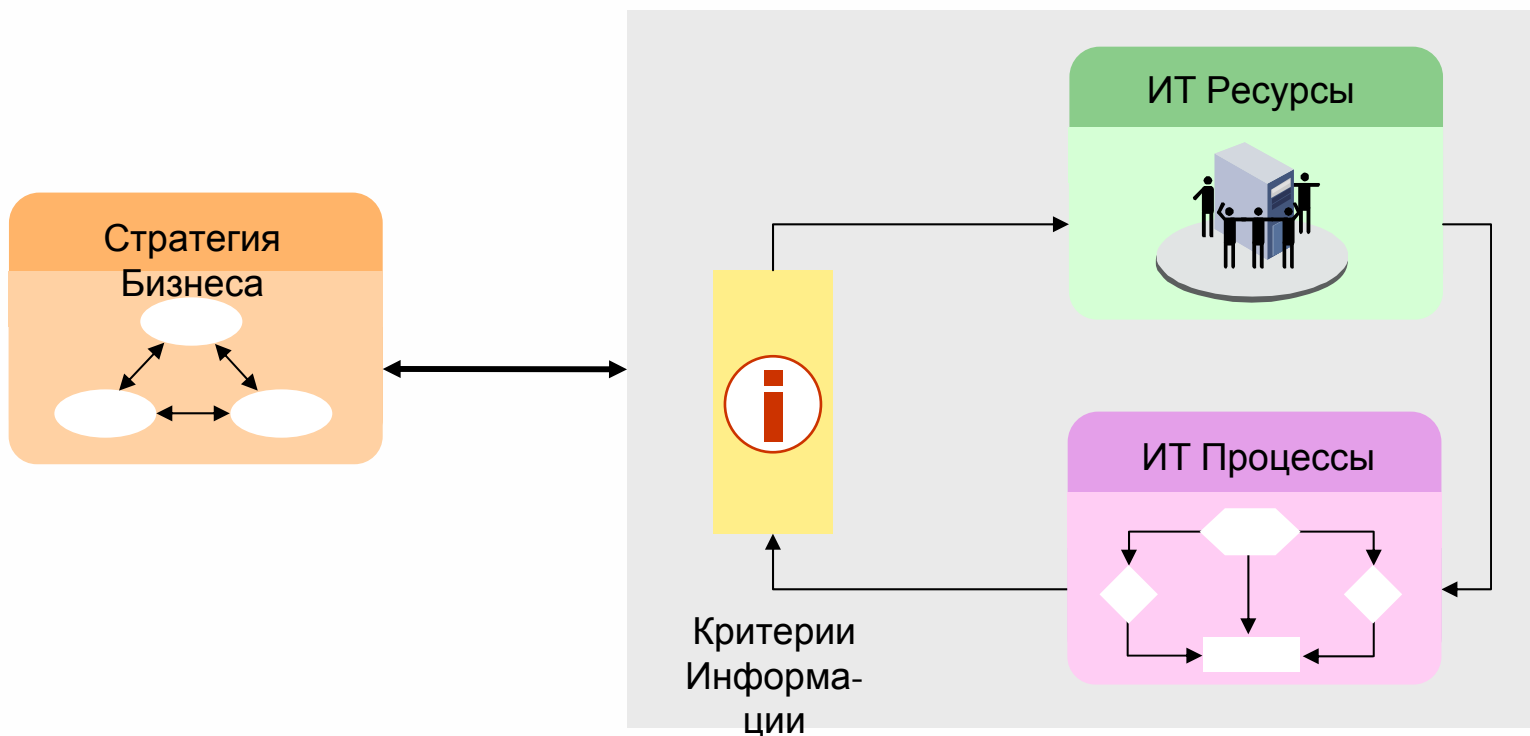


- ▶ Методика СовІТ основана на предпосылке, что ИТ необходимо предоставлять информацию, требуемую организации для достижения своих целей.



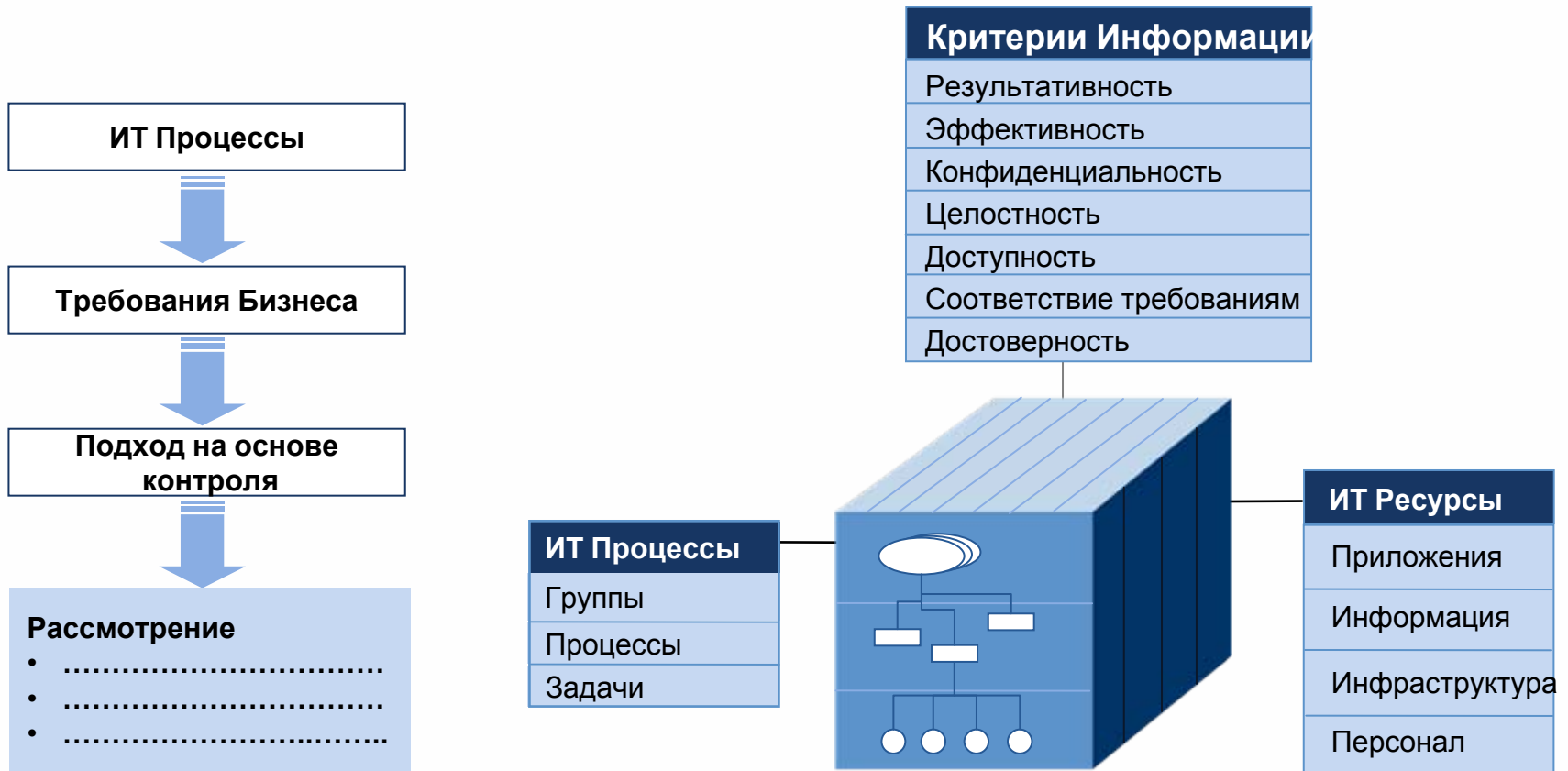
- ▶ Методика СовІТ помогает связать ИТ и бизнес посредством фокусировки на требованиях бизнеса к информации и организации ИТ ресурсов. СовІТ предоставляет методику и рекомендации для внедрения корпоративного управления ИТ.

Отличительной чертой методики COBIT является взаимосвязь ожиданий высшего руководства от ИТ с ответственностью высшего руководства в области ИТ. Цель - внедрение корпоративного управления ИТ, направленное на повышение пользы от ИТ с учетом ИТ-рисков.



Как методика управления и контроля ИТ, СовІТ фокусируется на двух ключевых областях:

- ▶ Обеспечение информацией, требуемой для поддержки целей и требований бизнеса
- ▶ Рассмотрение информации как результат взаимодействия ИТ-ресурсов, управляемых в рамках ИТ-процессов



BUSINESS OBJECTIVES AND GOVERNANCE OBJECTIVES

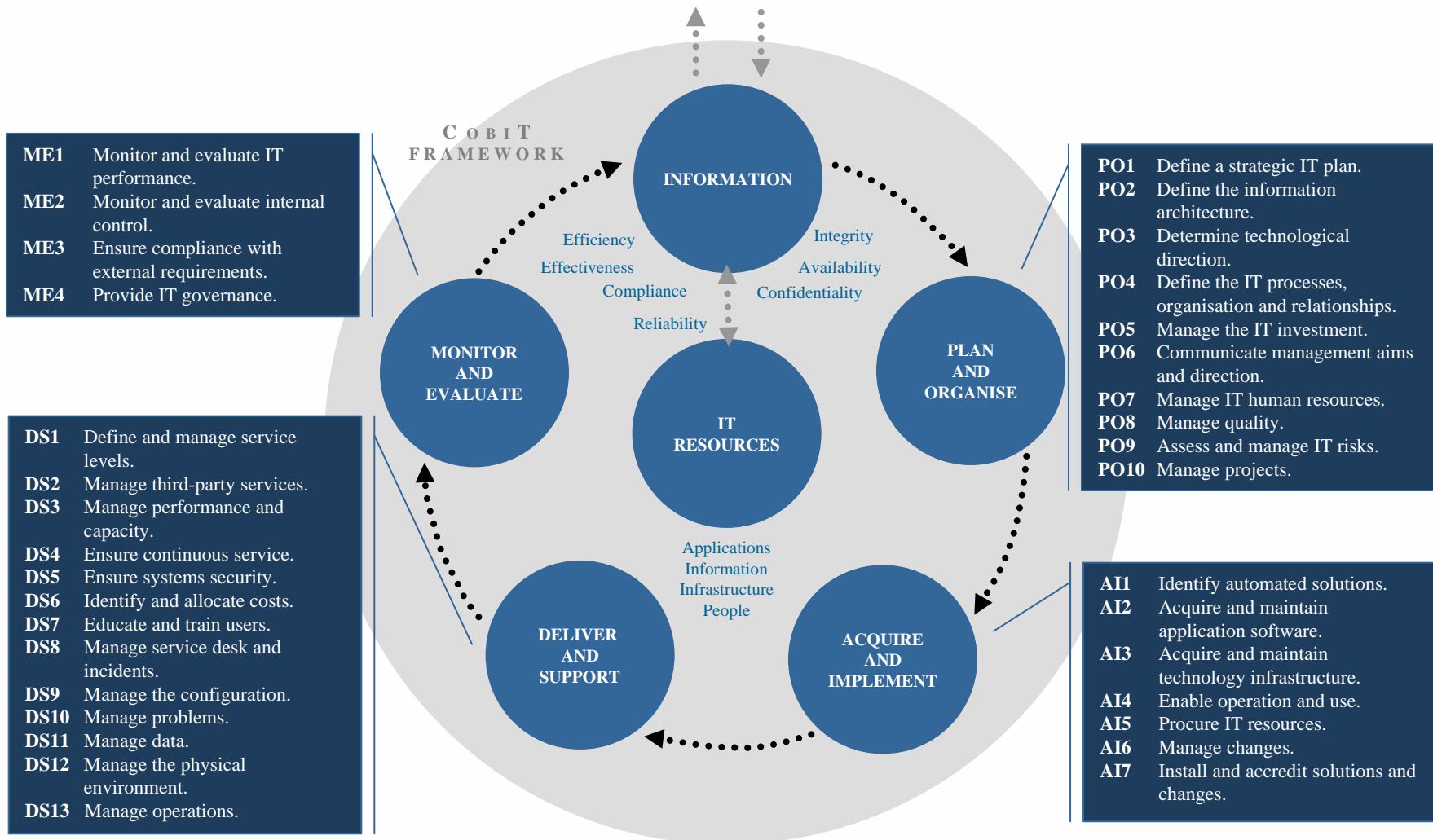
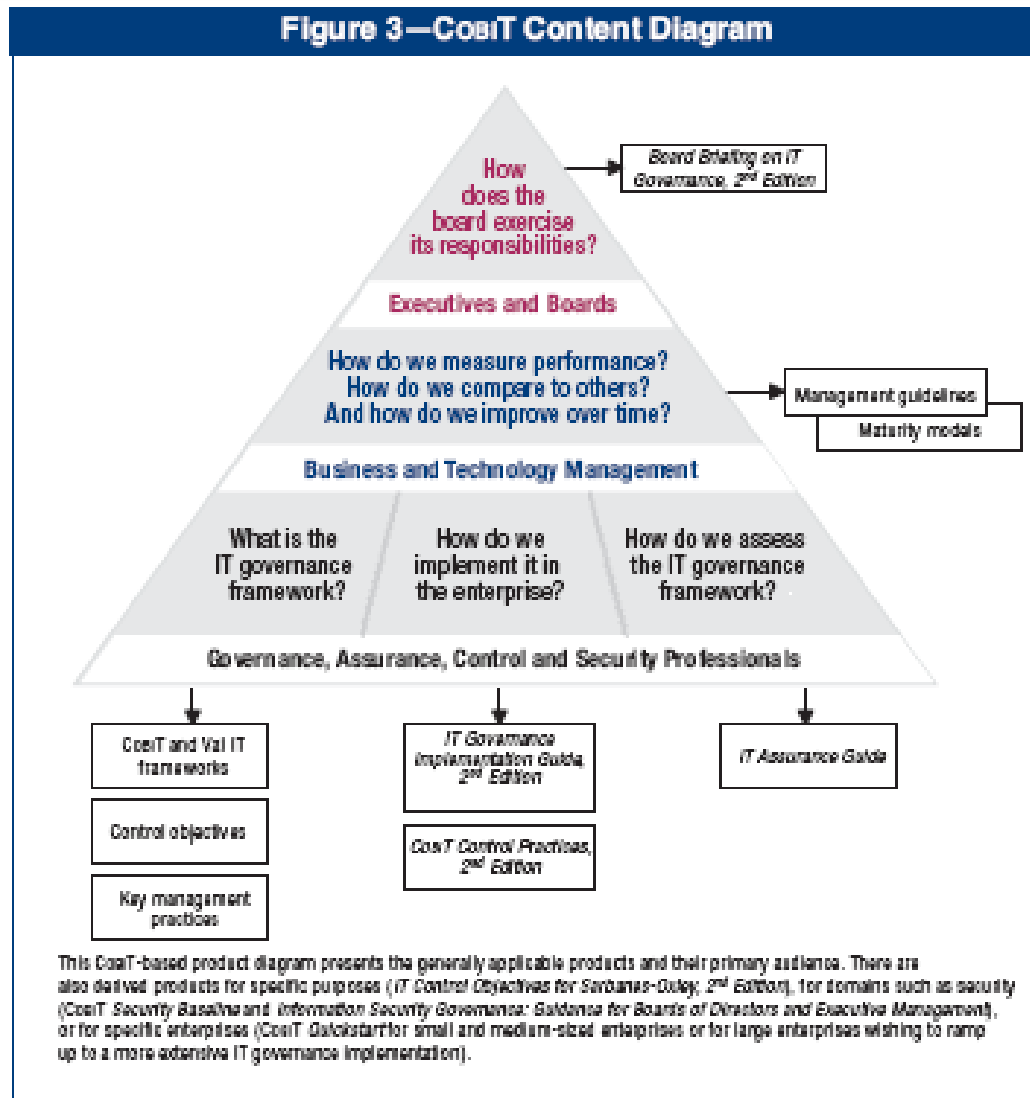


Figure 3—CobIT Content Diagram



ENTERPRISE VALUE: GOVERNANCE OF IT INVESTMENTS

The Val IT Framework

Цель: Обеспечение ценности для бизнеса от инвестиций в ИТ при разумных затратах и приемлемом уровне рисков

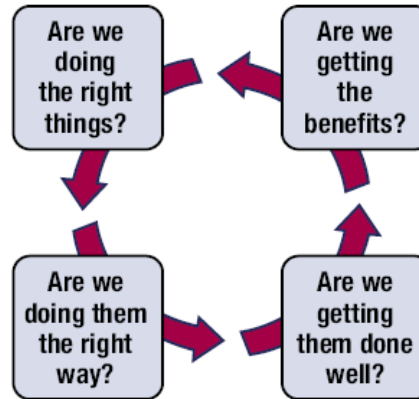
Figure 2—'Four Ares'

The **strategic** question. Is the investment:

- In line with our vision
- Consistent with our business principles
- Contributing to our strategic objectives
- Providing optimal value, at affordable cost, at an acceptable level of risk

The **architecture** question. Is the investment:

- In line with our architecture
- Consistent with our architectural principles
- Contributing to the population of our architecture
- In line with other initiatives



The **value** question. Do we have:

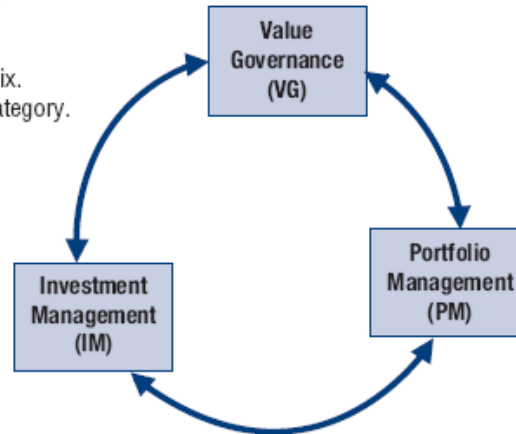
- A clear and shared understanding of the expected benefits
- Clear accountability for realising the benefits
- Relevant metrics
- An effective benefits realisation process

The **delivery** question. Do we have:

- Effective and disciplined management, delivery and change management processes
- Competent and available technical and business resources to deliver:
 - The required capabilities
 - The organisational changes required to leverage the capabilities

Figure 8—Key Management Practices Supporting the Three Val IT Processes

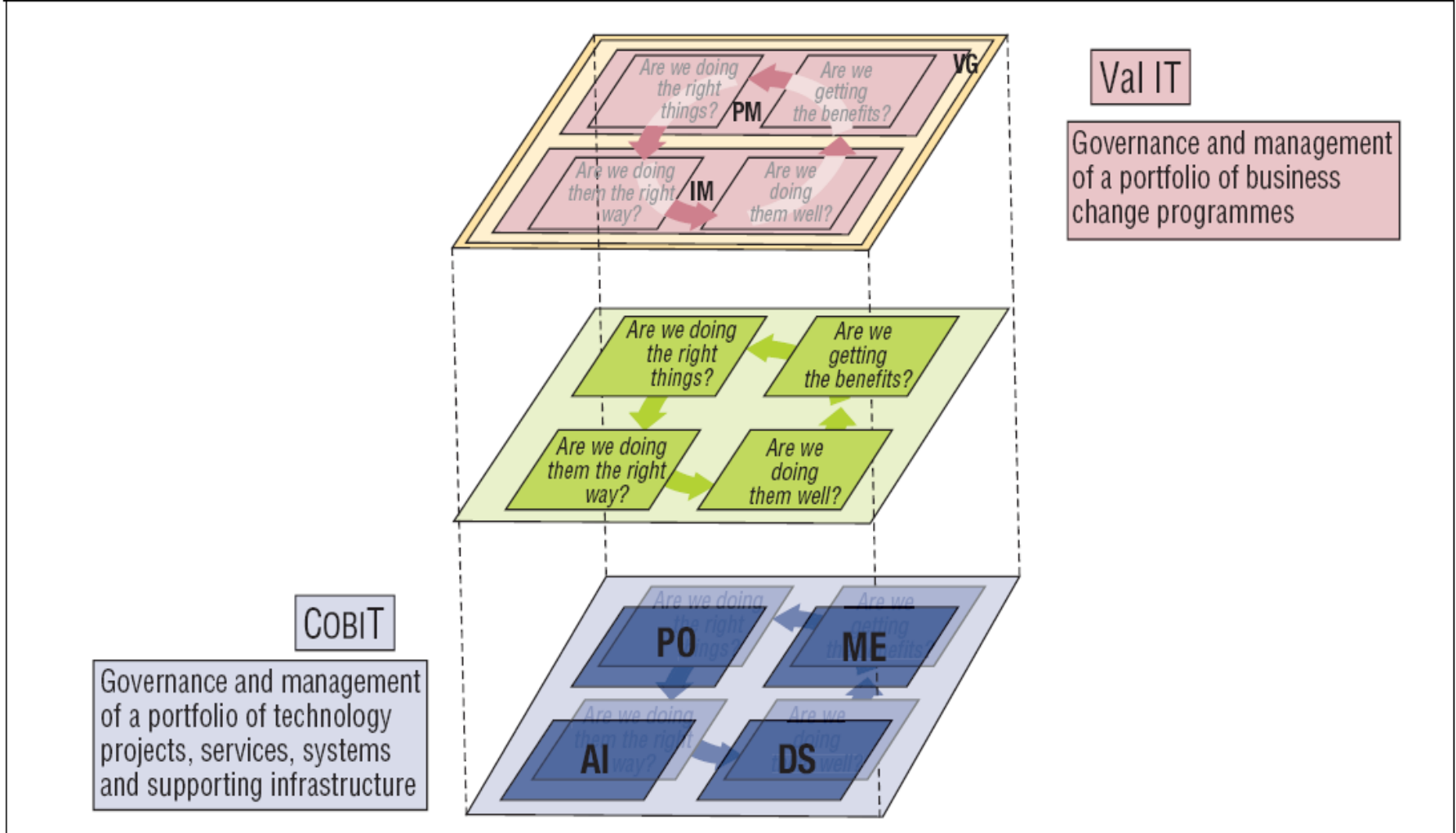
- VG1 Ensure informed and committed leadership.
- VG2 Define and implement processes.
- VG3 Define roles and responsibilities.
- VG4 Ensure appropriate and accepted accountability.
- VG5 Define information requirements.
- VG6 Establish reporting requirements.
- VG7 Establish organisational structures.
- VG8 Establish strategic direction.
- VG9 Define investment categories.
- VG10 Determine a target portfolio mix.
- VG11 Define evaluation criteria by category.



- PM1 Maintain a human resource inventory.
- PM2 Identify resource requirements.
- PM3 Perform a gap analysis.
- PM4 Develop a resourcing plan.
- PM5 Monitor resource requirements and utilisation.
- PM6 Establish an investment threshold.
- PM7 Evaluate the initial programme concept business case.
- PM8 Evaluate and assign a relative score to the programme business case.
- PM9 Create an overall portfolio view.
- PM10 Make and communicate the investment decision.
- PM11 Stage-gate (and fund) selected programmes.
- PM12 Optimise portfolio performance.
- PM13 Re-prioritise the portfolio.
- PM14 Monitor and report on portfolio performance.

- IM1 Develop a high-level definition of investment opportunity.
- IM2 Develop an initial programme concept business case.
- IM3 Develop a clear understanding of candidate programmes.
- IM4 Perform alternatives analysis.
- IM5 Develop a programme plan.
- IM6 Develop a benefits realisation plan.
- IM7 Identify full life cycle costs and benefits.
- IM8 Develop a detailed programme business case.
- IM9 Assign clear accountability and ownership.
- IM10 Initiate, plan and launch the programme.
- IM11 Manage the programme.
- IM12 Manage/track benefits.
- IM13 Update the business case.
- IM14 Monitor and report on programme performance.
- IM15 Retire the programme.

Figure 10—Relationship Between Val IT Processes and COBIT Domains

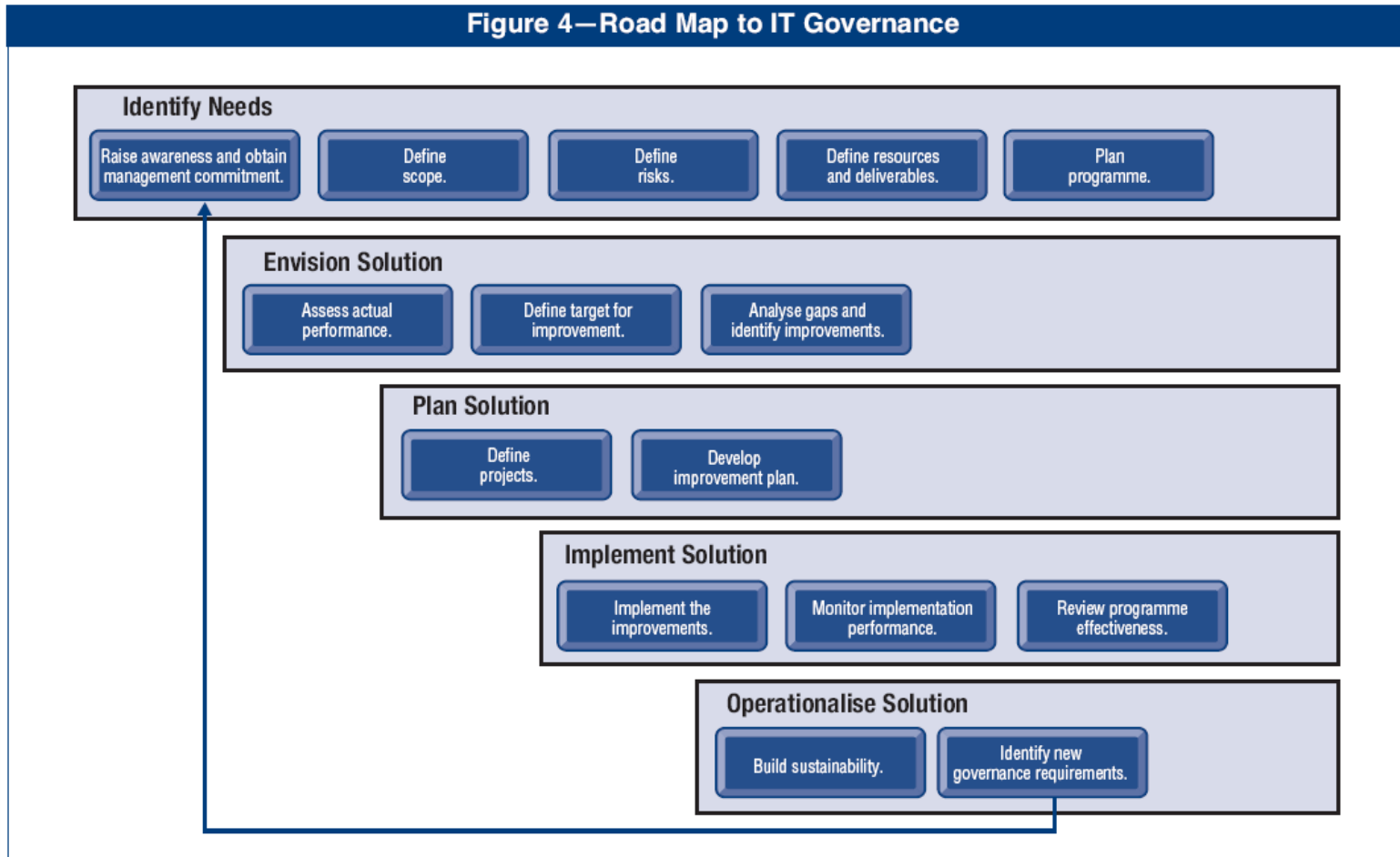


2ND
EDITION

IT GOVERNANCE IMPLEMENTATION GUIDE

USING COBIT[®] AND VAL IT[™]

Figure 4—Road Map to IT Governance



Андрей Дроздов, CISA, CISM, CGEIT
Вице-президент Московского отделения ISACA
Старший менеджер KPMG

adrozdov@kpmg.ru

+7(916)104-15-77