COBIT5 framework as internal audit standard of Industry 4.0

NEW TRENDS IN FINANCIAL TECHNOLOGIES: BLOCKCHAIN, CRYPTOCURRENCIES AND SECURITY

—

Baku, May 17-18, 2018

Вступление

Содержание

- Вступление
- Цифровая трансформация в финансовом секторе
- Основные результаты о роли аудита в эпоху цифровой трансформации
- COBIT 5 как бизнес модель по руководству и управлению ИТ
- Методологии COBIT 5 для целей аудита
- Анализ процесса управления инновациями

Выступающий

Андрей Дроздов

Старший менеджер КПМГ

Вице-Президент Московского отделения ISACA, CISA, CISM, CGEIT, COBIT 5 Foundation Accredited Trainer

ISACA®
Надежные и эффективные информационные системы
Moscow Chapter

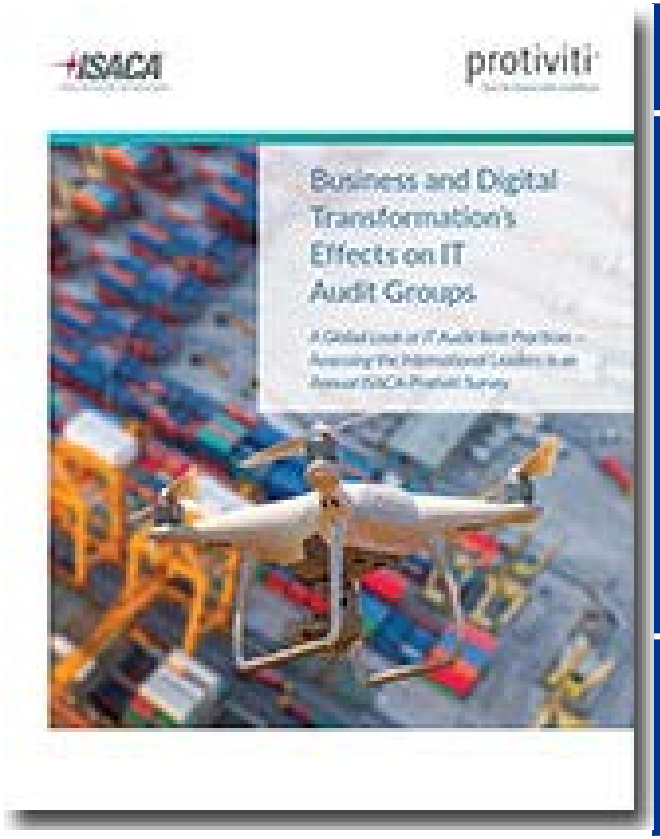
Что означают эти термины?

Industry 4.0
Digital Transformation, Digitalization
Четвертая промышленная революция
Цифровая экономика
AI, ML, Big Data, IoT, Robotics, AR, API
Cloud computing
Blockchain, Cryptocurrency, Bitcoin, ICO
CDO, PSD2, GDPR, DPO, PCI DSS 3.2
Information Security, Cybersecurity
Governance, Culture
Audit (1-st,2-ed,3-ed party)
Assurance
Monitoring
Evaluation
Assessment
Analysis
Control
Review
Testing
Attestation
Compliance
Conformance
Follow-up activities

Финансовый сектор и цифровизация

- Крупные банки опасаются конкуренции от технологических компаний, и сами становятся FinTech компаниями, PSD2 в ЕС
- Крупные банки нанимают ИТ персонал, небольшие – фокус на аутсорсинге ИТ
- Mobile banking services
- Data management, data strategy, BIG Data – в приоритетах
- Cybersecurity, GDPR
- Cloud computing
- Интерес к инновациям
- Robotics and AI
- Блокчейн технологии развиваются, криптовалюты – ограниченно

Глобальный взгляд на лучшие практики ИТ аудита в условиях цифровизации



ISACA и **Protiviti** провели седьмое ежегодное исследования в области ИТ аудита в 3 и 4 кварталах 2017 года.

Этот глобальный анализ был проведен в форме онлайн-опроса, который состоял из групп вопросов, разделенных на 7 категорий:

- Главные современные технологические и бизнес вызовы.
- Вовлечение аудита в ИТ проекты
- Взаимосвязь ИТ аудита и внутреннего аудита.
- Оценка рисков.
- Планирование аудита.
- Вопросы кибербезопасности при планировании аудита
- Навыки и возможности.

Более чем 1300 руководителей и специалистов в области общего и ИТ аудита а также вице-президенты по ИТ приняли участие в исследовании. 26% опрошенных представляли финансовый сектор.

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/a-global-look-at-it-audit-best-practices.aspx

Основные выводы исследования

Цифровая трансформация и Кибербезопас-ность – основные вызовы для аудита

Рост осознания важности ИТ аудита, появление роли директора по ИТ аудиту

Цифровая трансформация, Agile методы требуют тесного взаимодействия ВА с бизнесом/ИТ

Рост вовлеченности ИТ аудита в технологические проекты

Рост ко-соурсинга ВА обусловленный нехваткой ресурсов

Основные технологические вызовы и тренды

Current	YOY Trend*	2016
IT security and privacy/cyber security	⇔	IT security and privacy/cyber security
Infrastructure Management	⇔	Infrastructure Management
Emerging technology and infrastructure changes–transformation, innovation, disruption	⇔	Emerging technology and infrastructure changes–transformation, innovation, disruption
Resource/staffing/skills management	⇔	Resource/staffing/skills management
Regulatory compliance	⇔	Regulatory compliance
Budgets and controlling costs	⇔	Budgets and controlling costs
Cloud computing/virtualization	⇔	Cloud computing/virtualization
Third party/vendor management	⇑	Bridging IT and the business
Project management and change management	⇔	Project management and change management
Data management and governance	⇑	Third party/vendor management

* Отображает изменение в тенденции к 2016

Интересные факты

Около половины организаций имеют директора по ИТ аудиту, который, как правило, подчиняется руководителю ВА; рост привлечения внешних ресурсов для ИТ аудита

По направлениям ИТ аудита в лидерах: оценка общих ИТ-контролей, контролей приложений, процессов руководства и управления ИТ, безопасности, ИТ-инфраструктуры, анализ проектов по результатам внедрения, анализ данных, распространен интеграционный аудит. По затратам времени ВА в лидерах деятельность, связанная с обеспечением уверенности и комплаенс, хотя есть и консалтинг

При проведении внутреннего ИТ- аудита COBIT применяется более чем в половине организаций, для ИБ – аудита также NIST Cybersecurity Framework

Острая потребность в квалифицированных кадрах для ИТ аудита

Что такое ИТ-аудит?

ИТ-аудит представляет собой независимую оценку выбранных направлений деятельности ИТ против определенных стандартов и критериев.

Потребность в ИТ-аудите

Потребность в ИТ-аудите часто обусловлена необходимостью повышения прозрачности и эффективности функционирования блока ИТ.

В некоторых случаях организации необходимо соответствовать определенным локальным, отраслевым и международным стандартам. Это может быть связано как с требованиями регулирующих органов, так и с необходимостью улучшения инвестиционной привлекательности организации.

Состав работ

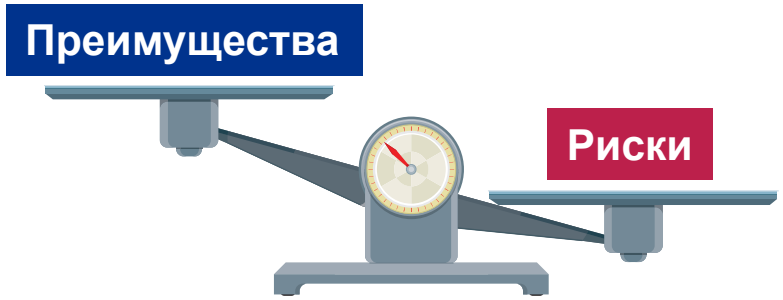
- Идентификация требований бизнеса к ИТ
- Анализ текущего состояния и определение уровня зрелости ИТ
- Разработка рекомендаций на основе полученных аналитических данных
- Оценка экономической эффективности рекомендованных мероприятий

Зачем это нужно?

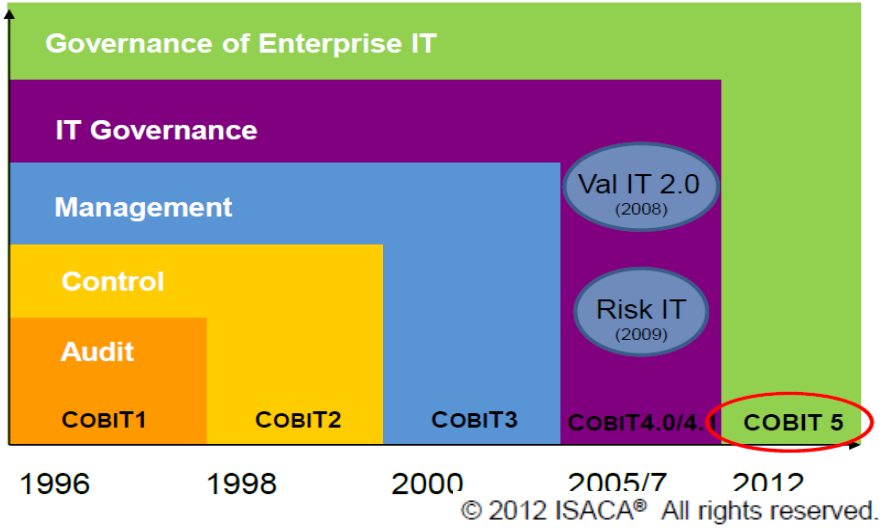
- Сбор и анализ информации об ИТ-инфраструктуре и информационных системах
- Анализ используемых ИТ-решений и ИТ-процессов на соответствие требованиям бизнеса организации
- Оценка совокупной стоимости владения и возврата инвестиций в ИТ
- Оценка информационных систем предприятия на функциональную полноту и соответствие международным и российским стандартам
- Анализ ИТ-рисков и рисков информационной безопасности организации, а также степени ее устойчивости к нежелательным событиям

COBIT 5 – бизнес-модель по руководству и управлению ИТ

COBIT 5 помогает предприятиям получить оптимальную пользу от ИТ, достигая баланса между достижением преимуществ и обеспечением приемлемого уровня рисков и затрат ресурсов.



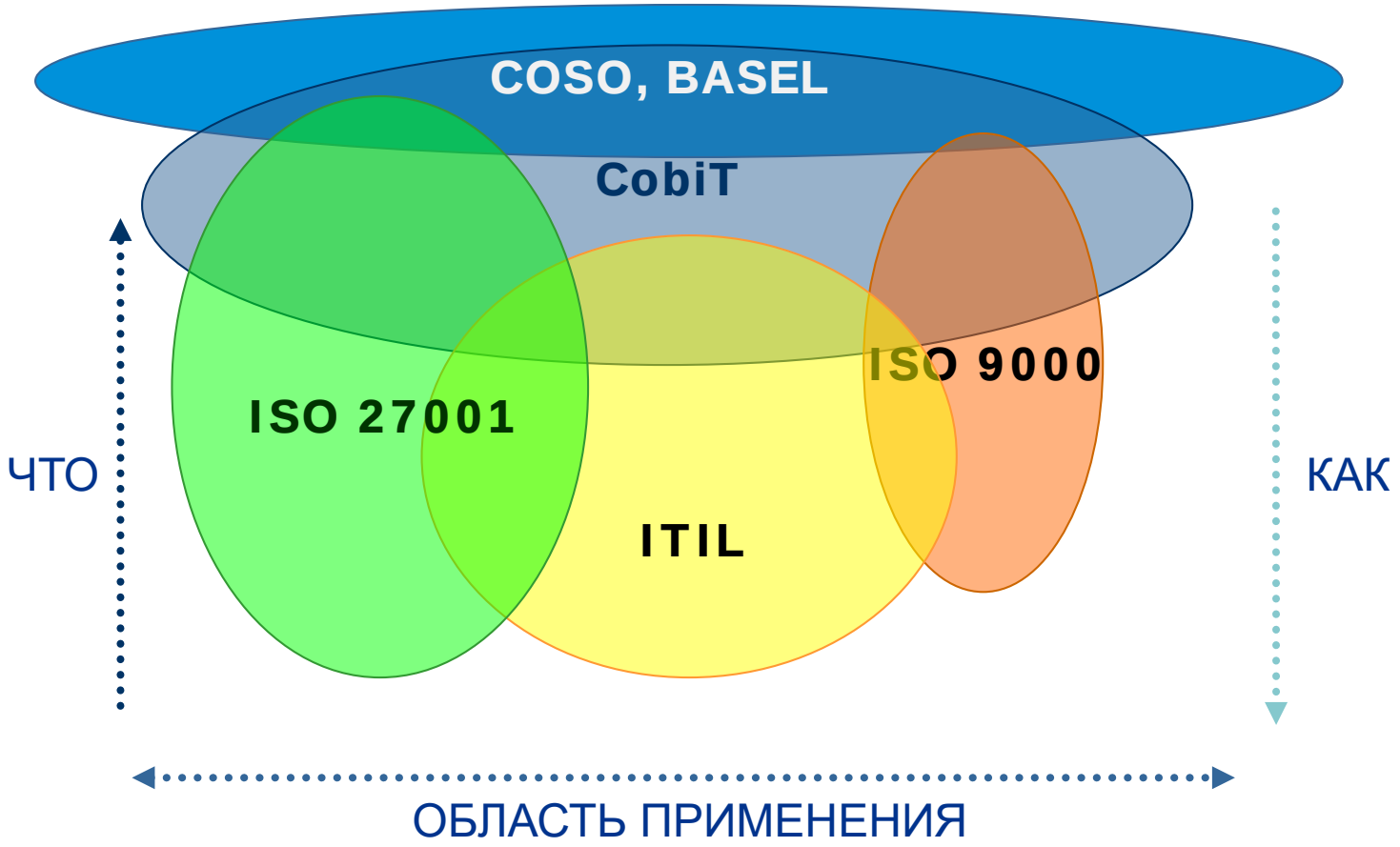
Эволюция COBIT



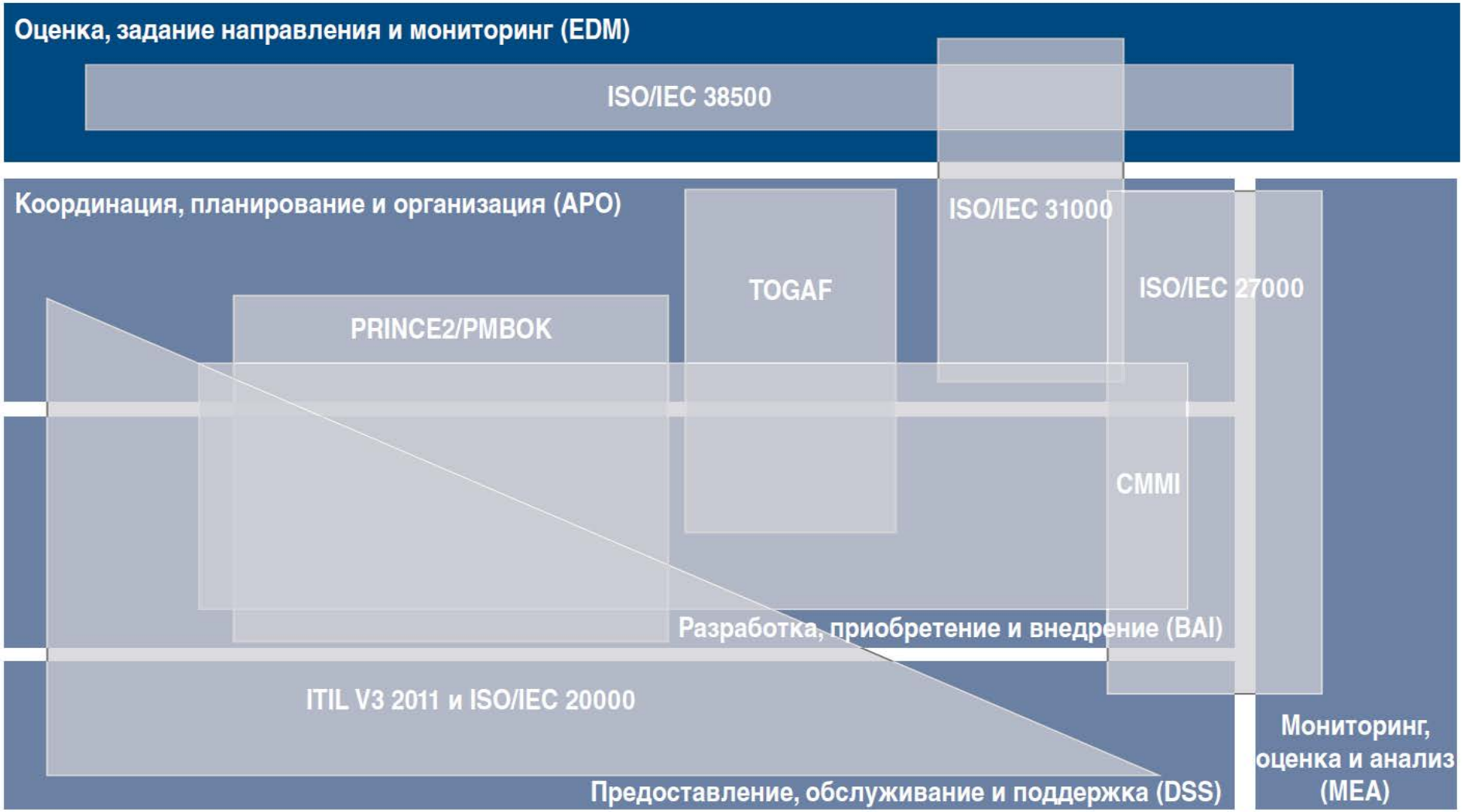
COBIT 5: Бизнес-модель по руководству и управлению ИТ на предприятии

Взаимосвязь различных стандартов в области систем управления и контроля

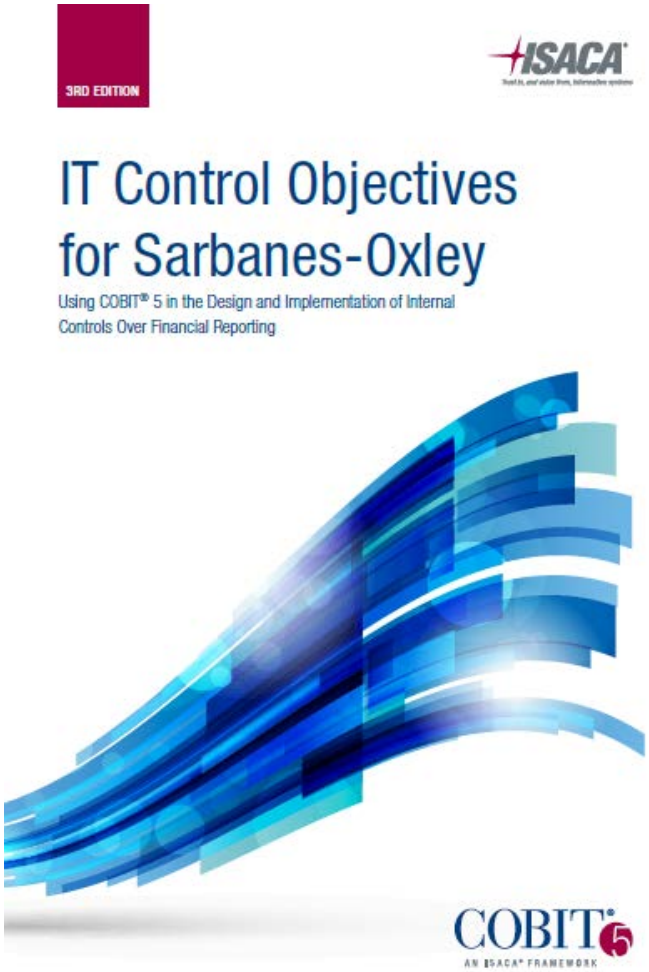
COBIT выступает в качестве “зонтичной” модели, связывая требования ИТ/ИБ и бизнеса

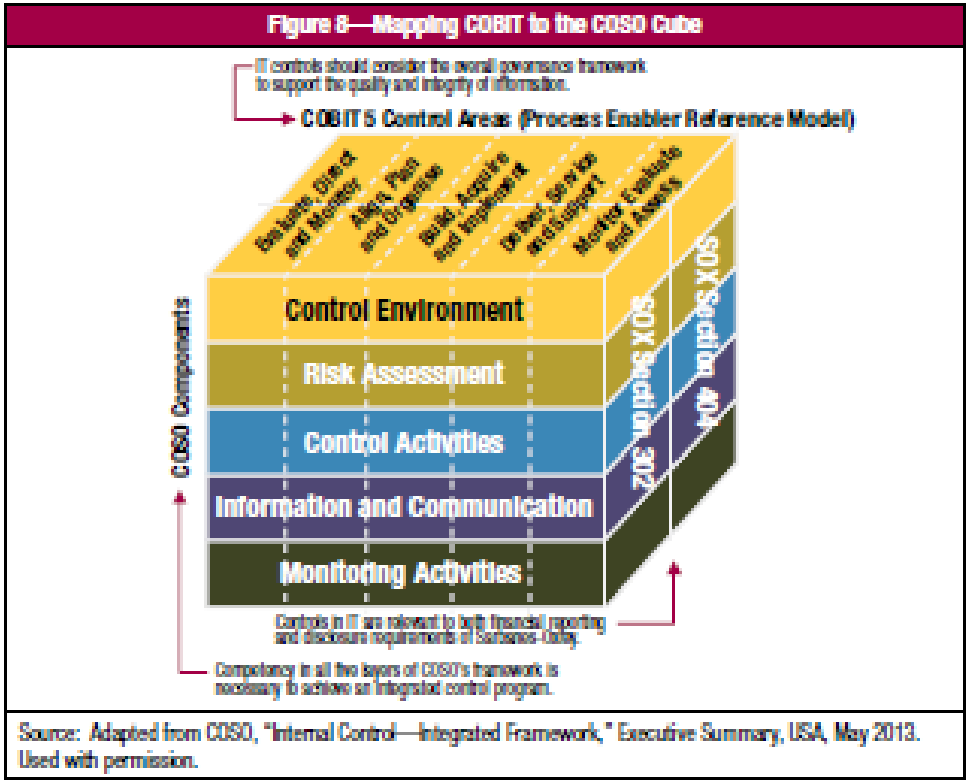


Взаимосвязь стандартов и требований



Взаимосвязь стандартов и требований





COBIT 5 – Публикации

COBIT 5 – Принципы

Руководство и управление

– Руководство

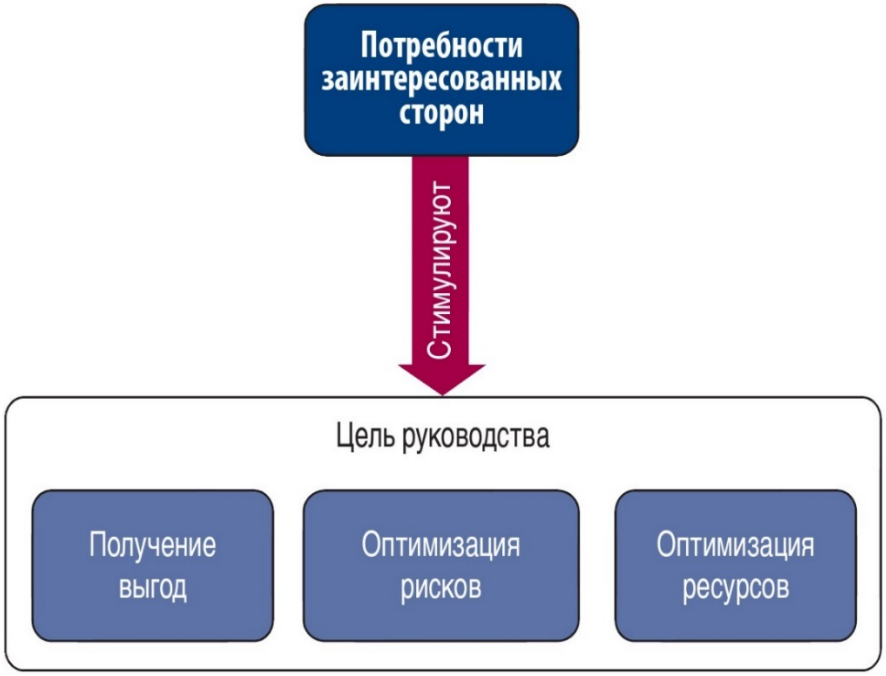
Руководство обеспечивает уверенность в достижении целей предприятия, путём: сбалансированной оценки потребностей заинтересованных сторон, существующих условий и возможных вариантов; установления направления развития через приоритизацию и принятие решений; постоянного мониторинга соответствия фактической производительности и степени выполнения требований установленным направлению и целям предприятия.

В большинстве случаев обязанности по руководству на предприятии выполняет совет директоров, возглавляемый председателем совета директоров. Некоторые обязанности могут быть делегированы специальным организационным единицам соответствующего уровня – особенно, в крупных организациях.

– Управление

Управление заключается в планировании, построении, выполнении и отслеживании деятельности, в соответствии с направлением, заданным органом руководства, для достижения целей предприятия.

Принцип 1. Каскад Целей



Цели предприятия vs. ИТ-цели

ISACA Moscow Chapter

Приоритизация ИТ-процессов
в соответствии с целями предприятия:

- 4 области BSC
- 17 целей предприятия
- 17 ИТ-целей
- 37 ИТ процессов

Пример:

Цель предприятия: Финансовая прозрачность

ИТ-цели: Прозрачность ИТ затрат, выгод, рисков

ИТ-процессы:

(P) BAI09 – Управление активами

(S) BAI01 – Управление программами и проектами

(S) BAI10 – Управление конфигурациями

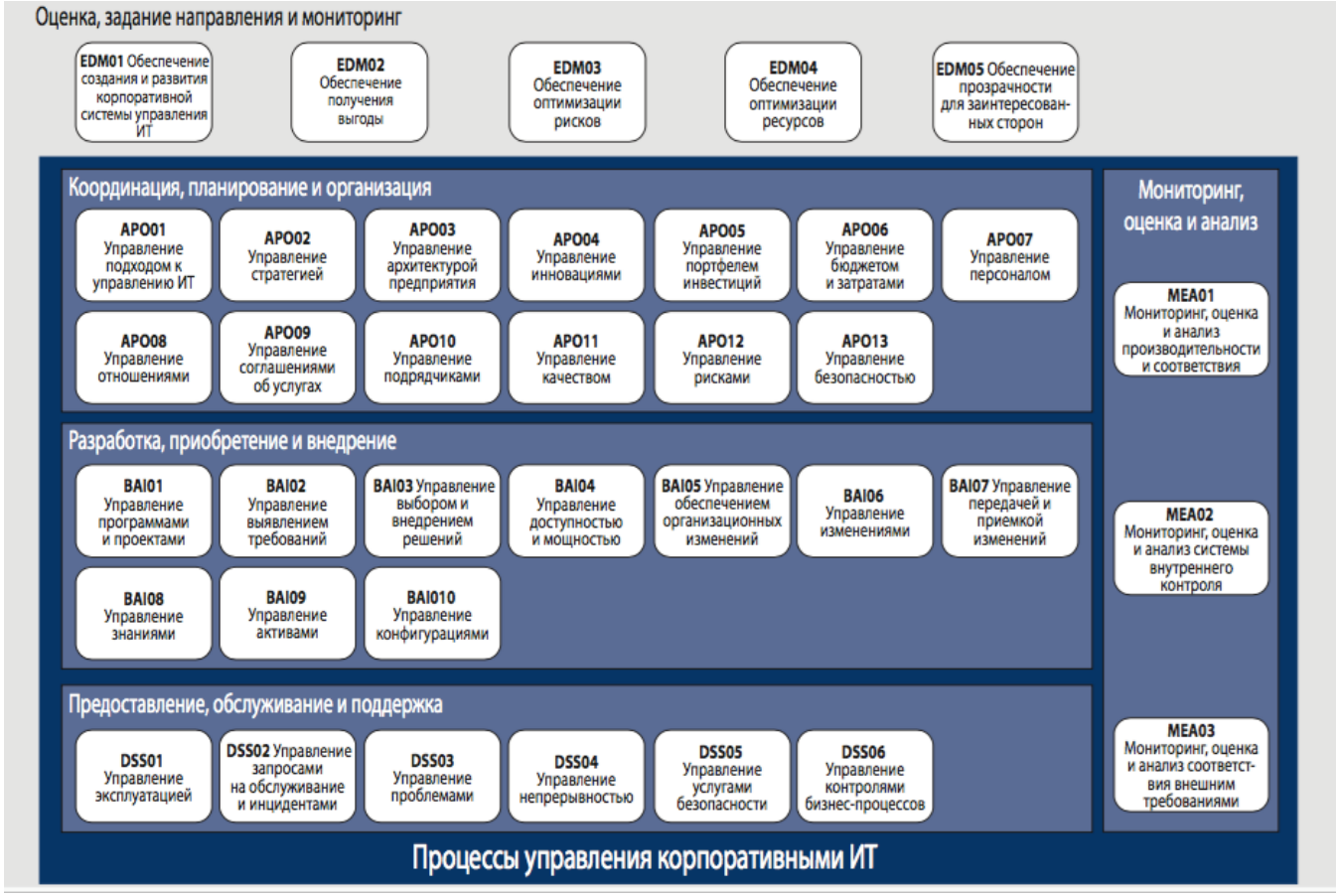
(S) MEA01 – Мониторинг, оценка и анализ производительности и соответствия

(S) MEA02 – Мониторинг, оценка и анализ системы внутреннего контроля

			Цель предприятия																	
			Отдача от инвестиций для заинтересованных сторон	Портфель конкурентоспособных товаров и услуг	Управляемые бизнес-риски (защита активов)	Соответствие внешним законам и регулирующим нормам	Финансовая прозрачность	Клиентоориентированная сервисная культура	Непрерывность и доступность бизнес-услуг	Гибкая реакция на изменяющиеся условия ведения бизнеса	Принятие стратегических решений на основе информации	Оптимизация затрат на предоставление услуг	Оптимизация функциональности бизнес-процессов	Оптимизация затрат бизнес-процессов	Управление программами бизнес-изменений	Операционная производительность персонала	Соблюдение внутренних политик	Квалифицированный и мотивированный персонал	Культура долгосрочных инноваций продуктов и бизнеса
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		ИТ-цели	Финансы					Заказчик					Внутреннее управление					Обучение и развитие	
Финансы	01	Соответствие между ИТ- и бизнес-стратегиями	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Следование внешнему законодательству и регулирующим требованиями в области ИТ и поддержка бизнес-соответствия			S	P											P		
	03	Лидирующая роль руководства в принятии решений в области ИТ	P	S	S					S	S		S		P			S	S
	04	Управляемые ИТ-риски			P	S			P	S		P			S		S	S	
	05	Получение выгод от инвестиций с использованием ИТ и портфеля услуг	P	P				S		S		S	S	P		S			S
	06	Прозрачность ИТ-затрат, выгод и рисков	S		S		P				S	P		P					
Заказчик	07	Предоставление ИТ-услуг в соответствии с бизнес-требованиями	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Адекватное использование приложений, информации и технических решений	S	S	S			S	S		S	S	P	S		P		S	S
Внутреннее управление	09	Гибкость ИТ	S	P	S			S		P			P		S	S		S	P
	10	Безопасность информации, обрабатывающей инфраструктуры и приложений			P	P			P								P		
	11	Оптимизация ИТ-активов, ресурсов и способностей	P	S						S		P	S	P	S	S			S
	12	Обеспечение работы и поддержка бизнес-процессов, путем интеграции приложений и технологий в бизнес-процессы	S	P	S			S		S		S	P	S	S	S			S
	13	Извлечение выгоды из программ и проектов, выполняемых в рамках сроков, бюджета и соответствующих требованиям и стандартам качества	P	S	S			S				S		S	P				
	14	Доступность надежной и нужной информации для принятия решений	S	S	S	S			P		P		S						
	15	Соблюдение внутренних политик			S	S											P		
Обучение и развитие	16	Компетентный и мотивированный персонал ИТ	S	S	P			S		S						P		P	S
	17	Знания, экспертиза и инициативность для осуществления бизнес-инноваций	S	P				S		P	S		S		S			S	P

COBIT 5 – Факторы влияния

COBIT 5 – процессная модель

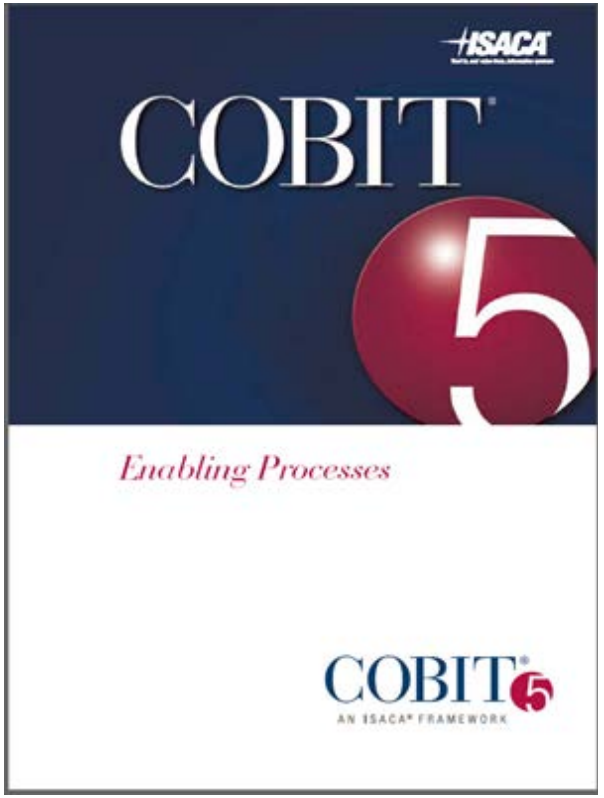


Уровни возможностей процессов:

0- Неполный процесс
1- Осуществленный процесс
2- Управляемый процесс
3- Установленный процесс
4- Предсказуемый процесс
5- Оптимизирующий процесс

Методология оценки в соответствие с ISO 15504 описана в *Process Assessment Model (PAM): Using COBIT 5*

COBIT 5 – процессная модель



Для каждого из 37 процессов

— Назначение и цели процесса

1- Хорошие (базовые) практики

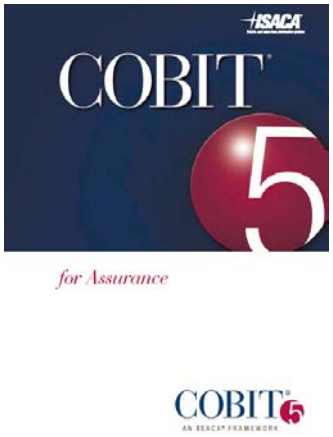
2- Действия (activities)

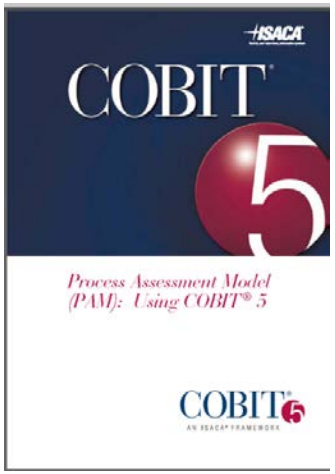
3- Входы и выходы

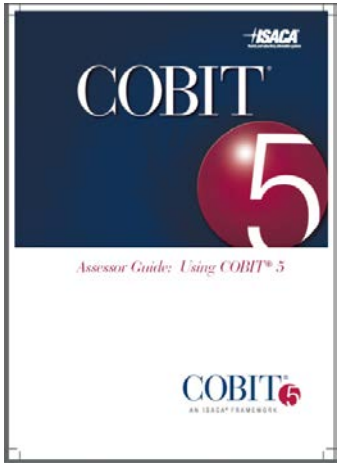
4- RACI матрицы

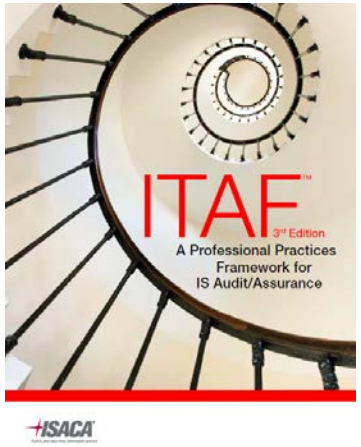
5- Метрики

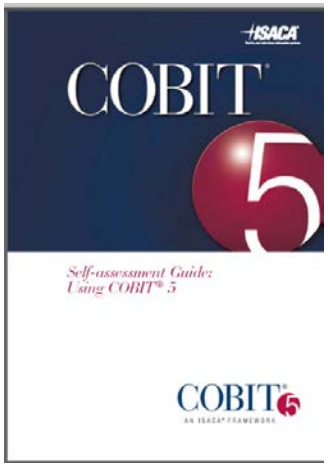
Публикации ISACA по аудиту











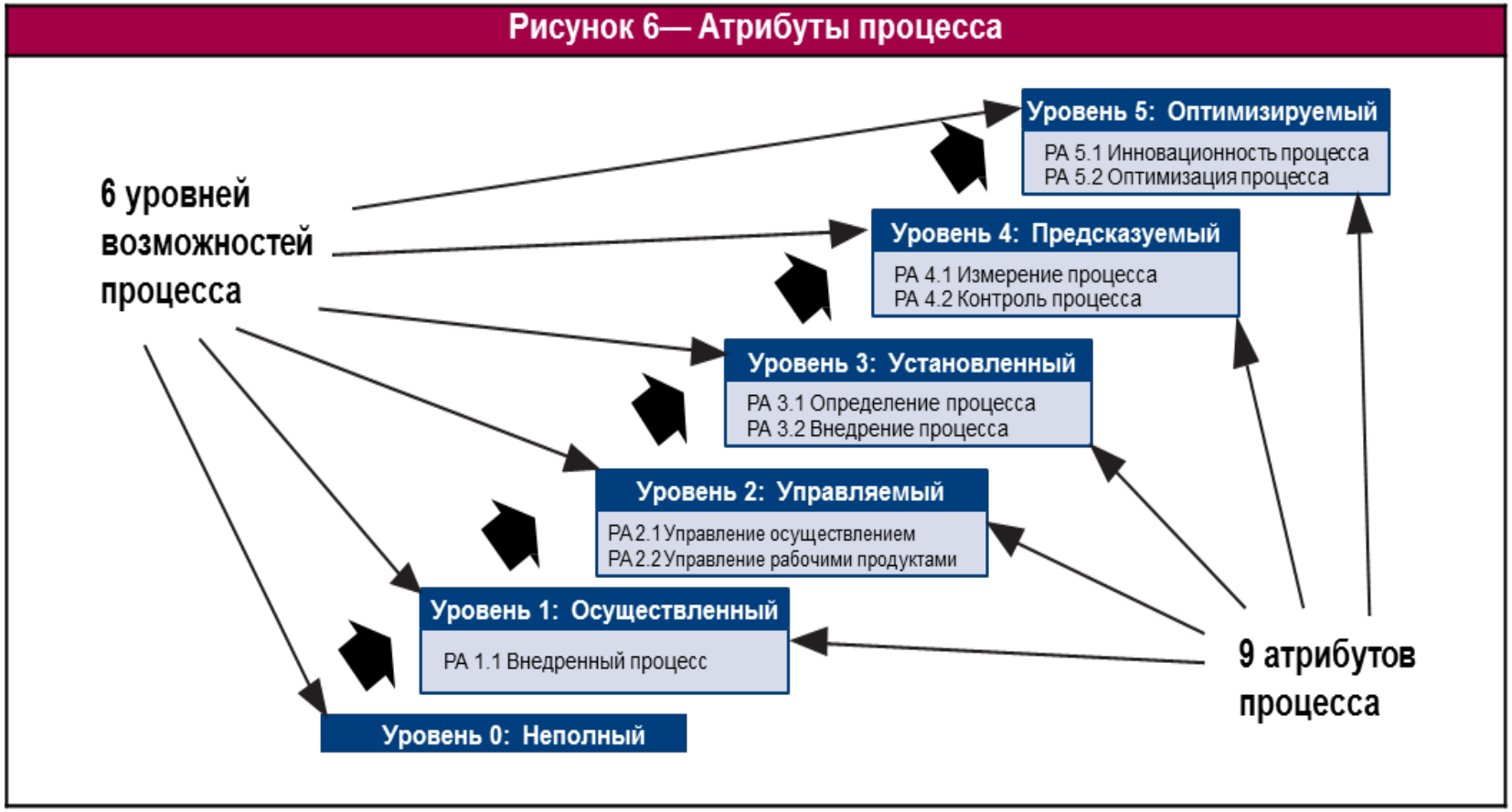
Форматы проверок

1. **Оценка уровней зрелости процессов (COBIT 4.1 Maturity Model)**
2. **Оценка уровней возможностей процессов (COBIT 5 PAM)**
3. **Оценка результативности и эффективности контролей (COBIT 5 for Assurance)**

COBIT 5 for Assurance – методология ИТ аудита

COBIT 5 предлагает детальные программы аудита по процессам – по остальным факторам влияния можно использовать, например, чек-листы от ISACA и вендоров

COBIT 5 PAM – Уровни возможностей процесса



8 GP, 2 GWP

11 GP, 5 GWP

11 GP, 5 GWP

10 GP, 4 GWP

BP, WP специфичные для каждого процесса

Процесс APO04 – Управление инновациями

Цель процесса: Достижение конкурентного преимущества, инновационности бизнеса, повышение операционной результативности и эффективности за счет развития информационных-технологий

Результаты процесса:

1. Ценность предприятия создается за счет отбора и внедрения наиболее подходящих достижений и инноваций в сфере технологии, ИТ-методов и решений
2. Задачи предприятия выполняются с получением выгод в виде улучшения качества и/или сокращения затрат в результате выявления и внедрения инновационных решений
3. Инновации поощряются и поддерживаются, являясь составной частью культуры предприятия

Базовые практики:

1. Создание среды, способствующей проведению инноваций
2. Поддержание понимания заинтересованных сторон
3. Мониторинг и изучение технологического окружения
4. Оценка потенциала передовых технологий и инновационных идей
5. Выработка рекомендаций по дальнейшим инициативам
6. Мониторинг внедрения и использования инноваций

Рабочие продукты на выходе процесса:

1. План инноваций
2. Программа признания и поощрения
3. Возможности для инноваций, привязанные к движущим силам бизнеса
4. **Исследование возможностей для инноваций**
5. **Оценка инновационных идей**
6. Рамки прототипа и краткое бизнес-обоснование
7. Результаты тестирования инициатив по созданию экспериментальных версий
8. Результаты и рекомендации, полученные по итогам выполнения инициатив по созданию экспериментальных версий
9. Анализ отклоненных инициатив
10. Оценка с использованием инновационных подходов
11. Оценка выгод от инноваций
12. Скорректированные планы инноваций

KPMG

Вопросы

kpmg.ru

kpmg.com/app