ИТ-аудит

—

Январь, 2019

Today, the course is being led by

Жанна Мусрепова

Менеджер группы
консультирования в области ИТ

zmusrepova@kpmg.kz

KPMG

Домен «Руководство и управление ИТ»

Руководство и управление ИТ

Руководство ИТ
ИТ стратегия
Модели зрелости и усовершенствования процессов;
Практики инвестирования и распределения ИТ ресурсов;
Политики и процедуры;
Управление рисками;
Практики управления ИТ;
Организационная ИТ структура и обязанности;
Планирование непрерывности бизнеса;
Политики и процедуры;
Управление рисками;
Практики управления ИТ;
Организационная ИТ структура и обязанности;
Аудит структуры и функционирования руководства (governance) ИТ;
Планирование непрерывности бизнеса;
Аудит непрерывности бизнеса.

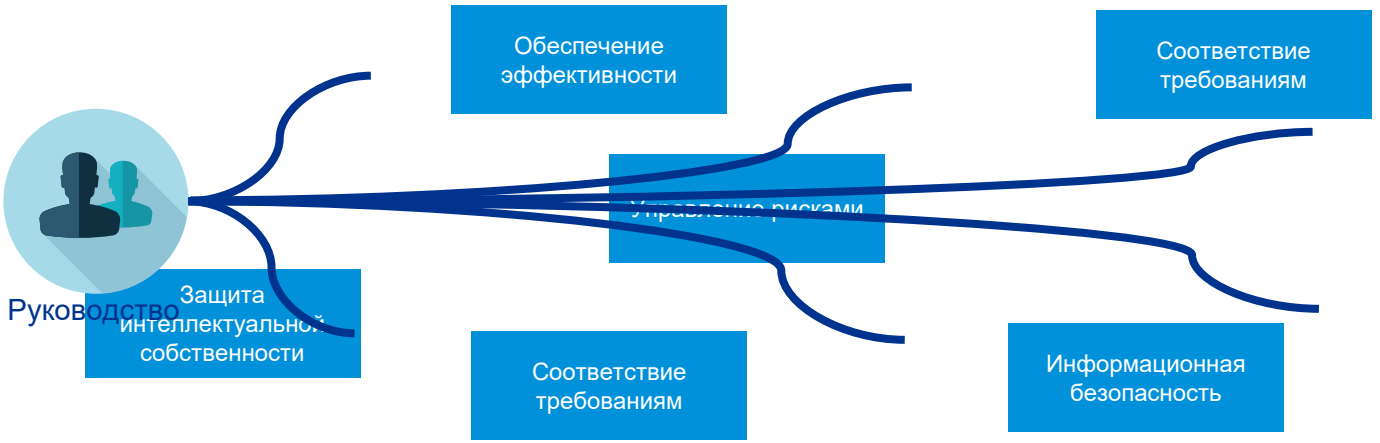
KPMG

Руководство ИТ

Руководство ИТ

В 21-ом веке информация и технологии ведут к успеху большинство международных и локальных компаний, но они так же ведут к трудностям в комплексном управлении Компании для руководства, затрагивая вопросы доверия и предоставления выгоды для всех заинтересованных сторон.

Обеспечение уверенности в соответствии ИТ целям бизнеса возлагается на руководство компании.
Требования регуляторов и постоянно развивающиеся сценарии риска требуют прямого вовлечения руководства в вопросы ИТ.



Возникает потребность в видении управления ИТ и эффективного использования ИТ для целей бизнеса. Но с чего начать, чтобы решать возникающие вопросы быстро и эффективно?

Риски, связанные с неэффективным руководством ИТ:
— Уязвимости
— Искажение информации и данных
— Нарушенная целостность системы
— Потеря конфиденциальных данных
— Скомпрометированные системы

COBIT5 (Control OBjectives for Information and related Technologies)

COBIT 5 представляет свод опыта и рекомендации мировых экспертов по эффективному управлению ИТ.

помогают

Структура

Инструменты

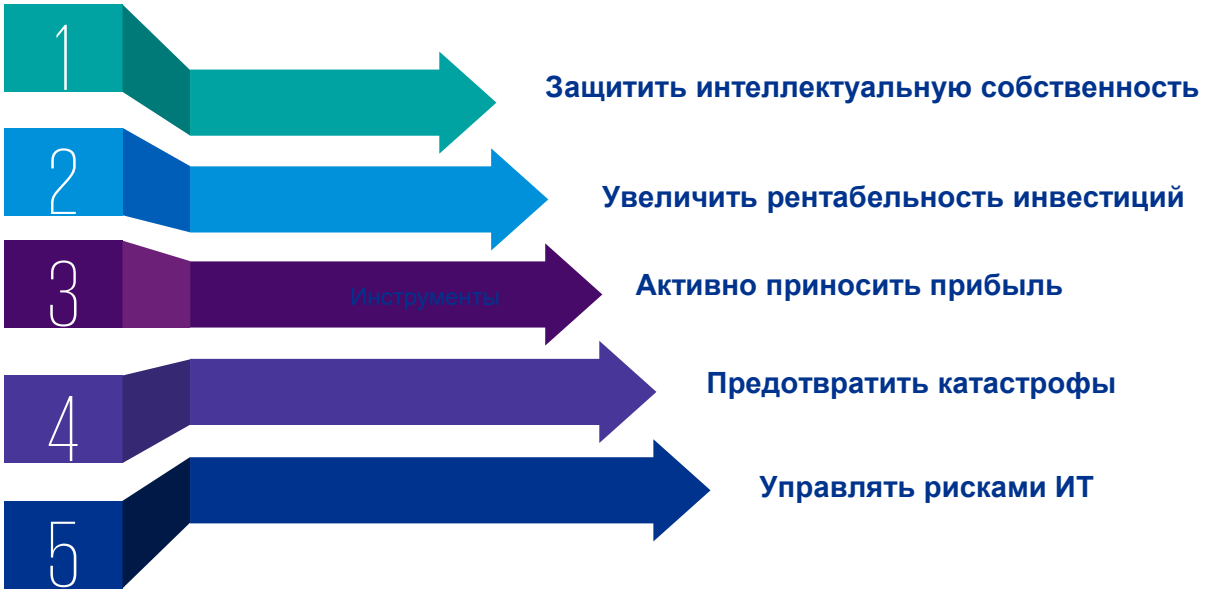
Лучшие практики

ISACA®

Trust in, and value from, information systems

COBIT5 (Control OBjectives for Information and related Technologies)

COBIT 5 представляет свод опыта и рекомендации мировых экспертов по эффективному управлению ИТ.



Цели

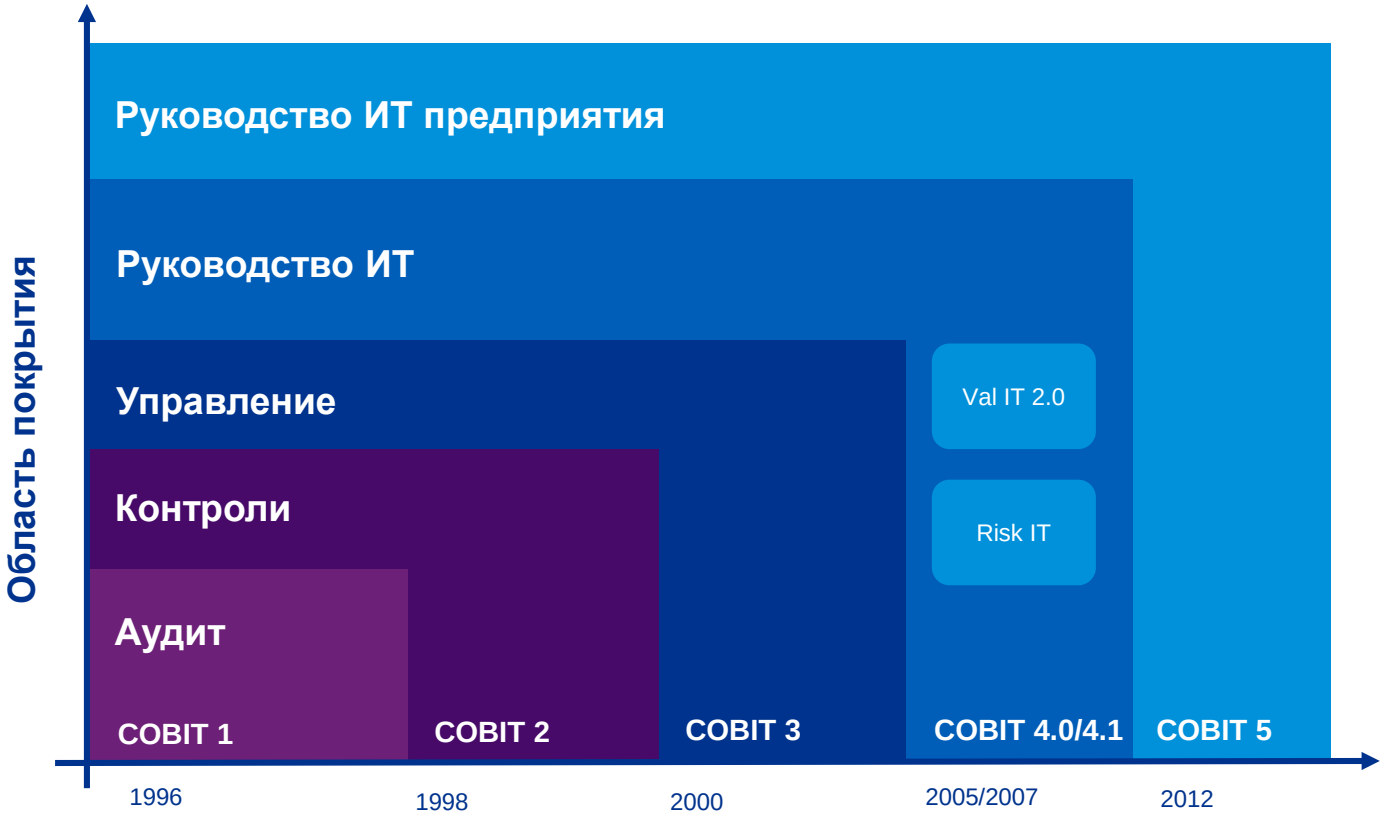
Ориентация ИТ на потребности бизнеса

Помощь в увеличении выгод, получаемых бизнесом;

Рациональное использование ИТ ресурсов

Управление ИТ-рисками надлежащим образом

Эволюция COBIT



COBIT5 Принципы

Основание: Система руководства и управления ИТ должна поддерживать реализацию целей предприятия и отвечать потребностям внешних и внутренних заинтересованных сторон (stakeholders).

Возможность: COBIT 5 предлагает расширенный и дополненный каскад целей, демонстрирующий распределение интересов заинтересованных сторон в цели предприятия, далее в цели руководства и управления ИТ на предприятии и, наконец, в цели отдельных компонентов системы руководства и управления ИТ

Предостережение: Нельзя слепо копировать эти цели в практику конкретной компании, следует использовать принцип каскадирования целей и сверяться со списками целей, предложенными COBIT, для проверки собственных решений. (COBIT предлагает каскад целей в приложениях)

Соответствие требованиям заинтересованных сторон

1

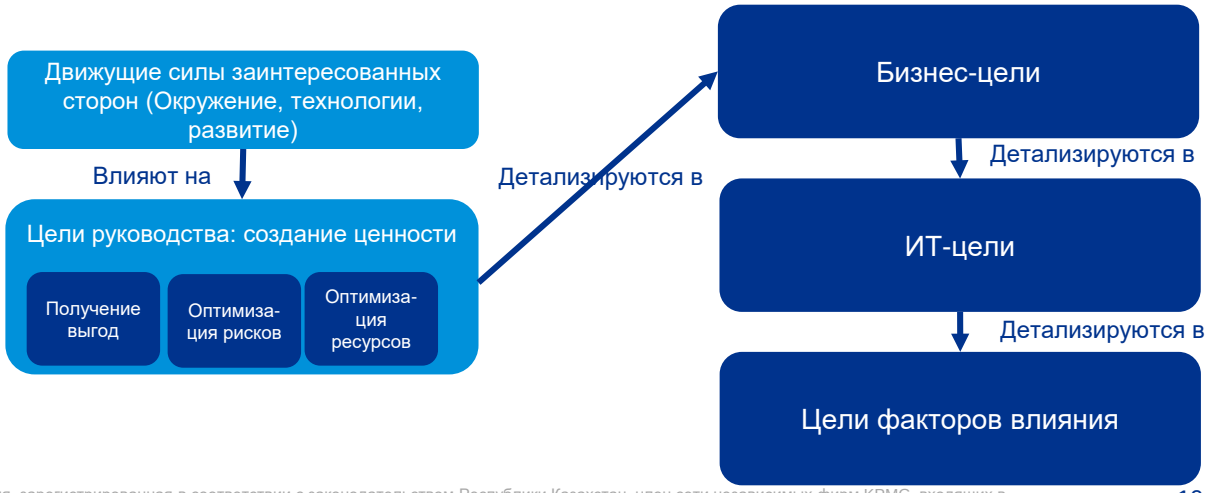


Рисунок 22 — Таблица соответствия бизнес-целей и ИТ-целей согласно COBIT

			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

Рисунок 23 — Таблица соответствия ИТ-целей и ИТ-процессов согласно COBIT 5

			ИТ-цели																
			Соответствие между ИТ- и бизнес-стратегиями	Следование внешнему законодательству и регулирующим требованиям в области ИТ и поддержка бизнес-соответствия	Лидирующая роль руководства в принятии решений в области ИТ	Управляемые ИТ-риски	Получение выгод от инвестиций с использованием ИТ и портфеля услуг	Прозрачность ИТ-затрат, выгод и рисков	Предоставление ИТ-услуг в соответствии с бизнес-требованиями	Адекватное использование приложений, информации и технических решений	Гибкость ИТ	Безопасность информации, обрабатывающей инфраструктуры и приложений	Оптимизация ИТ-активов, ресурсов и способностей	Обеспечение работы и поддержка бизнес-процессов, путем интеграции приложений и технологий в бизнес-процессы	Извлечение выгоды из программ и проектов, выполняемых в рамках сроков, бюджета и соответствующих требованиям и стандартам качества	Доступность надежной и нужной информации для принятия решений	Соблюдение внутренних политик	Компетентный и мотивированный персонал ИТ	Знания, экспертиза и инициативность для осуществления бизнес-инноваций
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	Процессы COBIT 5		Финансы					Заказчик					Внутреннее управление					Обучение и развитие	
Оценка, задание направления и мониторинг	EDM01	Обеспечение создания и развития корпоративной системы управления ИТ	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Обеспечение получения выгоды	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Обеспечение оптимизации рисков	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Обеспечение оптимизации ресурсов	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Обеспечение прозрачности для заинтересованных сторон	S	S	P			P	P						S	S	S		S
	APO01	Управление подходом к управлению ИТ	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Управление стратегией	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Управление архитектурой предприятия	P		S	S	S	S	S	S	P	S	P	S		S			S

COBIT5 Принципы

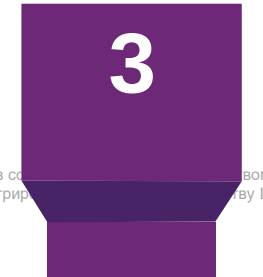
Основание:	Руководство ИТ следует рассматривать как неотъемлемую часть руководства предприятием в целом; COBIT описывает все функции и процессы, необходимые для руководства и управления информационными технологиями на предприятии.
Возможность:	Специальных инструментов, поддерживающих второй принцип, COBIT не предлагает. Тем не менее следование этому принципу определило состав ролей в матрицах ролей и ответственности для процессов, состав заинтересованных лиц, а также структуру и состав процессной модели. COBIT 5 – «методология для бизнеса», не для ИТ-отдела.

Комплексный взгляд на предприятие

COBIT5 Принципы

Основание:	Руководство ИТ следует рассматривать как неотъемлемую часть руководства предприятием в целом; COBIT описывает все функции и процессы, необходимые для руководства и управления информационными технологиями на предприятии.
Возможность:	Специальных инструментов, поддерживающих второй принцип, COBIT не предлагает. Тем не менее следование этому принципу определило состав ролей в матрицах ролей и ответственности для процессов, состав заинтересованных лиц, а также структуру и состав процессной модели. COBIT 5 – «методология для бизнеса», не для ИТ-отдела.

Применение
единой
интегрированной
методологии



COBIT5 Принципы

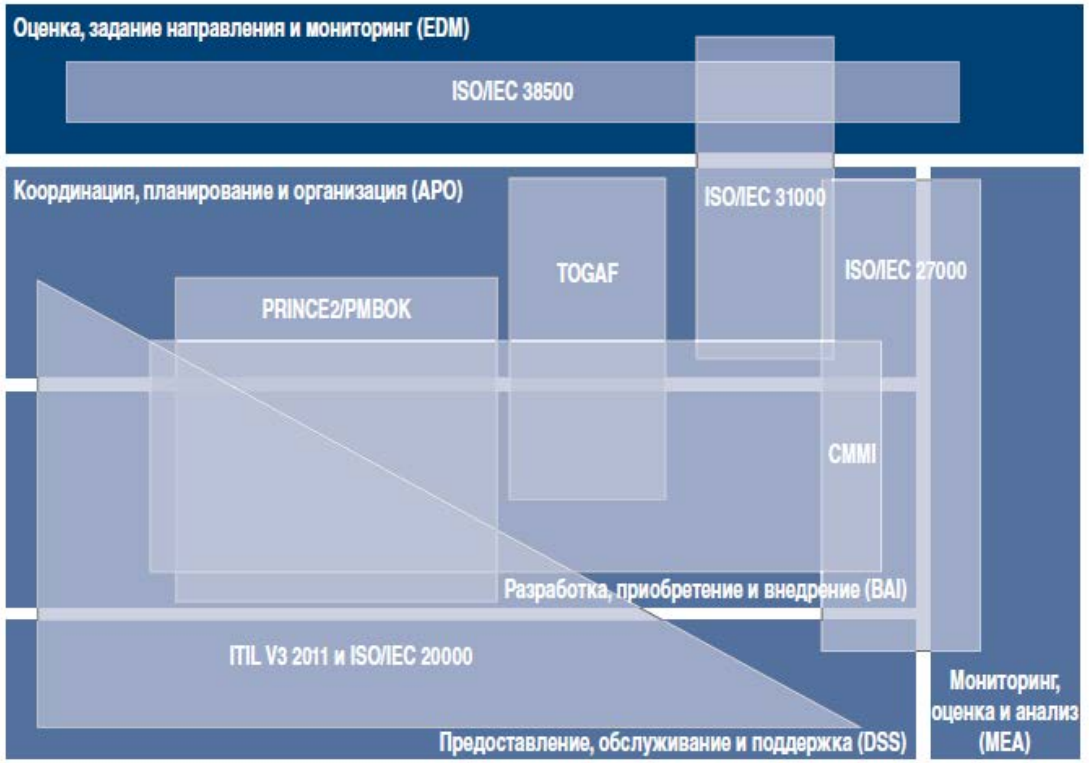
Основание:

Для руководства и управления ИТ удобно использовать единую методологию, объединившую все лучшее из современных стандартов и сводов знаний.

Возможность:

В COBIT использованы элементы стандартов (ISO 38500, ISO 27002, ISO 20000, ISO 15504, NIST и др.) и сводов знаний (ITIL, PMBOK, PRINCE2, ValIT, RiskIT, SFIA и др.), авторские подходы (Д. Коттер). В большинстве случаев явно указана ссылка на источник, во многих случаях – на конкретные главы/разделы/положения источника. Такой подход позволяет не просто лучше понимать связи рекомендаций COBIT с уже используемыми на предприятии подходами и стандартами, но и дает направление для развития компетенций при решении прикладных задач организации управления ИТ.

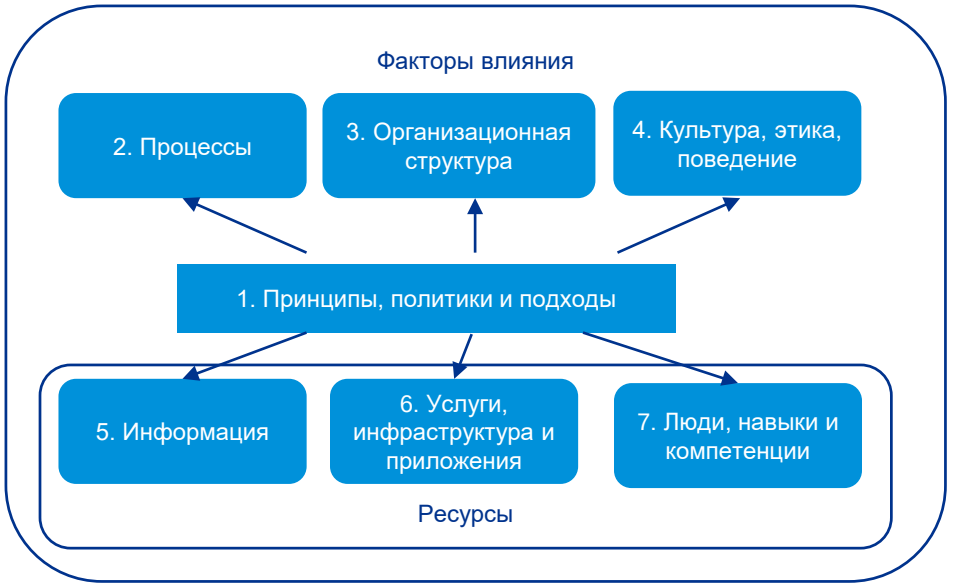
Связь COBIT 5 с другими стандартами



COBIT5 Принципы

Основание: Для эффективного руководства и управления ИТ одних процессов недостаточно, нужны и другие компоненты

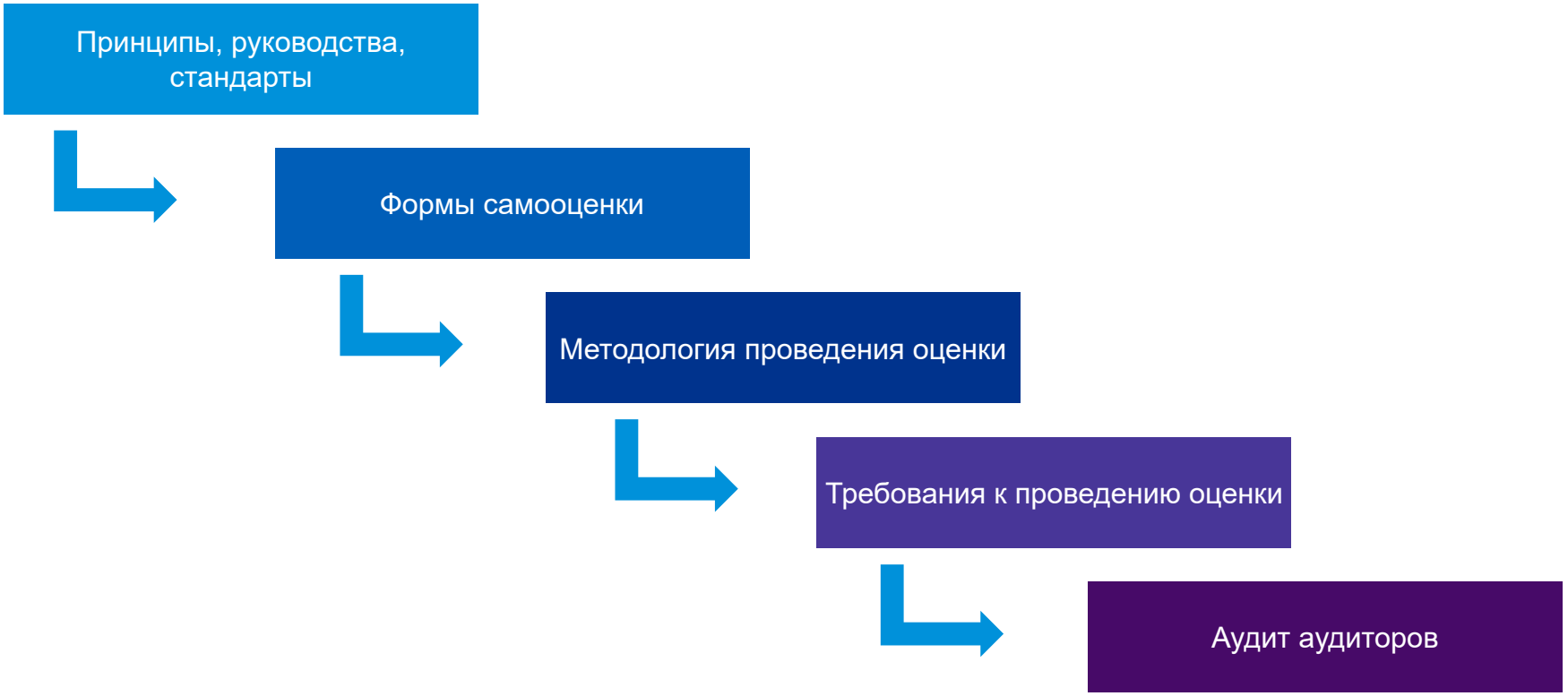
Возможность: эти компоненты в COBIT 5 называются enablers, что можно перевести как «факторы влияния».



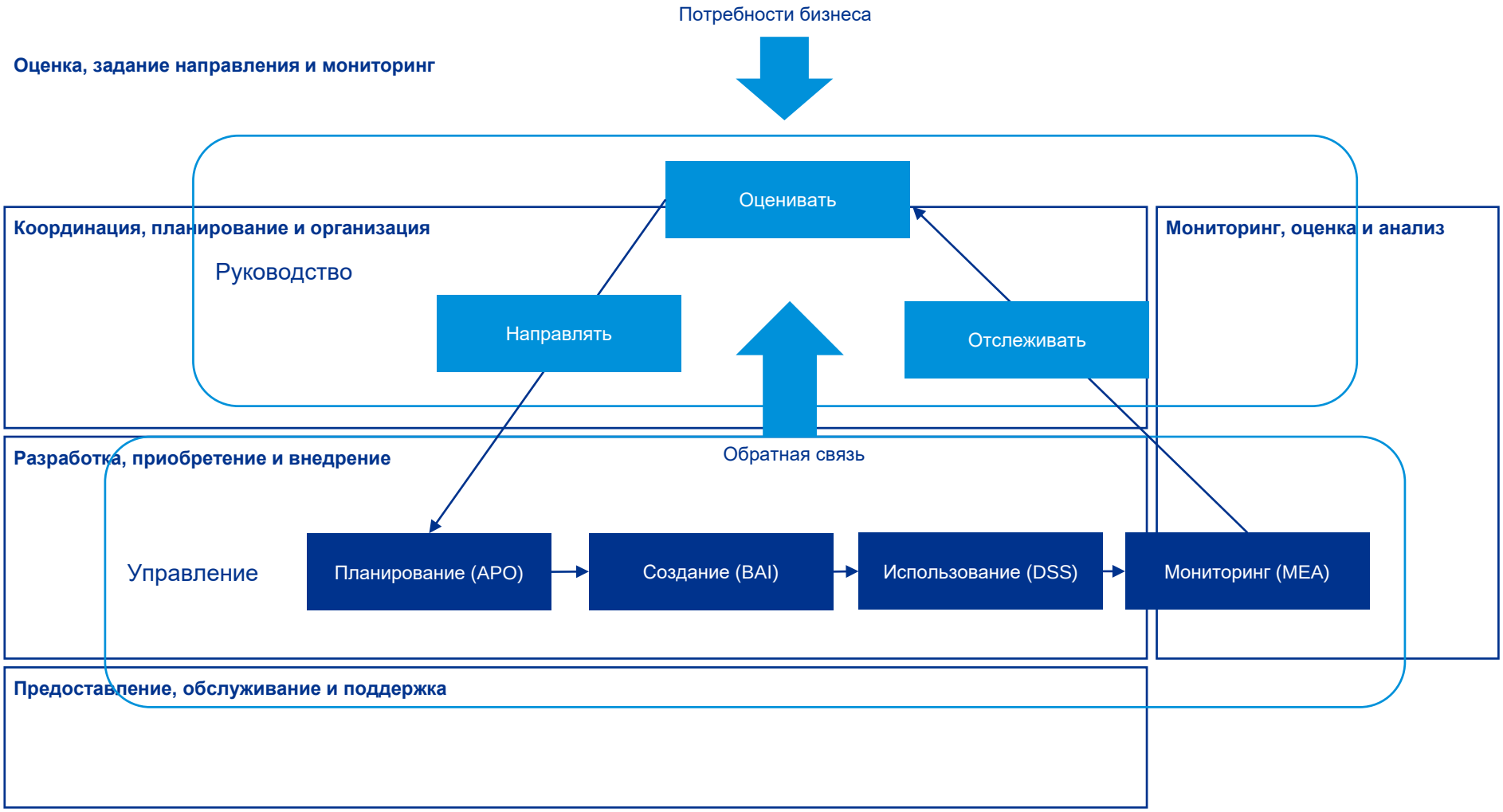
Разделение руководства и управления

Для каждого фактора влияния приведено краткое описание – в единой структуре, включающей в себя заинтересованные стороны, цели, жизненный цикл, практики и продукты, а также метрики. Структура публикаций COBIT предполагает выпуск так называемых Enabler guides, детально описывающих каждый фактор влияния. Опубликованная одновременно с базовой публикацией Enabling processes – это 230 страниц, на которых детально описаны 37 процессов.

Общий подход - начинать с руководств



Модель процессов



Модель процессов

Оценка, задание направления и мониторинг

- **EDM01** Обеспечение создания и развития корпоративной системы управления ИТ
- **EDM02** Обеспечение получения выгоды
- **EDM03** Обеспечение оптимизации рисков
- **EDM04** Обеспечение оптимизации ресурсов
- **EDM05** Обеспечение прозрачности для заинтересованных сторон

Координация, планирование и организация

- APO01 Управление подходом к управлению ИТ
- APO02 Управление стратегией
- APO03 Управление архитектурой компании
- APO04 Управление инновациями
- APO05 Управление портфелем инвестиций
- APO06 Управление бюджетом и затратами
- APO07 Управление персоналом
- APO08 Управление отношениями
- APO09 Управление соглашениями об услугах
- APO10 Управление подрядчиками
- APO11 Управление качеством
- APO12 Управление рисками
- APO13 Управление безопасностью

Разработка, приобретение и внедрение

- BAI01 Управление программами и проектами
- BAI02 Управление выявлением требований
- BAI03 Управление выбором и внедрением решений
- BAI04 Управление доступностью и мощностью
- BAI05 Управление обеспечением организационных изменений
- BAI06 Управление изменениями
- BAI07 Управление передачей и приемкой изменений
- BAI08 Управление знаниями
- BAI09 Управление активами
- BAI10 Управление конфигурациями

Предоставление, обслуживание и поддержка

- DSS01 Управление эксплуатацией
- DSS02 Управление запросами на обслуживание и инцидентами
- DSS03 Управление проблемами
- DSS04 Управление непрерывностью
- DSS05 Управление услугами безопасности
- DSS06 Управление контролями бизнес-процессов

Мониторинг, оценка и анализ

- MEA01 Мониторинг, оценка и анализ производительности и соответствия
- MEA02 Мониторинг, оценка и анализ системы внутреннего контроля
- MEA03 Мониторинг, оценка и анализ соответствия внешним требованиями

Матрица ответственностей

Strategic alignment	Risk management	Value delivery	Performance management	Resource m	Process assurance

Board of directors

Executive management

Steering committee

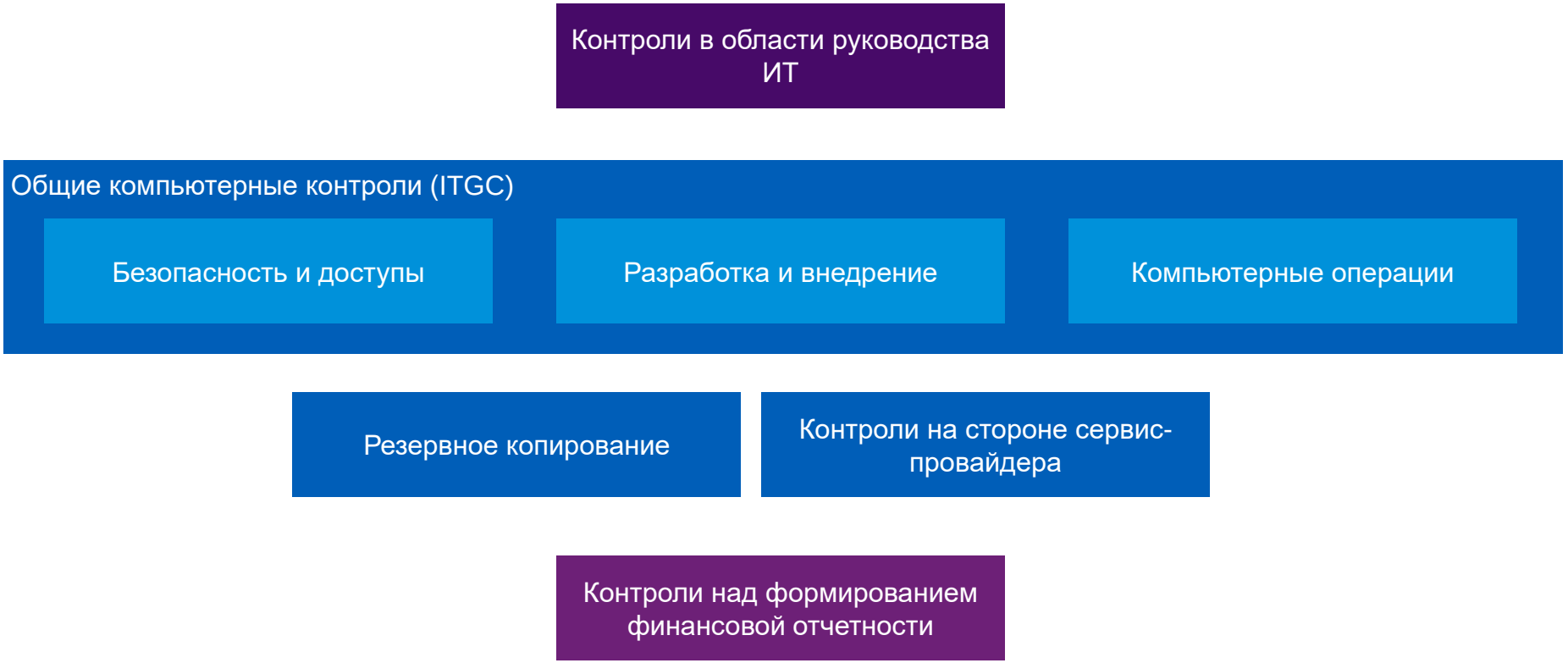
Information security management

Audit executives

Exhibit 2.6—Relationships of Security Governance Outcomes to Management Responsibilities

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	Process Assurance
Board of directors	Require demonstrable alignment.	• Establish risk tolerance. • Oversee a policy of risk management. • Ensure regulatory compliance.	Require reporting of security activity costs.	Require reporting of security effectiveness.	Oversee a policy of knowledge management and resource utilization.	Oversee a policy of assurance process integration.
Executive management	Institute processes to integrate security with business objectives.	• Ensure that roles and responsibilities include risk management in all activities. • Monitor regulatory compliance.	Require business case studies of security activities.	Require monitoring and metrics for security initiatives.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all assurance functions and plans for integration.
Steering committee	• Review and assist security strategy and integration efforts. • Ensure that business owners support integration.	Identify emerging risks, promote business unit security practices and identify compliance issues.	Review and advise on the adequacy of security initiatives to serve business functions.	Review and advise whether security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	• Identify critical business processes and assurance providers. • Direct assurance integration efforts.
CISO/ information security management	Develop the security strategy, oversee the security program and initiatives, and liaise with business process owners for ongoing alignment.	• Ensure that risk and business impact assessments are conducted. • Develop risk mitigation strategies. • Enforce policy and regulatory compliance.	Monitor utilization and effectiveness of security resources.	Develop and implement monitoring and metrics approaches, and direct and monitor security activities.	Develop methods for knowledge capture and dissemination, and develop metrics for effectiveness and efficiency.	• Liaise with other assurance providers. • Ensure that gaps and overlaps are identified and addressed.
Audit executives	Evaluate and report on degree of alignment.	Evaluate and report on corporate risk management practices and results.	Evaluate and report on efficiency.	Evaluate and report on degree of effectiveness of measures in place and metrics in use.	Evaluate and report on efficiency or resource management.	Evaluate and report on effectiveness of assurance processes performed by different areas of management.

Компоненты оценки ИТ согласно PCAOB/AICPA



KPMG

ИТ стратегия

КОНТЕКСТ СТРАТЕГИЯ

1 Сбор ожиданий

- Стратегические цели и задачи
- Болевые точки
- Анализ роли и направлений развития ИТ
- Анализ текущего состояния архитектуры
- Текущие проекты, Цифровой Казахстан
- Анализ операционной модели ИТ
- Исследование международного опыта и определение эффектов (быстрых побед)

Результат

— Стратегический контекст (модель мотивации)
— Приоритизированный перечень ожиданий бизнеса
— Обзор релевантных технологий

2 Анализ возможностей ИТ и мирового опыта

- Определение возможностей ИТ для качественного скачка автоматизации, поддержки инновационного развития
- Интегрированный подход к ИТ и цифровой трансформации
  - Сравнение с референс моделями основных процессов
  - Определение инициатив
- Концептуальный дизайн модели ИТ
  - Управление ИТ-процессами
  - Компетенции

Результат

— Экспертное заключение по референс-моделям
— Определение приоритетов инициатив (включая критерии, веса и т.д.)
— Разработка модели приоритизации инициатив (включая критерии, веса и т.д.)
— Анализ рыночных предложений для сорсинга
— Презентация концептуального видения ИТ-архитектуры с учетом цифровой трансформации и паспортов инициатив

3 Целевая архитектура

- Спринт: Бизнес-архитектура
- Спринт: Данные + Системы
- Спринт: Инфраструктура
- Спринт: Концепт по ИБ (КБ)

Результат

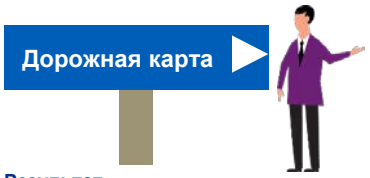
— Целевые модели
— ГЭП-анализ
— Варианты проектов

4 Оценка бизнес-кейсов

- Определение требований с привлечением международных экспертов (с указанием диапазонов NPV. IRR)
- Требования к технологиям
- Требования к цифровым платформам
- Требования к инфраструктуре
- Каталог ИТ-сервисов

Результат

— Бизнес-кейсы проектов с учетом верхнеуровневых требований
— Определение целевого набора ИТ-сервисов



Результат

— Укрупненный план перехода к целевой архитектуре
— Разработка дорожной карты с учетом приоритетов и взаимосвязей между инициативами
— Формирование итоговой консолидированной согласованной (цифровой) стратегии развития ИТ
— Презентация результатов руководству

5 Управление компетенциями

- Организационная структура
- Управление компетенциями (talent management)
- Разработка дерева КПД

Результат

— Целевая операционная модель ИТ (target operating model)
— Перечень требований к управлению компетенциями сотрудников ИТ

Управление изменениями

Управление качеством

Планирование и реализация

6

- Детальные планы
- Выделение ресурсов
- Проектный офис

Результат

— Детализированный план внедрения, включая основные вехи и взаимозависимости

— Старт программы

Тестирование

8

- Тестирование проектов
- Доработка по результатам тестирования
- Обучение сотрудников

Результат

— Сценарии тестирования

— Интерфейсы готовы и протестированы

— Пост-анализ достижения целей

Фреймворк предоставления ценности

СТРАТЕГИЯ ДИЗАЙН СОЗДАНИЕ ВНЕДРЕНИЕ УЛУЧШЕНИЕ

Разработка

7

- Вовлечение бизнес-дивизионов
- Назначение ответственных
- Отслеживание разработки

Результат

— Поддержка дивизионов

— Всеобщая осведомленность о текущих изменениях

— Solution Architecture Development

— Разработка решений

Внедрение

9

- Отслеживание внедрения
- Управление изменениями
- Сопровождение проектов

Результат

— План исполнения ключевых показателей эффективности

— Управление портфелем решений (Solution Portfolio Management)

Сопровождение

Ценность реализована

KPMG

Кейс

Кейс

Крупная региональная компания предоставляет сервисы, на рынке более 15 лет. В ней параллельно развиваются несколько организационных «проектов»:

- активное развитие новых услуг и, соответственно, при необходимости перестройка бизнес- процессов;
- региональная экспансия путем скупки небольших региональных фирм либо путем создания новых организационных единиц;
- рассматривается возможность войти в состав глобального холдинга, который выбирает объект для покупки. При этом руководство компании, не планирует выходить из бизнеса.

Все происходящие процессы требуют серьезной поддержки со стороны ИТ, поскольку таков бизнес компании (например, это телеком-оператор). Руководство компании решает вопрос о том, какие процессы, ИТ-системы и технологии должны получить дополнительные инвестиции в ближайшее время.

kpmg.kz