KPMG

Оценка ИТ в цифровую эру

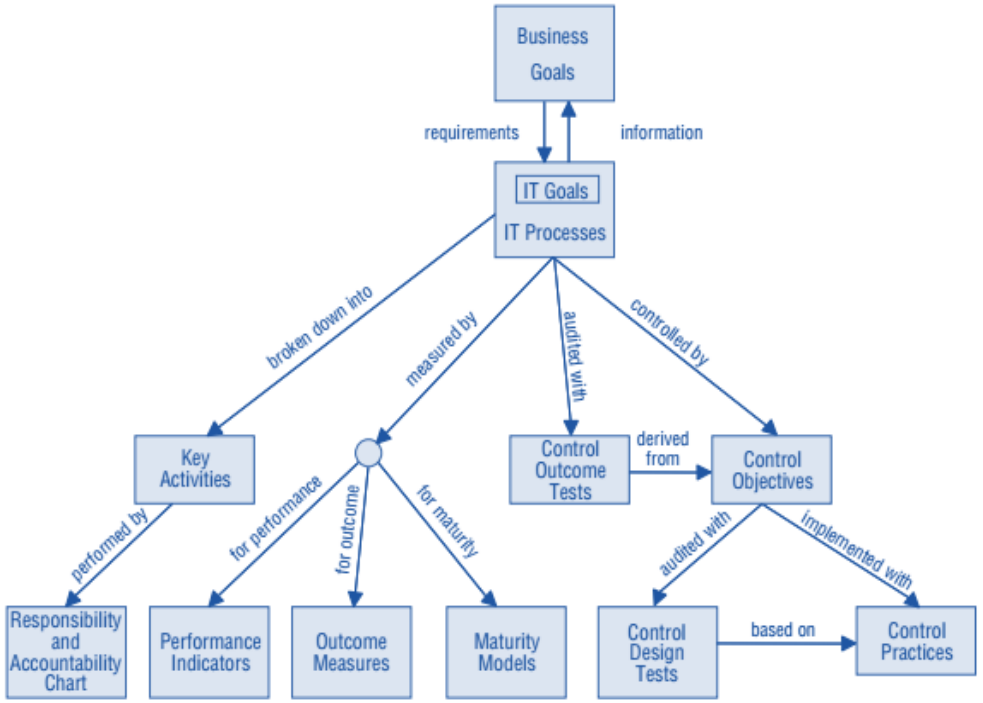
Константин Аушев

Profit Finance Day, 3 июня 2016

Традиционные методы оценки ИТ и ИБ

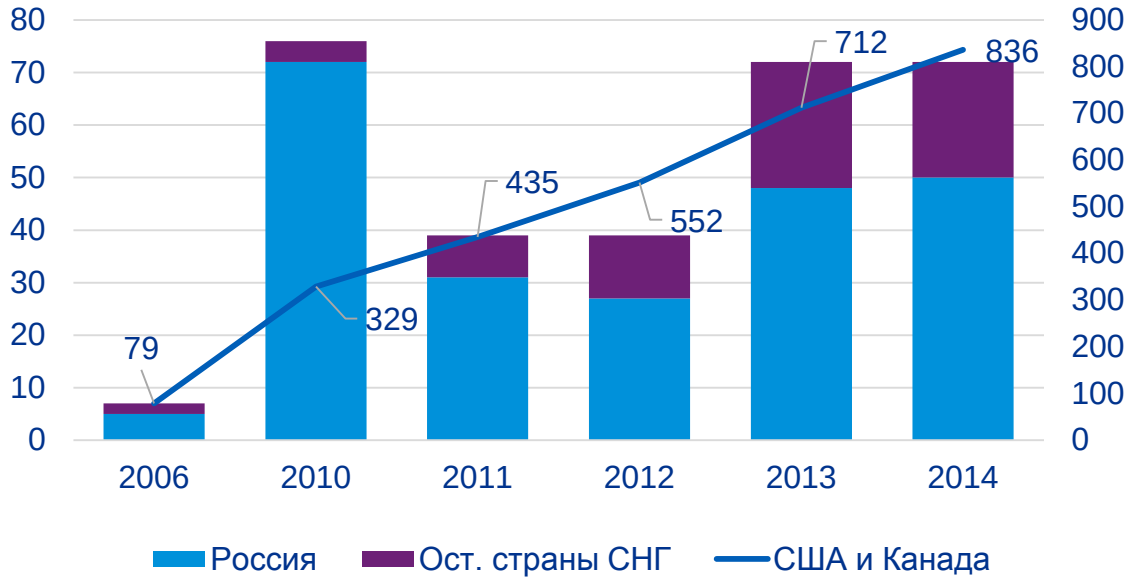
Управление ИТ — COBIT (up to 4.1)

- Подходы к управлению ИТ-процессами. Процессы, роли и ответственность
- Цели контроля и средства их достижения



Информационная безопасность — ISO 27001

- «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью»
- Измерение общих подходов и оценка контролей



© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

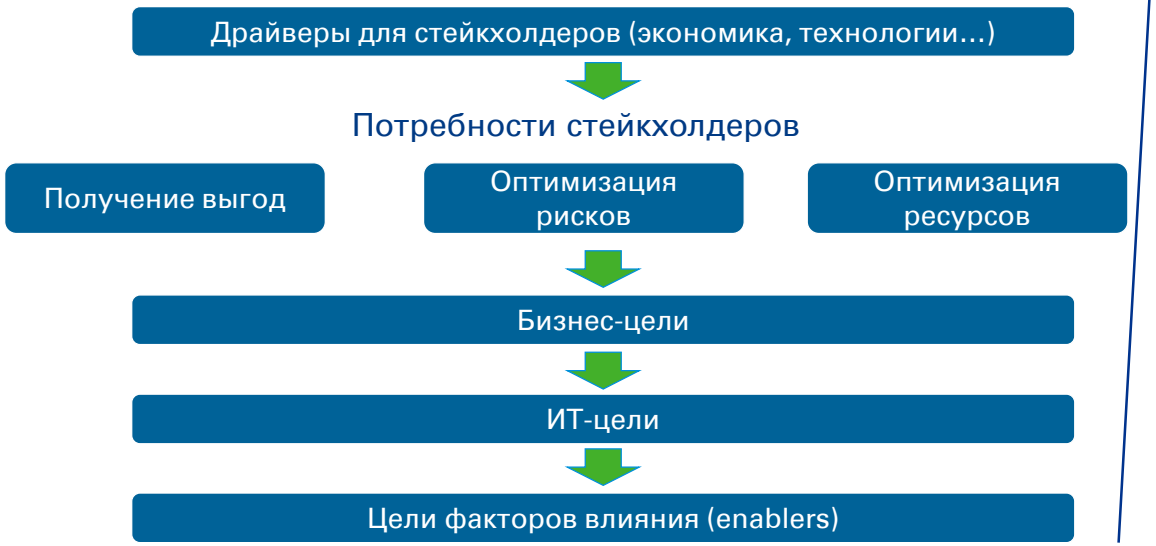
Статус документа: Публичный

Традиционные методы оценки ИТ

Появление COBIT 5:

Новые фокусы

- Корпоративное руководство и управление информационными технологиями. Процессы, роли и ответственность
- Ценности для стейкхолдеров и цели бизнеса
- Возможности, драйверы (мотивы), факторы влияния



И новая модель оценки процессов (ISO 15504)

- **Другая шкала:**

0 Неполный процесс

1 Осуществлённый процесс

2 Управляемый процесс

3 Установленный процесс

4 Предсказуемый процесс

5 Оптимизируемый процесс

+ Атрибуты процесса

Индикаторы производительности

- Результаты процесса
- Лучшие практики
- Рабочие продукты

Индикаторы возможностей

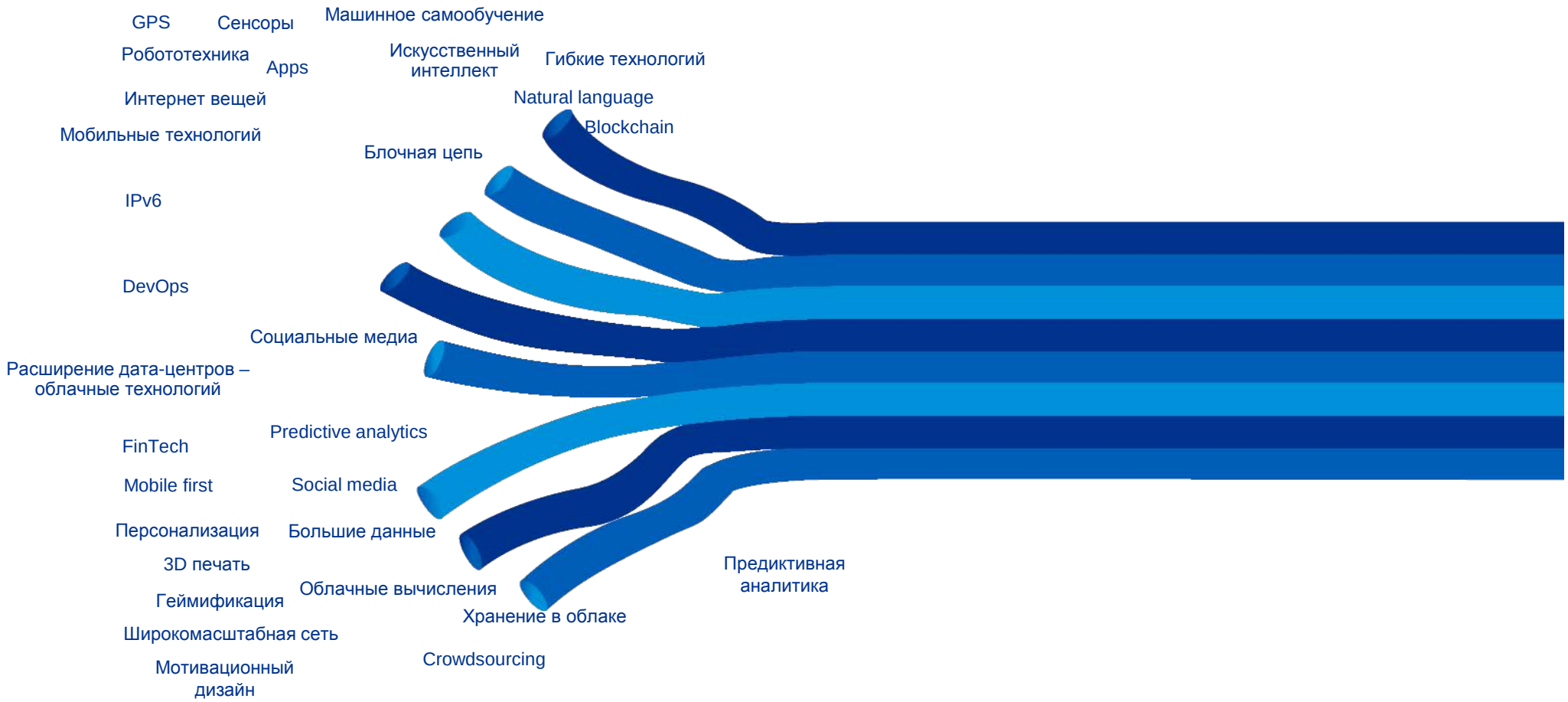
- Универсальные проекты
- Универсальные ресурсы
- Универсальные рабочие продукты

KPMG

© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

3-я индустриальная революция – Digital Disruption



© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

4-ая революция: сделать всё

Третья индустриальная революция: Цифровые инноваций

Четвертая индустриальная революция: Возможности инноваций

Нововведения путем внедрения цифровых технологий для:

- **Непрерывно продвижения технологий вперед**
- **Внедрения привлекательных и доступных решений**
- **Оцифровки и «умная» автоматизации практически всех сервисов и услуг**
- **Обеспечения постоянного доступа к данным**

© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

Цифровая оценка ИТ и ИБ сегодня

Digital Maturity Level

Cyber Security Maturity Level

KPMG

Определение цифровой зрелости

Вызовы для CIO

- Системы
  - Сложное, негибкое наследство
  - «Ипотека» по крупным старым системам
- Процессы
  - Медленная разработка процессов и методологий
  - Накопленные незавершенные проекты
- Люди и культура
  - Неполное понимание бизнеса
  - Плохие отношения с бизнесом
  - Несбалансированные знания
  - Не расположенная к риску культура
- Управление и внешняя среда
  - Строгие регуляторные требования
  - Недостаток ресурсов и фондирования
  - Проблемы с защитой информации и персональных данных

KPMG

© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

Референсные значения некоторых критериев

Приоритеты CIO

Подотчетность CEO	Вхождение в СД	Взаимодействие с бизнесом (мин. 1 д./нед. вне ИТ
34 %	57 %	40 %

Технологический фокус

На проекты, производящие деньги — 63 % / 37 % — На проекты, сохраняющие деньги

Люди и знания

Недостаток знаний и навыков	Планы по увеличению ИТ-штата на сл. год	Обеспокоенность сохранением талантов
65 %	44 %	89 %

Работа с Digital

Наличие цифровой стратегии	Наличие CDO	Ответ Digital
35 %	19 %	27 % - новые сервисы 23 % - новые каналы

Управление технологиями

Рост инвестиций в облака	Уверенность в кибербезопас-ности	Ответ Digital
31 % (в SaaS)	22 %	27 % - новые сервисы 23 % - новые каналы

Бюджетирование

45 % Факт роста бюджета	50 % Рост инвестиций в аутсорсинг	10 % Более ½ бюджета вне ИТ

Источник: KPMG & Harvey Nash CIO Survey, June 2016.

© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

Оценка уровня кибербезопасности

- Методология **Cyber Maturity Assessment (CMA)** используется для формирования целостного представления о состоянии СУИБ
- Данная методология позволяет оценить уровень зрелости информационной безопасности по определенным критериям, которые построены на основе международных стандартов и практик (**ISO2700x, BIS Ten Steps, Cyber Essentials и ITIL**)

Управление и руководство

Роли (топ-)менеджмента, владение и управление верхнеуровневыми рисками.

Человеческий фактор

Культура (знания, умения, навыки) в области информационной безопасности.

Управление ИТ-рисками

Подходы к управлению рисками владения информацией, в том числе интеллектуальной собственностью.

Непрерывность бизнеса

Уровень подготовленности к сбоям, возможности по предотвращению сбоев и минимизации последствий таковых.

Процессы и технологии

Уровень эффективности среды внутреннего контроля.

Соответствие регуляторным требованиям

Подходы к поддержанию и повышению уровня соответствия требованиям различных регуляторов, национальных и международных стандартов.

© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

Выбор направлений оценки

ЦЕЛИ

ПЕРВЫЙ ПРИОРИТЕТ

ОРГАНИЗАЦИЯ

Структура, люди, установки, фондирование

РУКОВОДСТВО

Ответственность, подотчетность, лидерство

СРЕДА И ПРЕДМЕТНАЯ ОБЛАСТЬ

Политики, руководства, стандарты

ВНУТРЕННИЕ СЕРВИСЫ

Осведомленность, тренинги, инструменты поддержки

ВТОРОЙ ПРИОРИТЕТ

РЕАЛИЗАЦИЯ И ВНЕДРЕНИЕ

Стаффинг, комплайенс, зрелость, технологии

БИЗНЕС-ВЛИЯНИЕ

БИЗНЕС-ВОЗМОЖНОСТЬ

Новые модели Cash-flow, новые модели ведения бизнеса

РАСШИРЕНИЕ СКОУПА

Приобретение конкурентных преимуществ, увеличение доли рынка, количества услуг

ЗАЩИТА БИЗНЕСА

Удовлетворение запросов к кибербезопасности с целью защиты доходов

ЗАЩИТА БРЕНДА

Минимизация репутационных рисков

ЖИЗНЕННЫЙ ЦИКЛ

ОБОРУДОВАНИЕ
Поддержка, обследование, анализ

ПРОДУКТ
Разработка, внедрение, верификация и поддержка релиза

ПРОЕКТ
Проработка, реализация, тестирование, приемка результатов

ФОКУС НА ОСНОВАНИЕ ПРИСУЩИЕ КОМПАНИИ РИСКИ

© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

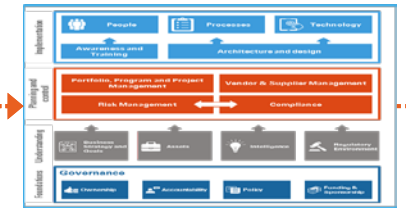
Процесс оценки кибербезопасности

ОЦЕНКА ВНЕШНИХ ФАКТОРОВ

- Угрозы
- НПА
- Взгляд клиентов

ПОНИМАНИЕ ДРАЙВЕРОВ

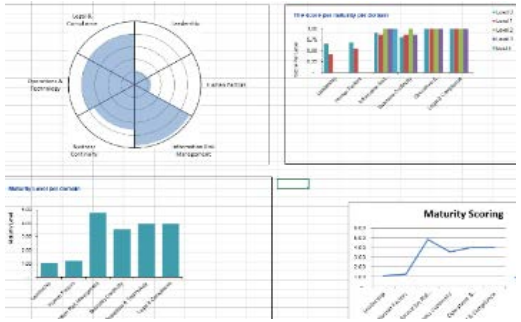
- Бизнес-требования



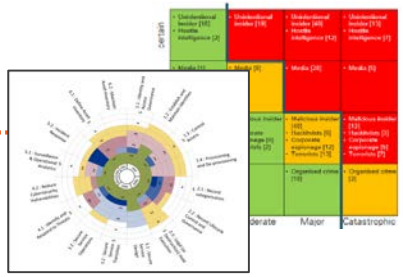
Выстраивание понимания того, что важно для СД, функции кибербезопасности и клиентов

Исследование и бенчмарк

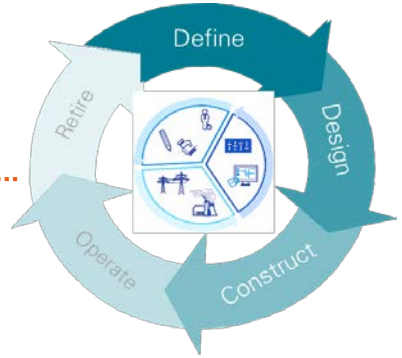
Бизнес-контекст
(Бренд, Защита бизнеса)



Обсуждение с СД



Графическое представление результатов



Детализация общей методологии оценки кибербезопасности

© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

Группы критериев оценки кибербезопасности

- Гэп-анализ (по требованиям), оценка рисков
- Безопасность в бизнес-кейсах, RFI/RFP, договорах
- Объем: роли и ответственность, результаты, конфигурация, планы, одобрения, комплайенс

- Безопасно управляемые сервисы, лицензионные обязательства
- Отказоустойчивость, способность к быстрому восстановлению
- Управление миграцией данных
- Безопасное уничтожение активов

Оценка следования стандартным процедурам и формальному контролю изменений, в том числе в части:

- Обновления ПО и оборудования
- Улучшения процессов ИБ
- Приобретения инструментов для СУИБ (например, SIEM)
- Обновления политик
- Тестирование СОНБ

- Проверка поставщиков/ вендоров
- Целевая операционная модель ИБ
- Разработка применимых политик, стандартов, процедур, контролей
- Безопасность коммуникаций и конфигурации сети
- Разработка планов тестирования, проверки кода

Реализация процессов, приобретение необходимых инструментов и прочих ресурсов для обеспечения процессов:

- Управления рисками и комплайенс
- Мониторинга информационной безопасности и реагирования на инциденты
- Управления доступом
- Идентификации уязвимостей и патч-менеджмента
- Управления антивирусными средствами
- Конфигурации сети

© 2016 ТОО «КПМГ Аудит», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Статус документа: Публичный

KPMG

Спасибо

Константин Аушев

Менеджер

Консультирование в области ИТ

kaushev@kpmg.kz

kpmg.kz

kpmg.com/app

Информация, содержащаяся в настоящем документе, 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 тщательного анализа конкретной ситуации.

© 2016 ТОО «КПМГ Такс энд Эдвайзори», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative (“KPMG International”), зарегистрированную по законодательству Швейцарии. Все права защищены.

KPMG и логотип KPMG являются зарегистрированными товарными знаками ассоциации KPMG International.