



cutting through complexity™

Первый региональный обзор по информационной безопасности в Казахстане и Кыргызстане

Февраль 2012



ТОО «КПМГ Такс энд Эдвайзори»
проспект Достык, 180
Алматы, Казахстан, 050051

Тел: +7 (727) 298 08 98
Факс: +7 (727) 298 07 08
E-mail company@kpmg.kz

Уважаемые дамы и господа,

Искренне благодарим Вас за проявленный интерес к участию в первом региональном обзоре KPMG по вопросам информационной безопасности в Казахстане и Кыргызстане.

Данный обзор призван помочь выявить общие вопросы, угрозы, риски, и тенденции в области информационной безопасности, а также оценить их влияние на деятельность организаций в Казахстане и Кыргызстане. По завершению обзора организациям-участникам будет предоставлен отчет, на основании которого Вы сможете сравнить собственные оценки со средними оценками респондентов по отрасли и региону.

Мы искренне надеемся, что данный обзор поможет Вам определить области для дальнейшего развития и улучшения информационной безопасности в Ваших организациях.

Вопросы представленные в анкете являются обобщенными, и как правило не требуют раскрытия конфиденциальной информации. Тем не менее, мы обязуемся обеспечить все необходимые меры для обеспечения конфиденциальности предоставляемых Вами данных.

В случае вопросов или комментариев просим Вас связаться с координатором обзора в Казахстане: Владимиром Ремыга по тел.+ 7 727 298 08 98 вн. 62500 или по электронной почте: VRemyga@kpmg.kz.

С уважением,

Дэвид Алун Боуэн

Управляющий Партнер в Казахстане и Центральной Азии

ТОО «КПМГ Такс энд Эдвайзори»

Анкета

Общие вопросы об организации

Название организации

Отрасль деятельности

Существует в Вашей организации специализированное подразделение по информационной безопасности?

Сколько человек в данном подразделении?

Раздел 1. Управление информационной безопасностью

1. Кто в Вашей организации курирует вопросы обеспечения информационной безопасности? (Выберите один вариант)

- Генеральный директор
- Директор по информационным технологиям
- Директор по информационной безопасности
- Директор по безопасности
- Директор по обеспечению соблюдения нормативных требований
- Директор по обеспечению защиты персональных данных
- Технический директор
- Руководитель службы внутреннего аудита
- Директор по управлению рисками
- Специалист по информационным технологиям
- Специалист по информационной безопасности
- Сетевой/системный администратор
- Иное:

2. Кому подчиняется и подотчетно данное лицо в Вашей организации? (Выберите один вариант)

- Совету директоров
- Генеральному директору
- Директору по информационным технологиям
- Директору по управлению рисками
- Техническому директору
- Иное (пожалуйста укажите):

3. Какие из перечисленные ниже направления включены в зону ответственности подразделения информационной безопасности в Вашей организации? (Выберите все подходящие варианты)

- Делопроизводство
- Защита персональных данных
- Обеспечение непрерывности бизнеса/ восстановления деятельности после сбоев
- Охрана интеллектуальной собственности/коммерческой тайны
- Разработка приложений/систем
- Расследование мошеннических действий
- Реализация проектов и программ
- Соблюдение нормативных требований в отношении ИТ (например, Базель II, закон Сарбейнса-Оксли, HIPAA, PCI DSS, FISMA, ФЗ №152, ISO 27001, и т.д.)
- Управление активами
- Управление рисками, связанными с отношениями с поставщиками

4. Какие из перечисленных ниже направлений деятельности в области информационной безопасности переданы на поддержку третьей стороне, либо рассматривается возможность их передачи? (Выберите все подходящие варианты ответа)

Переданы на субподряд в наст. время	Проводится оценка / планируется передача на субподряд	Планы передачи на субподряд отсутствуют
-------------------------------------	---	---

- Оценка/аудит информационной безопасности
- Обучение и повышение осведомленности в вопросах безопасности
- Проведение тестов на проникновение
- Расследование инцидентов /борьба с недобросовестными действиями
- Служба Help Desk (управление паролями/доступом)
- Тестирование приложений
- Управление настройками межсетевого экрана или иных средств обеспечения безопасности (например, IDS, IPS)
- Управление уязвимостями/обновлениями
- Управление непрерывностью деятельности/восстановлением после сбоев
- Управление инцидентами информационной безопасности

5. Выберите из приведенного ниже списка три главных приоритета в области безопасности на предстоящие 12 месяцев? (пожалуйста выделите только три области, отметте первую по значимости цифрой “1”, вторую по значимости – цифрой “2”, а третью – цифрой “3”)

Три приоритета

- Внедрение или совершенствование технологий и процессов по предотвращению утечки данных
- Внедрение или совершенствование технологий и процессов управления доступом и учетными записями
- Внедрение или улучшение внутренних процессов разработки ПО (например, процесса разработки защищенного ПО (secure coding), процесса контроля качества)
- Внедрение механизмов расследования инцидентов/борьбы с недобросовестными действиями
- Внедрение технологий виртуализации
- Внедрение стандартов (напр., ISO/IEC 27001, BS 25999, Webtrust, и т.д.)
- Внедрение иных технологий (просьба перечислить):
- Комплектование кадрами (например, обучение и программы повышения квалификации сотрудников)
- Передача функций обеспечения безопасности на аутсорсинг
- Разработка внутренних программ повышения осведомленности и обучения сотрудников по вопросам безопасности
- Соблюдение нормативных требований
- Совершенствование системы управления рисками информационной безопасности (включая мониторинг соблюдения требований регулирующих органов)
- Тестирование функции обеспечения информационной безопасности (например, тестирование на проникновение)
- Управление рисками

6. Отметьте то определение, которое лучше всего характеризует ежегодные инвестиции в информационную безопасность в Вашей организации. (Выберите один вариант)

- Увеличение доли в общих расходах организации
- Снижение доли в общих расходах организации
- Относительно постоянная доля в общих расходах организации

7. Для каждого из перечисленных перспектив развития информационной безопасности выберите определение, которое лучше всего характеризует текущую ситуацию в Вашей организации.

Увеличить расходы	Уменьшить расходы	Без изменений
----------------------	----------------------	------------------

- Внедрение или совершенствование технологий и процессов по предотвращению утечки данных
- Внедрение или совершенствование технологий и процессов управления доступом и учетными записями
- Внедрение или совершенствование внутренних процессов разработки ПО (например, процесса разработки защищенного ПО (secure coding), процесса контроля качества)
- Внедрение механизмов расследования инцидентов в области ИБ/борьбы с недобросовестными действиями
- Внедрение стандартов (например, ISO/IEC 27001, BS25999, и .т.д.)
- Внедрение технологий виртуализации
- Внедрение иных технологий (просьба перечислить):

- Комплектование кадрами (напр., привлечение собственных ресурсов)
- Передача функций обеспечения безопасности на аутсорсинг
- Разработка внутренних программ повышения осведомленности и обучения сотрудников в области безопасности
- Соблюдение нормативных требований
- Совершенствование системы управления рисками в области информационной безопасности (включая мониторинг соблюдения требований регулирующих органов)
- Тестирование функции обеспечения информационной безопасности (например, тестирование на проникновение)
- Управление рисками

8. Утверждена ли в Вашей организации стратегия информационной безопасности на ближайшие 1-3 года?

- Да – перейти к вопросу 9.
- Нет – перейти к вопросу 10.

9. Выберите варианты ответов, применимые в отношении Вашей стратегии информационной безопасности:

- За последние год проводился её пересмотр и обновление
- Она разработана в соответствии с общей бизнес-стратегией организации
- Она разработана в соответствии с ИТ стратегией организации
- В стратегию информационной безопасности включен план мероприятий в области безопасности на ближайшие 3-5 лет

10. Утверждена ли в Вашей организации политика информационной безопасности?

- Да – перейти к вопросу 11.
- Нет – перейти к вопросу 12.

11. Выберите варианты ответов, применимые в отношении Вашей политики информационной безопасности:

- За последние 12 месяцев проводился её пересмотр и обновление
- Она была официально утверждена высшим руководством компании
- В политике регламентированы роли и должностные обязанности сотрудников
- В политике рассматриваются правовые аспекты обеспечения безопасности
- Политика содержит определение организационной структуры службы информационной безопасности
- Политика доведена до сведения всех работников Вашей организации (включая: штатных сотрудников, подрядчиков, временных сотрудников и третьих лиц)

12. Какие из перечисленных ниже разделов определены политикой информационной безопасности или несколькими нормативными документами в области ИБ? (Выберите все подходящие варианты)

- Классификация данных/информации
- Использование электронной почты и Интернета
- Использование мобильных или портативных устройств/носителей (планшеты, смартфоны, USB-носители и т.п.)
- Обеспечение конфиденциальности данных/защиты персональных данных
- Правила чистого рабочего стола/экрана
- Требования к используемым паролям
- Хранение/уничтожение данных/информации

13. Оцените перечисленные ниже факторы, влияющие на реализацию инициатив в области информационной безопасности в Вашей организации (шкала оценок от 1 до 5, где 1 – "Не представляет затруднений", 5 – "Существенные затруднения")

Не представляет затруднений

Существенные
затруднения

1 2 3 4 5

- Неопределенность в бизнесе (например, из-за финансового кризиса)
- Организационные изменения (например, в результате слияний и поглощений)
- Изменения или отсутствие ясности в нормативных и законодательных актах
- Поддержка со стороны руководства
- Наличие требуемых ресурсов
- Адекватный бюджет
- Изучение новых технологий
- Выявление/оценка новых угроз и уязвимостей
- Повышение осведомленности персонала

14. Каким образом в вашей организации производится оценка эффективности работы процесса обеспечения информационной безопасности? (Выберите все подходящие варианты ответа)

- Самостоятельная внутренняя оценка силами службы ИТ или информационной безопасности
- Проведение оценки службой внутреннего аудита
- Оценка внешними аудиторами в рамках проведения внешнего аудита финансовой отчетности
- Оценка независимым подрядчиком
- Сравнение с аналогичными/конкурирующими организациями
- Официальная сертификация в соответствии с международными стандартами безопасности (напр., ISO/IEC 27001 или Webtrust)

Официальная сертификация в соответствии с отраслевыми стандартами безопасности, напр., стандарт защиты информации в индустрии платежных карт (Payment Card Industry Data Security Standard – PCI DSS)

Оценка не проводится

15. Внедрена ли в Вашей организации система управления информационной безопасностью (СУИБ)? (Выберите один вариант)

Да, внедрена и официально сертифицирована (напр., ISO/IEC 27001)

Да, внедрена, но задача сертификации не ставится

Да, в процессе внедрения

Нет, но такая возможность рассматривается

Нет, и такая возможность не рассматривается

16. Каким из перечисленных ниже стандартов/лучших практик управления информационной безопасностью используются в Вашей организации? (Отметьте основной стандарт/лучшие практики цифрой “1”, а любые используемые вместе с ним вспомогательные стандарты/системы – цифрой “2”)

ISO/IEC 27002:2005

ISO/IEC 27001:2005

Information Security Forum’s (ISF) Standard of Good Practice

CobIT

COSO

Information Technology Infrastructure Library (ITIL)

Capability Maturity Model Integration (CMMI)

Generally Accepted Privacy Principles

PCI DSS

Webtrust

Иной отраслевой стандарт:

Иное:

17. Изменился ли объем следующих видов тестирования на проникновение, проводимых в Компании, за последние 12 месяцев?

Объем тестирования увеличился	Объем тестирования уменьшился	Объем тестирования не изменился	Тестирование не проводится
-------------------------------	-------------------------------	---------------------------------	----------------------------

Проведение анализа исходных кодов приложений

Тестирование возможности внешнего проникновения из сети

Тестирование защищенности внутренней инфраструктуры организации (операционных систем, баз данных, сетей)

Анализ защищенности беспроводных сетей

Тестирование защищенности средств предоставления удаленного доступа (модемные пулы, VPN)

Проведение тестирования сотрудников организации с применением методов социальной инженерии

Тестирование физического периметра путем физического проникновения в защищенные помещения и здания

Тестирование защищенности систем IP-телефонии

Иное:

18. Как часто сотрудники подразделения информационной безопасности в Вашей организации проводят встречи со ключевыми лицами или группами для обсуждения потребностей/мероприятий в области информационной безопасности?

Каждый месяц Каждый квартал Дважды в год Ежегодно Никогда

Совет директоров
 Топ-менеджмент (напр., генеральный директор, финансовый
 Комитет по аудиту
 Руководители операционных подразделений
 Отдел информационных технологий
 Служба внутреннего аудита
 Служба контроля соблюдения законодательства
 Юридический отдел / Главный юрисконсульт
 Служба управления рисками
 Ответственный за обеспечение защиты персональных
 Отдел кадров
 Служба эксплуатации и обслуживания
 зданий/сооружений
 Иное:

Раздел 2. Технические мероприятия по ИБ

19. Какие механизмы используются в Вашей организации для повышения эффективности управления процессом информационной безопасностью? (Выберите все подходящие варианты ответа)

Внедрение средств непрерывного мониторинга контроля доступа
 Аутсорсинг отдельных мероприятий в области безопасности
 Стандартизация на базе единой системы контрольных процедур
 Внедрение системы сбалансированных показателей (ССП или KPI)
 Внедрение средств управления учетными записями
 Внедрение дополнительных средств обеспечения безопасности

20. Какие из перечисленных ниже механизмов управления доступом и учетными записями внедрены или планируются к внедрению в Вашей организации? (Выберите все подходящие варианты ответа)

Внедрено в наст. момент Планируется в течение года Внедрение не планируется

Автоматизация процесса предоставления доступа (запрос, согласование, предоставление)
 Федеративный доступ к данным
 Единый вход в корпоративные информационные системы (Single sign-on)
 Управление ролями пользователей
 Управление правами пользователей
 Управление учетными записями пользователей
 Управление паролями пользователей
 Многофакторная аутентификация (E-token, SmartCard, ...)
 Защищенное хранение паролей/управление привилегированным доступом
 Виртуальный каталог/централизованное хранилище учетных записей
 Управление доступом к веб-приложениям
 Централизованное журналирование и мониторинг
 Инфраструктура открытых ключей (Public Key Infrastructure – PK)
 Контроль за доступом в сеть/построение сетей (NAC)

21. Какие из перечисленных ниже средств в Вашей организации используются для контроля за утечкой конфиденциальной информации? (Выберите все подходящие варианты)

- Внедрены средства мониторинга/фильтрации контента
- Используются средства аудита
- Внедрены средства анализа журнала событий
- Доступ к конфиденциальной информации ограничен определенными периодами времени
- Применяется блокировка/ограничение использования отдельных компонентов аппаратного обеспечения (портов USB/ FireWire)
- Запрещено использование устройств со встроенной камерой в зонах ограниченного доступа
- Разработана специальная политика в отношении классификации конфиденциальной информации и порядка работы с ней
- Внедрены дополнительные механизмы безопасности в целях защиты информации (напр., шифрование)
- Ограничено/запрещено использование систем мгновенного обмена сообщениями или электронной почты для передачи конфиденциальной информации
- Сформулированы конкретные требования к пересылке/удаленному доступу к конфиденциальной информации

22. Проведена ли в Вашей организации инвентаризация и классификация информационных ресурсов? (Выберите один вариант)

- Да, для всех критичных ресурсов
- Да, для некоторых критичных ресурсов, работа не завершена
- Нет, не проведена

23. Каким образом Вы проверяете, обеспечивают ли Ваши партнеры, поставщики или подрядчики необходимый уровень защиты Вашей информации при ее обработке, передаче и хранении? (Выберите все подходящие варианты)

- Анализ результатов оценок и иных сертификаций, проводимых внешними поставщиками или подрядчиками (например ISO/IEC 27001, BS 25999)
- Анализ результатов проведения независимых оценок партнеров, поставщиков или подрядчиков, проведенных внешними организациями (например, SAS 70, ISAE 3402)
- Проведение оценки силами Вашего подразделения информационной безопасности или службы внутреннего аудита (напр., выезд на место, тестирование системы безопасности)
- Анализ или оценка не проводится
- Иное:

24. Какое из приведенных ниже определений в отношении защиты персональных данных могла бы сделать Ваша организация? (Выберите все подходящие варианты ответа)

- Мы имеем четкое представление о законодательных и нормативных актах в области защиты персональных данных, которые могут оказать влияние на нашу организацию
- Мы провели инвентаризацию информационных активов, на которые распространяются требования по защите персональных данных
- Мы провели оценку жизненного цикла персональных данных (сбор, использование, хранение, передача и уничтожение)
- Мы внедрили специальные контрольные процедуры для защиты персональных данных
- Мы внедрили процесс мониторинга и сопровождения контрольных процедур, связанных с защитой персональных данных
- Мы внедрили процедуру реагирования и управления инцидентами, относящимися к защите персональных данных
- Мы включили требования по защите персональных данных в договоры с независимыми партнерами, поставщиками и подрядчиками

25. Включены ли в договоры, заключаемые Вашей организацией с клиентами, партнерами или подрядчиками, конкретные требования по обеспечению информационной безопасности? (Выберите один вариант)

Да, все договора включают в себя конкретные требования к обеспечению информационной безопасности

Да, отдельные договора включают в себя конкретные требования к обеспечению информационной безопасности

Нет, конкретные требования к обеспечению информационной безопасности не включаются в договора

26. Какие из перечисленных пунктов входят в программу по обеспечению непрерывности бизнеса в Вашей организации? (Выберите все подходящие варианты)

Установленные отношения с местными экстренными службами (пожарные, полиция, скорая медицинская помощь)

Определение очередности восстановления критичных бизнес-процессов

Согласованные полномочия и обязанности всех участников группы по восстановлению в условиях инцидента или кризисной ситуации

Выявление и оценка основных угроз и рисков, влияющих на непрерывность деятельности

Процедуры управления инцидентами или кризисной ситуацией (в том числе, порядок эскалации кризисной ситуации, а также внутренние и внешние коммуникации)

План восстановления ИТ инфраструктуры после сбоев (IT DRP)

Процедуры восстановления бизнес-процессов

План тестирования системы обеспечения непрерывности бизнеса, включающий в себя обзор упражнений и тестов

Стратегия по обеспечению непрерывности бизнеса, направленная на восстановление ИТ и телекоммуникаций, сопутствующей инфраструктуры, а также критичных бизнес-процессов в случае экстренной ситуации

Планы повышения осведомленности и обучения персонала по вопросам обеспечения непрерывности бизнеса

27. Каким образом в Вашей организации проходит оценка программы по обеспечению непрерывности деятельности? (Выберите все подходящие варианты)

Тестирование с использованием контрольных листов

Тестирование полного нарушения деятельности организации и функционирования ИТ-инфраструктуры (тестирование фактических отказов)

Проведение имитационного тестирования восстановления деятельности бизнес подразделений после сбоев

Проведение имитационного тестирования восстановления ИТ-инфраструктуры после сбоев

Проведение полного имитационного тестирования восстановления ИТ после сбоев

Моделирование процесса управления кризисной ситуацией (для руководителей операционных подразделений и высшего руководства)

Проведение полного имитационного тестирования нарушения непрерывности деятельности организации (моделирование экстренной ситуации)

Параллельное тестирование (проводится на резервных площадках)

Оценка не проводится

28. Как в Вашей организации построено взаимодействие с ключевыми контрагентами в контексте обеспечения непрерывности деятельности? (Выберите все подходящие варианты)

Рассылка анкеты с вопросами по обеспечению непрерывности деятельности

Запрос копий отчетов о тестировании планов обеспечения непрерывности деятельности

Проведение аудита программы по обеспечению непрерывности деятельности

Выдвижение контрагенту требования о прохождении официальной сертификации в области обеспечения непрерывности деятельности (напр., BS 25999-1)

Никаких мер не предпринимается. Никакие запросы в отношении обеспечения непрерывности деятельности контрагентами не направляются

29. Какие вопросы рассматриваются в программе повышения осведомленности по вопросам безопасности, принятой в Вашей организации? (Выберите все подходящие варианты)

Повышение осведомленности по вопросам обеспечения информационной безопасности

Проверка, согласование и соблюдение действующих политик и стандартов в области безопасности

Оценка эффективности мероприятий по повышению осведомленности и улучшение существующей программы на основании результатов такой оценки

Распространение наглядных и регулярных новостей/оповещений о существующих угрозах для Вашей организации

Распространение информационных сводок по новым актуальным темам

Проведение специальных мероприятий или тренингов в области безопасности для пользователей, входящих в группы высокого риска

Иное:

30. Какие из перечисленных ниже технологий Ваша организация использует или планирует использовать? (Выберите все подходящие варианты)

Используется в наст. момент Планируется в течение года В процессе оценки

Радио частотные идентификаторы (RFID)

Виртуализация серверов

VoIP

Системы управления доступом и учетными записями

Беспроводная связь

Многофакторная аутентификация (802.1x, токены)

Storage area networks/network attached storage

Программные средства корпоративного управления, управления рисками и соблюдения нормативных требований

Средства мониторинга/фильтрации контента

Средства предотвращения утечки данных

Технические средства защиты авторских прав

Шифрование данных на жестких дисках ноутбуков

Шифрование данных на жестких дисках настольных компьютеров

Шифрование съемных носителей

Шифрование электронной почты

Облачные вычисления

Распределенные вычисления

Использование биометрических средств

Совмещение физической и логической безопасности (например, объединение параметров физического и логического доступа)

Раздел 3. Движущие факторы развития Информационной Безопасности

31. Насколько важны вопросы информационной безопасности для обеспечения следующих направлений деятельности Вашей организации? (шкала оценок от 1 до 5, где 1 – "Не важно", 5 – "Весьма важно")

Не важно					Весьма важно
1	2	3	4	5	
					Защита репутации и бренда
					Защита интеллектуальной собственности
					Обеспечение защиты персональных данных
					Обеспечение поддержки при запуске новой услуги или
					Обеспечение соблюдения нормативных требований
					Обеспечение соответствия внутренним политикам
					Повышение эффективности управления ИТ и операционной деятельности
					Повышение доверия со стороны заинтересованных лиц
					Взаимодействие с внешними поставщиками
					Изучение новых и развивающихся технологий
					Содействие в ходе слияний, поглощений и продажи
					Поддержка в вопросах управления операционными и/или корпоративными рисками

32. Какова значимость перечисленных ниже последствий потери или хищения информации Вашей организации? (шкала оценок от 1 до 5, где 1 – "Наименее значимо", 5 – "Наиболее значимо")

Наименее значимо					Наиболее значимо
1	2	3	4	5	
					Ущерб для репутации и бренда
					Снижение доходов
					Потеря клиентов
					Утрата доверия со стороны заинтересованных лиц
					Судебные/юридические разбирательства
					Ухудшение отношений с сотрудниками
					Нормативно-правовые действия/санкции
					Потеря конкурентных преимуществ (например, из-за потери объекта интеллектуальной собственности)

33. Учитывая современную экономическую ситуацию, предполагаете ли Вы увеличение вероятности реализации следующих угроз? (Выберите все подходящие варианты ответа)

- Рост внешних атак (например, фишинг, атаки на Интернет-сайт)
- Рост мошеннических действий со стороны клиентов/контрагентов/партнеров
- Рост атак изнутри (например, злоупотребление правами доступа, хищение информации и т.п.)
- Рост мошеннических действий, совершенных внутри компании
- Изменений не предполагаем

34. Учитывая современную экономическую ситуацию, насколько сильно Ваша организация обеспокоена возможностью злонамеренных действий со стороны сотрудников, уволившихся из организации за последнее время? (Выберите один вариант)

- Весьма обеспокоены и принимаем меры, позволяющие минимизировать риски
- Весьма обеспокоены, однако мы не оценивали потенциальные риски
- Несколько обеспокоены и стараемся получить представление о потенциальных рисках
- Не обеспокоены
- Неприменимо

35. Какие меры приняты в Вашей организации для минимизации потенциальных рисков, возникающих в результате сокращения штата? (Выберите все подходящие варианты ответа)

- Оценка и совершенствование средств контроля за изменениями в информационных системах
- Оценка и совершенствование средств управления доступом и учетными записями
- Внедрение программы предотвращения утечки данных
- Разработка программы сохранения знаний, обеспечивающей сохранение знаний в случае увольнения ключевых сотрудников
- Меры не принимались
- Неприменимо
- Иное:

36. Какое влияние оказывает соблюдение нормативных и регуляторных требований на величину годовых затрат на обеспечение информационной безопасности в Вашей организации?

За
предыдущие 3
года За текущий год

- Существенное увеличение затрат на обеспечение информационной безопасности
- Умеренное увеличение затрат
- Величина затрат не изменилась
- Затраты сократились

37. Какое влияние оказывает соблюдение нормативных и регуляторных требований на эффективность обеспечения информационной безопасности в Вашей организации?

За
предыдущие 3
года За текущий год

- Существенное увеличение эффективности обеспечения информационной безопасности в результате соблюдения нормативных требований
- Умеренное увеличение эффективности
- Без изменения
- Эффективность обеспечения информационной безопасности снизилась в результате соблюдения нормативных требований

Контакты

Дэвид Алун Боуэн
Управляющий Партнер в Казахстане и Центральной Азии
Т +7 727 2980898
E ABowen@kpmg.kz

Владимир Ремыга
Старший Менеджер
Т +7 727 2980898
E VRemyga@kpmg.kz

Алексей Кан
Старший Консультант
Т +996 312 623380
E AKan@kpmg.kg

www.kpmg.kz

www.kpmg.kg

© 2012 ТОО «КПМГ Такс энд Эдвайзори», компания, зарегистрированная в соответствии с законодательством Республики Казахстан находящаяся под контролем KPMG Europe LLP; член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

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 консультации с соответствующими специалистами и тщательного анализа конкретной ситуации.

KPMG, логотип KPMG и слоган "cutting through complexity" являются зарегистрированными товарными знаками ассоциации KPMG International.

