# Безопасность «облачных» вычислений - необходимые условия доверия

**Инфодокум 2012**

**Денис Безкоровайный, CISA, CISSP, CCSK**
**Вице-президент RISSPA,**
**Co-организатор Cloud Security Alliance Russian Chapter**

# Безопасность наглядно

cloud security alliance SM
CSA Russian Chapter


RISSPA

# Поедем?

# Почему клиенты не переходят в облака?

Безопасность данных

Потеря контроля

Доступность

Сложность выполнения требований

# Варианты повышения доверия

- Подтверждение и аудит эффективности ИБ третьей стороной
- Открытый диалог с клиентами на тему ИБ

# Сертификация и аудит облачных провайдеров – множество систем

ISO 27001

SSAE 16 / ISAE 3402 (SOC report)

AICPA/CICA Trust Services Examination

PCI DSS

FedRAMP / FISMA

CSA Open Certification Framework

CSA STAR

# Сертификация и аудит облачных провайдеров - категоризация

Проверка конкретного перечня контролей

PCI DSS, SOC report, FedRAMP

Проверка системы управления ИБ и управление рисками

ISO 27001

# Пример FedRAMP

Мотивация простая – доступ к госзаказу


RISSPA

# ISO 27001

Применимость:

- Information Security Management System

**(Система Управления Информационной Безопасностью, СУИБ)**

- Ответственность менеджмента
- Внутренний аудит СУИБ
- Оценка менеджментом СУИБ
- Улучшения СУИБ

Контроли из Приложения – только рекомендованные

Дополнительные контроли могут быть применимы к облачным провайдерам

# Недостатки существующих подходов

Не существует простого, недорого способа оценки и сравнения провайдеров по параметрам надежности и защиты данных.

Сложность соотнесения «облачных» контролей с существующими нормативами и стандартами.

Неполнота или недостаточность контролей:

1. ISO 27001 не проверяет эффективность контролей
2. SOC report проверяет работу контролей, но не оценивает эффективность их выбора

cloud security alliance SM
CSA Russian Chapter

OCF™
Open Certification Framework

Global, Trusted Certification of Cloud Providers

# Что такое OCF ?

RISSPA

# Что такое CSA OCF

Создание CSA Open Certification Framework направлено на создание глобальной, аккредитованной, доверенной сертификации провайдеров облачных услуг.

Это программа для гибкой, последовательной и многоуровневой сертификации провайдеров в соответствии с лидирующим в индустрии руководством по безопасности от Cloud Security Alliance.

Программа призвана интегрироваться с существующими практиками аттестации и аудита для избегания дублирования усилий и вложений.

# Cloud Security Alliance
# Open Certification Framework

Три ступени

- Самооценка
- Подтверждение аудитом
- Постоянный мониторинг соответствия

# Самооценка, первый этап

Единая форма для ИБ-вопросов на основе лучших мировых практик

Перевод документа от Cloud Security Alliance:

«Опросник оценки состояния безопасности облачной среды»

www.risspa.ru/csa

| Группа защитных мер (ГЗМ) | CGID (код группы) | CID (код меры) | Вопрос |
|---|---|---|---|
| **Соответствие требованиям** | | | |
| Планирование аудита | CO-01 | CO-01.1 | Формулируются ли аудиторские утверждения в общепринятой структурированной форме (например, CloudAudit/A6 URI Ontology, CloudTrust, SCAP/SYBEX, GRC XML, ISACA Cloud Computing Management Audit/Assurance Program и т.п.)? |
| Независимый аудит | CO-02 | CO-02.1 | Разрешаете ли вы просматривать клиентам отчеты об аудитах, подготовленных третьей стороной по стандартам SAS70 Type II/SSAE 16 SOC2/ISAE3402 или другим подобным стандартам? |
| | | CO-02.2 | Проводите ли вы регулярно сетевые тесты на проникновение в инфраструктуру ваших облачных сервисов в соответствии с рекомендациями отрасли и передовой практикой? |
| | | CO-02.3 | Проводите ли вы регулярно тесты на проникновение на уровне приложений в инфраструктуру ваших облачных сервисов в соответствии с рекомендациями отрасли и передовой практикой? |
| | | CO-02.4 | Проводите ли вы регулярные внутренние аудиторские проверки в соответствии с отраслевыми указаниями и передовой практикой? |
| | | CO-02.5 | Проводите ли вы регулярные внешние аудиторские проверки в соответствии с рекомендациями отрасли и передовой практикой? |
| | | CO-02.6 | Доступны ли результаты сетевых тестов на проникновение вашим клиентам по их запросу? |
| | | CO-02.7 | Доступны ли результаты внутренних и внешних аудиторских проверок вашим клиентам по их запросу? |
| Аудит третьей стороны | CO-03 | CO-03.1 | Разрешаете ли вы вашим клиентам проводить независимую оценку уязвимостей? |
| | | CO-03.2 | Проводится ли третьей стороной внешнее периодическое сканирование уязвимостей, а также периодические тесты на проникновение в ваши приложения и сети? |
| Сотрудничество с властями | CO-04 | CO-04.1 | Есть ли у Вас представитель или координатор, отвечающий за сотрудничество с местными властями в соответствии с договорными обязательствами и соответствующими нормативными документами? |
| Соотнесение информационных систем с законодательством | CO-05 | CO-05.1 | Есть ли у вас возможность логического сегментирования или шифрования данных клиентов таким образом, чтобы была возможность вывести только данные одного клиента, без случайного доступа к данным другого клиента? |

# Подтверждение независимым аудитом, этап 2

Аккредитация аудиторов

Программа аудита – разрабатывается

Основная методология – ISO 27001 и CSA Cloud Control Matrix

# Постоянный мониторинг, этап 3

Автоматизированный процесс сбора ИБ метрик с облачной инфраструктуры провайдера

Интеграция со средствами мониторинга клиентами облачных провайдеров

# С чего начать провайдерам?

Самооценка безопасности про CAIQ позволит:

1. Понять текущее состояние ИБ
2. Выявить области для улучшения
3. Результаты можно использовать для CSA STAR

# Клиентам следует требовать подтверждения безопасности

RISSPA

# Cloud Security Alliance
# Russian Chapter

Локализация руководств и результатов исследований CSA

Адаптирование лучших практик CSA к российским условиям и законодательству

Разработка рекомендаций для российских потребителей облачных услуг

www.risspa.ru/csa

# Вопросы?

RISSPA
be professional

bezkod@RISSPA.ru
Денис Безкоровайный

www.RISSPA.ru

LinkedIn