

Основные этапы процесса достижения соответствия PCI DSS

Сергей Шустиков

Digital Security

Руководитель направления менеджмента ИБ, CISA, PCI QSA

Соответствие PCI DSS

1. Соответствие PCI DSS – это **100% выполнение требований стандарта**
2. **Обязательно** для всех компаний, работающих с платежными картами: **банков, процессинговых центров, торгово-сервисных предприятий, поставщиков услуг**
3. **Крайний срок** достижения соответствия по требованиям Visa – **30 сентября 2010 года**
4. Для **поставщиков услуг**, обрабатывающих данные о более чем **300 000 платежных карт в год**, обязателен **ежегодный аудит**, подтверждающий соответствие требованиям PCI DSS, проводимый компанией, обладающей статусом **QSA**

Процесс достижения соответствия

1. **Предварительный аудит** – определение исходного уровня несоответствия
2. **Разработка рекомендаций** по устранению несоответствий
3. **Разработка технического проекта** изменений, вносимых в информационную инфраструктуру
4. **Внедрение изменений** в информационную инфраструктуру
5. **Разработка и документирование процессов управления** информационной безопасностью
6. **Регламентированные проверки** - тест на проникновение и ASV-сканирование
7. **Сертификационный аудит** – итоговое подтверждение соответствия
8. **Согласование результатов** оценки соответствия с МПС или эквайером

Роли исполняют

**Заказчик****QSA-консультант****Интегратор**

Варианты взаимодействия

1. **Малый или средний заказчик, который самостоятельно внедряет изменения:**



2. **Крупный заказчик, QSA-консультант является интегратором:**



3. **Крупный заказчик, QSA-консультант и интегратор – независимы:**



Оптимальный вариант для малого заказчика

1. **QSA-консультант** проводит предварительный аудит

2. **QSA-консультант** разрабатывает подробные рекомендации

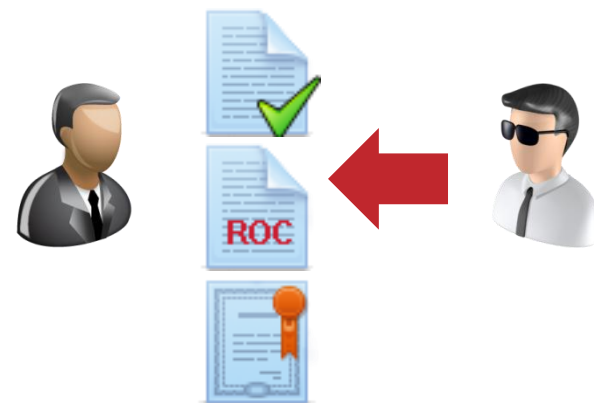


3. **Заказчик** планирует и внедряет изменения в инфраструктуру

4. **QSA-консультант** документирует процессы управления ИБ

5. **QSA-консультант** проводит регламентированные проверки

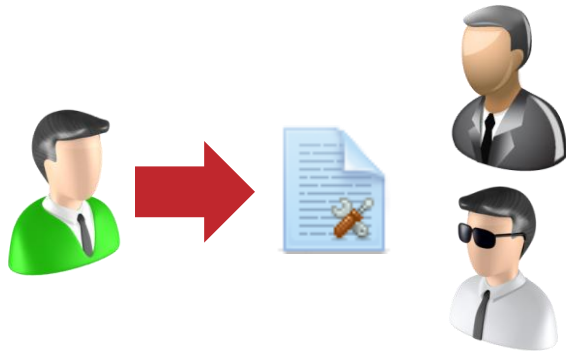
6. **QSA-консультант** проводит сертификационный аудит



Оптимальный вариант для крупного заказчика

1. **QSA-консультант** проводит предварительный аудит

2. **QSA-консультант** разрабатывает подробные рекомендации

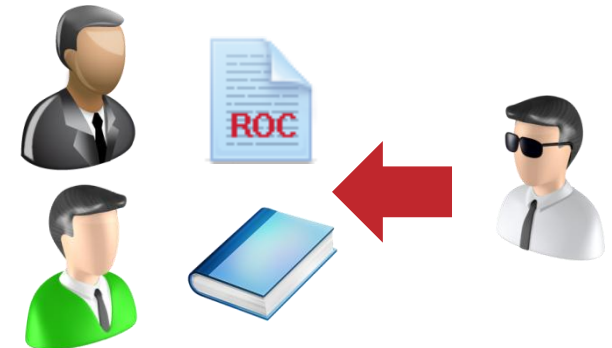


3. **Интегратор** разрабатывает технический проект изменений

4. **Заказчик и QSA-консультант** согласуют технический проект

5. **Интегратор** внедряет изменения в инфраструктуру

6. **QSA-консультант** контролирует процесс внедрения



Оптимальный вариант для крупного заказчика

7. **QSA-консультант** документирует процессы управления ИБ



8. **Интегратор** разрабатывает низкоуровневые процедуры



9. **QSA-консультант** проводит регламентированные проверки


10. **QSA-консультант** проводит сертификационный аудит

Документооборот




Результат

соответствие \neq безопасность



**Стремление к соответствию
не обеспечит безопасность**



**Стремление к безопасности
обеспечит соответствие**

Вопросы?

Ответы на PCIDSS.RU!

