

PCI DSS

Глазами клиента

Загарский С.М.

Директор Департамента сопровождения
информационных и платежных систем

ОАО «БИНБАНК»

Зачем моей компании PCI DSS?

— [Вы должны соответствовать требованиям PCI DSS если ваша компания обрабатывает, хранит, либо передает карточные данные.

— [PCI DSS как бизнес-требование со стороны ваших клиентов.

— [Вам нужен PCI DSS, чтобы обеспечить должный уровень защиты своего бизнеса и бизнеса своих клиентов.

В первую очередь...

- [Определите к какой категории предприятий относится ваша компания – от это зависит набор требований стандарта
- [Создайте проектную команду
- [Определите необходимые ресурсы и бюджет проекта

Выбор аудитора

Факторы, влияющие на выбор компании-аудитора (QSA):

— [Обоюдная заинтересованность в успешном результате

— [Уровень компетентности

— [Стоимость услуг

Типичные ошибки

— [Неверная интерпретация требований

— [Отсутствие сегментации сети

— [Попытка пройти аудит без тщательной предварительной подготовки

“Проблемные” пункты

— [3. Защита хранения данных

— [11. Периодическое тестирование систем и процессов

— [8. Контроль доступа

— [10. Аудит и логирование

Аудит пройден - что дальше?

— [Безопасность - это процесс, у которого есть начало, но нет конца

— [RSI аудит сложен только в том случае, если вы его еще не разу не прошли