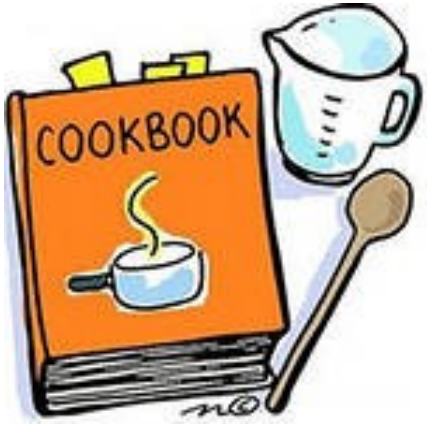
«PCI DSS Cookbook – рецепты приготовления»

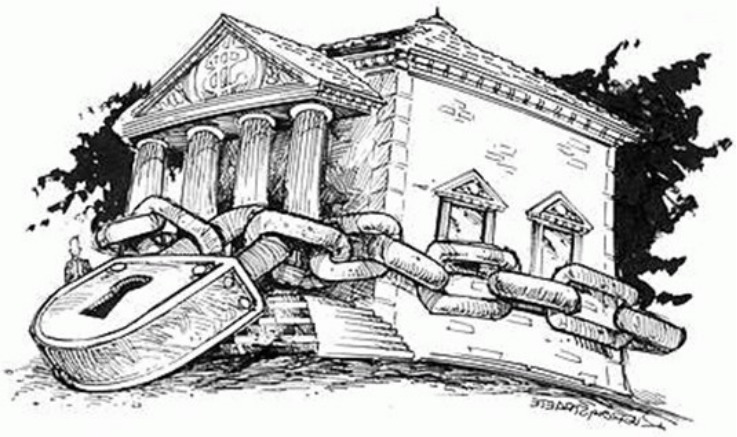
Начальник УИБ Банка «ХКФБ»
Юрий Лысенко.

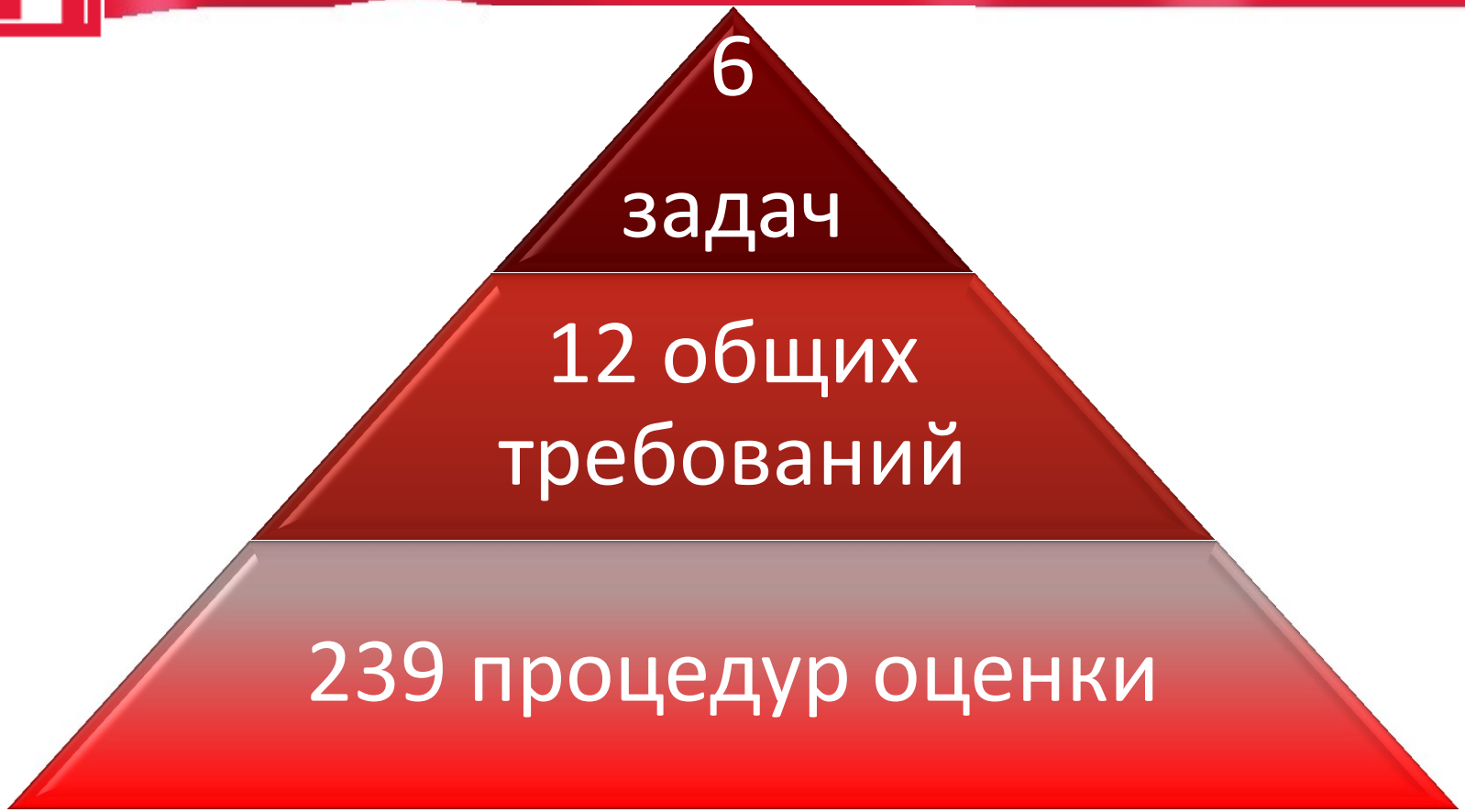


«Я сейчас расскажу Вам, что такое PCI и где у меня этот DSS»

Андрей Грициенко, начальник СИБ АКБ «Возрождение»

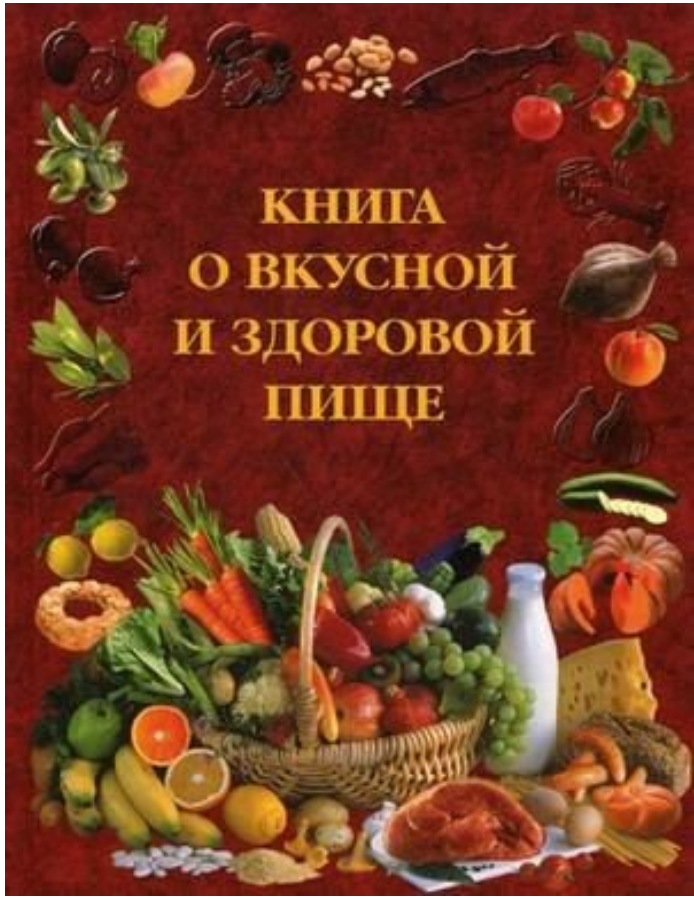
(фраза сказанная на одном из форумов по ИБ после сертификационного аудита банка)





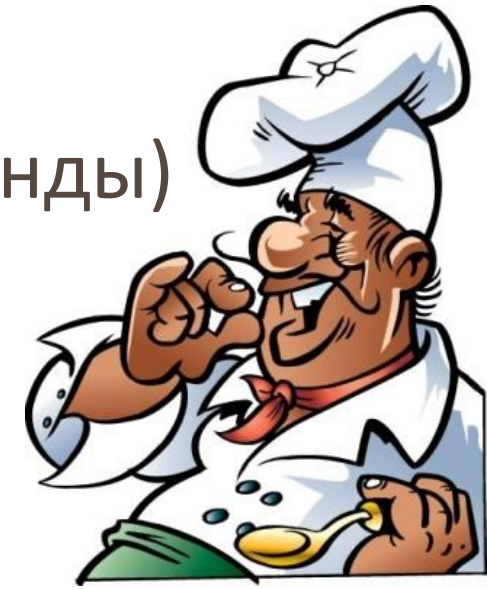
PCI DSS - Информационная инфраструктура (системные компоненты – любое сетевое оборудование, сервер или приложение, а также виртуализованные компоненты, которые включены в среду данных (совокупность людей, процессов, оборудования о держателях карт или соединено с ней), если в ней хранятся, обрабатываются или передаются карточные данные (включают данные о держателях карт и критичные аутентификационные данные).

1. Шеф-повар и помощники
2. Контроль качества продуктов
3. Составление меню
4. Ингредиенты
5. Готовка
6. Время приготовления
7. Дегустация



1. Шеф-повар и помощники

(Формирование проектной команды)

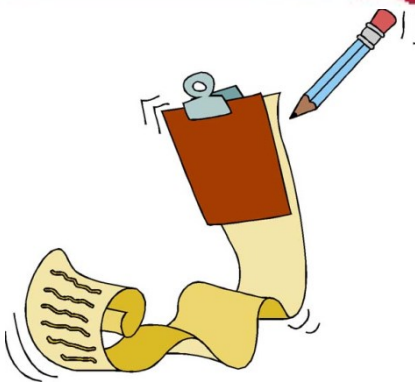


- Приказ
- Формирование проектной команды
- Зоны ответственности
- Полномочия
- Ресурсы
- Выбор аудитора

2. Контроль качества продуктов

(Предаудит)

- Определение области проверки
- Инвентаризация данных платежных карт
- Опрос сотрудников
- Получение информации
- Анализ конфигураций



3. Составление меню

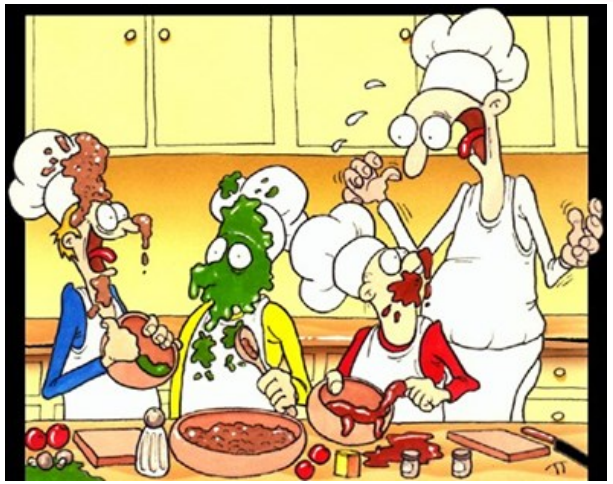
(Сужение области проверки)

- Основное для уменьшения времени и ресурсов
- Разработка решений по изменению инфраструктуры
- Пересмотр логики приложений
- Определение бизнес-процессов возможных к изменению
- Подготовка обоснований для исключений

4. Ингредиенты

(Поиск решений)

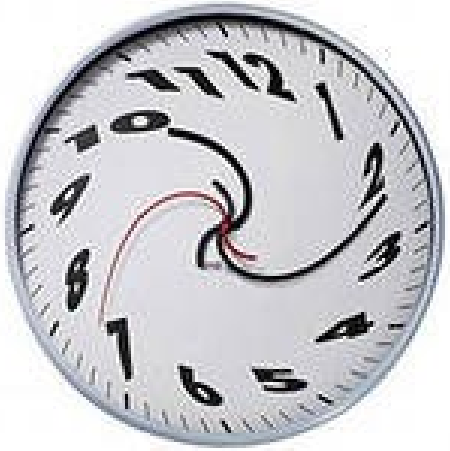
- Возможность компенсационных мер
- Маскирование
- Анонимизация
- Выбор и установка средств защиты
- Внедрение новых процессов



5. Готовка

(Приведение в соответствие)

- Разработка плана
- Определение ответственных
- Распределение работ
- Контроль выполнения
- Решение новых проблем (которые не были учтены)
- Консультирование
- Документация!!!



6. Время приготовления

(Срок прохождения аудита)

- Средний срок от 9 месяцев до 2 лет
- +30% времени лучше иметь в запасе
- Время = деньги
- Мы уложились в ~1 год от принятия решения (это только 1 этап)

7. Дегустация

(Сертификационный аудит)

- ASV сканирование
- Внутренний и внешний Pentest
- Проверка аудитором выполнения ВСЕХ требований

Спасибо за внимание!

ВОПРОСЫ