Международные и отраслевые стандарты

Payment Card Industry Data Security Standard

Илья Воложанин
Руководитель группы консалтинга

Проверка связи

Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти

Поставьте в чат:

\+ если меня видно и слышно

– если нет

Илья Воложанин

О спикере:

- руководитель группы консалтинга
- практикующий аудитор в области PCI DSS — 7 лет
- общий опыт в области информационной безопасности — 15 лет
- QSA, CISSP, CISA

Правила участия

1. Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
2. Продолжительность вебинара — 80 минут
3. Вы можете писать свои вопросы в чате
4. Запись вебинара будет доступна в LMS

Вспомним материалы лекции

1. Узнали назначение и область применения международного стандарта PCI DSS
2. Выяснили, на каких участников платёжного процесса с использованием платёжных карт распространяются требования PCI DSS
3. Узнали базовые принципы и методы определения области действия стандарта PCI DSS
4. Проанализировали 12 доменов требований стандарта PCI DSS (требуемые процессы, технологии и средства защиты информации)

Вспоминаем материалы лекций

Вопрос: кто может проводить сертификационный аудит по PCI DSS?

Варианты ответов:

1. Qualified Security Assessor (QSA)
2. Internal Security Assessor (ISA)
3. QSA или ISA

Вспоминаем материалы лекций

Вопрос: кто может проводить сертификационный аудит по PCI DSS?

Правильный ответ:

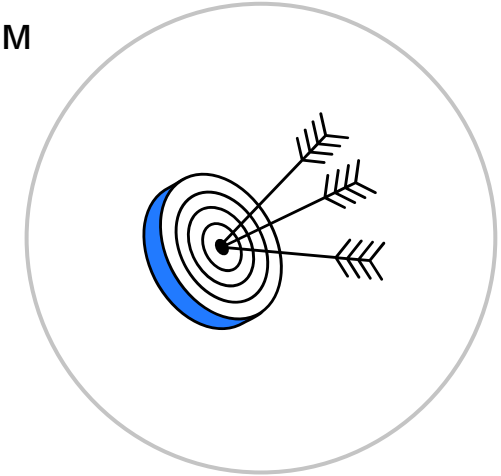
1. Qualified Security Assessor (QSA)
2. Internal Security Assessor (ISA)
3. Qualified Security Assessor (QSA) или Internal Security Assessor (ISA)

Зачем это специалисту по ИБ?

Ваши вопросы?

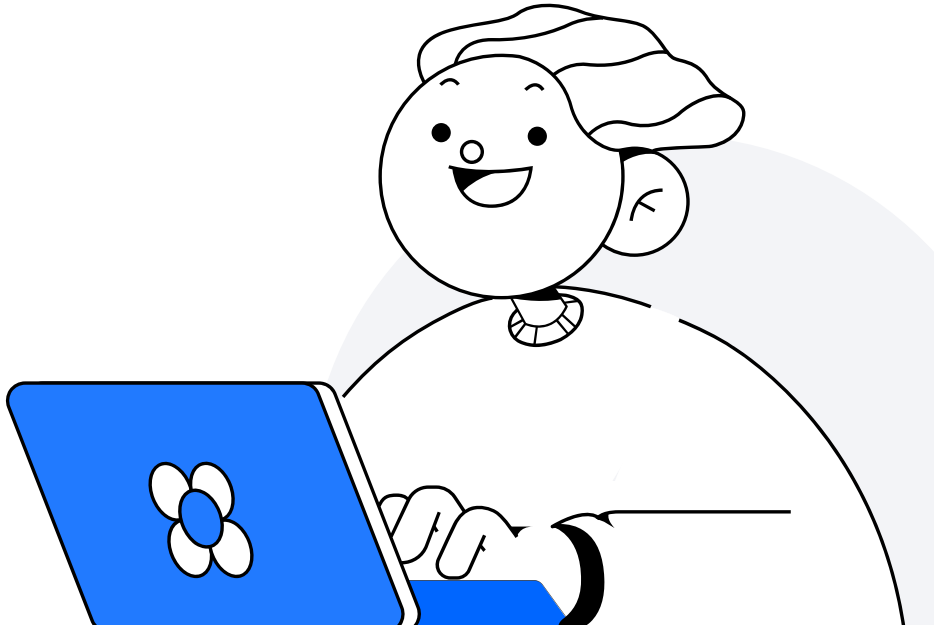
Цели занятия

- Узнать, что необходимо для того, чтобы стать сертифицированным аудитором по PCI DSS
- Разобрать, как проходит сертификационный аудит по PCI DSS
- Рассмотреть на практике, как аудитор определяет область действия стандарта PCI DSS
- Узнать, как заполняется отчёт о соответствии требованиям
- PCI DSS, и разобрать выборочные требования
- стандарта PCI DSS



План занятия

1. Требования к QSA
2. Этапы проведения сертификационного аудита
3. Практика проверки области действия стандарта PCI DSS
4. Анализ выборочных требований стандарта PCI DSS
5. Итоги
6. Домашнее задание



Требования к QSA

1

Вспоминаем материалы лекций

Вопрос: кто же такой QSA?

Варианты ответов:

1. Регулятор по стандарту PCI DSS
2. Внешний аудитор по стандарту PCI DSS
3. Внутренний аудитор по стандарту PCI DSS

Вспоминаем материалы лекций

Вопрос: кто же такой QSA?

Правильный ответ:

1. Регулятор по стандарту PCI DSS
2. Qualified Security Assessor. Внешний аудитор по требованиям стандарта PCI DSS
3. Внутренний аудитор по стандарту PCI DSS

Требования к QSA

1. Навыки и опыт работы по направлениям «аудит» и «обеспечение ИБ»
2. актуальные сертификации по направлениям «аудит» и «обеспечение ИБ»
3. Согласие с PCI SSC Code of Professional Responsibility
4. Знание стандарта PCI DSS
5. Ежегодная реквалификация
6. Быть сотрудником QSA-компании

Требования к QSA

Опыт работы по направлениям «обеспечение ИБ» и «аудит/оценка соответствия требованиям»

- Не менее одного года работы по каждому направлению обеспечения ИБ:
  - информационная безопасность приложений
  - информационная безопасность ИТ-инфраструктуры
  - сетевая безопасность
- Не менее одного года работы по каждому направлению аудита/оценки соответствия требованиям:
  - аудит информационной безопасности
  - оценка или управление рисками информационной безопасности

Требования к QSA

Сертификации для QSA

Направление Information Security

- (ISC)2 Certified Information System Security Professional (CISSP)
- ISACA Certified Information Security Manager (CISM)
- Certified ISO 27001 Lead Implementer
- (METI) Registered Information Security Specialist (RISS)

Направление Audit

- ISACA Certified Information Systems Auditor (CISA)
- GIAC Systems and Network Auditor (GSNA)
- Certified ISO 27001, Lead Auditor, Internal Auditor
- IRCA ISMS Auditor
- IIA Certified Internal Auditor (CIA)

Требования к QSA

PCI SSC Code of Professional Responsibility (код профессиональной этики)

Профессиональная компетентность:

- ответственность и честность при выполнении услуг
- действия в интересах клиентов, для которых выполняются услуги
- продвижение современных методов и стандартов информационной безопасности

Обеспечение безопасности, конфиденциальности и целостности защищаемых данных:

- уважение и защита конфиденциальной информации при оказании услуг
- уведомление о фактах компрометации систем или выявлении нарушений ИБ

Добросовестность:

- отказ от действий, которые могут нарушить репутацию PCI SSC
- отказ от действий, которые могут привести к конфликту интересов
- уведомление об этических нарушениях в PCI SSC

Соблюдение всех применимых законов, правил и отраслевых стандартов

Требования к QSA. Обучение и экзамен

Курс обучения стандарту состоит из двух частей:

1. PCI Fundamentals — онлайн, экзамен с 60 вопросами
2. QSA Qualification Course — онлайн/офлайн, экзамен с 75 вопросами

$3 000*
Стоимость обучения

→

По завершении — сертификат на 12 месяцев

→

По истечении срока сертификата — реквалификация

→

$1 800*
Стоимость реквалификации

* Стоимость указана на сентябрь 2022 г. и может меняться в зависимости от региона проведения обучения

Выводы

1. Стать QSA сложно
2. Стать QSA дорого
3. QSA — это не навсегда

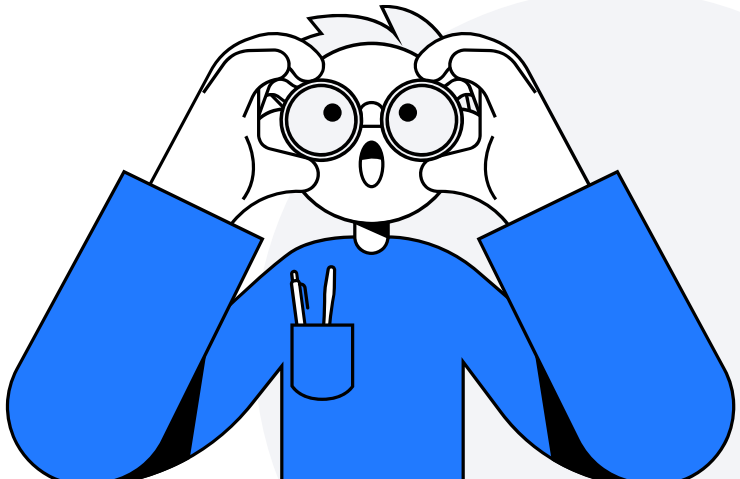
Ваши вопросы?

Этапы проведения сертификационного аудита

2

Итак, вы — QSA

- Как же проводить сертификационный аудит?
- Что надеть?
- Что говорить?
- Куда смотреть?



Таймлайн сертификационного аудита

1–2 дня → Подготовка к оценке

10–15 дней → Обследование и интервьюирование

10–15 дней Анализ свидетельств и отчётность

Подготовка к оценке (удалённо)

1. Анализ перечня компонентов ИТ-инфраструктуры в области действия PCI DSS
2. Анализ организационно-распорядительной документации
3. Подготовка выборки компонентов ИТ-инфраструктуры в области аудита PCI DSS
4. Планирование интервьюирования и обследования

Обследование и интервьюирование (в офисе заказчиков)

1. Проведение интервьюирования сотрудников заказчика
2. Обследование систем, средств защиты информации
3. Наблюдение за процессами обеспечения ИБ
4. Получение свидетельств реализации настроек и выполнения процессов, например:
   - конфигурации сетевого оборудования и межсетевых экранов
   - заявки на предоставление доступа
   - примеры журналов событий на уровне операционной системы
5. Проверка реализации компенсирующих мер*

* Понятие компенсирующей меры рассмотрим далее

Анализ свидетельств и отчётность (удалённо)

- Анализ полученных свидетельств
- Разработка отчётных документов
- Предоставление отчётных документов заказчику
- Передача аттестата о соответствии (Attestation of Compliance) платёжным системам

Payment Card Industry Data Security Standard

PCI DSS Certificate of Compliance

This is to certify that

SoftPos sp. z o.o.

has been assessed by SC2labs sp. z o.o. - official PCI QSA and PCI ASV company
and has been found to be compliant with PCI Data Security Standard v 3.2.1
as set out by the PCI Security Standard Council and endorsed by all leading card providers.

Company: SoftPos sp. z o.o.
ul. Okopowa 56/77
01-042 Warszawa
POLAND

Category: Service Provider, level 1

QSA Auditor: Grzegorz Kosmowski
PCI QSA #205-710

Date of issue: 19.02.2021

Renewal date: 18.02.2022

Signed: Grzegorz Kosmowski

www.sc2labs.com

Certificate of Compliance

[Источник]

Вспоминаем материалы лекций

Вопрос: а какой ещё отчётный документ (кроме аттестата о соответствии) является результатом сертификационного аудита по PCI DSS?

Вспоминаем материалы лекций

Вопрос: а какой ещё отчётный документ (кроме аттестата о соответствии) является результатом сертификационного аудита по PCI DSS?

Ответ: Report of Compliance (RoC), или отчёт о соответствии требованиям PCI DSS

Выводы

1. Проведение сертификационного аудита включает три основных этапа: подготовка к оценке, обследование и интервьюирование, анализ свидетельств и отчётность

2. Навыки, которые требуются QSA на практике:

- анализ большого объёма документации
- анализ конфигураций ИТ-инфраструктуры и средств защиты информации
- анализ схем сети передачи данных и потоков данных платёжных карт
- наблюдательность

Ваши вопросы?

Практика проверки области действия стандарта PCI DSS

3

Вспоминаем прошлое занятие

Вопрос: какие компоненты ИТ-инфраструктуры включаются в область действия PCI DSS?

Вспоминаем прошлое занятие

Вопрос: какие компоненты ИТ-инфраструктуры включаются в область действия PCI DSS?

Варианты ответов (множественный выбор):

1. Серверы баз данных, которые хранят данные платёжных карт
2. Сервер мониторинга доступности и нагрузки на серверы баз данных
3. Средство антивирусной защиты, не установленное на серверах баз данных, но установленное на рабочих станциях администраторов БД
4. Веб-сервер, не связанный с указанными выше системами и серверами, на котором размещён сайт организации

Вспоминаем прошлое занятие

Вопрос: какие компоненты ИТ-инфраструктуры включаются в область действия PCI DSS?

Правильный ответ:

1. Серверы баз данных, которые хранят данные платёжных карт
2. Сервер мониторинга доступности и нагрузки на серверы баз данных
3. Средство антивирусной защиты, не установленное на серверах баз данных, но установленное на рабочих станциях администраторов БД
4. Веб-сервер, не связанный с указанными выше системами и серверами, на котором размещён сайт организации

Вспоминаем материалы лекции

Область действия PCI DSS

1

Среда данных платёжных карт (CDE*)

Системные компоненты, хранящие, обрабатывающие или передающие ДПК

2

Подключённые системы

Системные компоненты, имеющие прямое или непрямое подключение к CDE

3

Компоненты, влияющие на безопасность CDE

Системные компоненты, влияющие на конфигурацию или безопасность CDE либо реализующие функции безопасности**

* CDE — cardholder data environment

** Также включают системные компоненты, которые обеспечивают сегментацию CDE и поддерживают выполнение требований PCI DSS

Вне области действия PCI DSS

1

Системные компоненты, не хранящие,
не обрабатывающие и не передающие ДПК

2

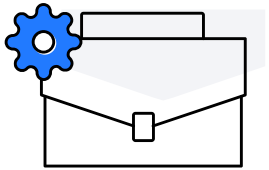
Системные компоненты, расположенные
не в том же сегменте сети или VLAN,
что и компоненты CDE

3

Системные компоненты, не имеющие
подключения к CDE

4

Системные компоненты, не влияющие
на безопасность CDE



Кейс

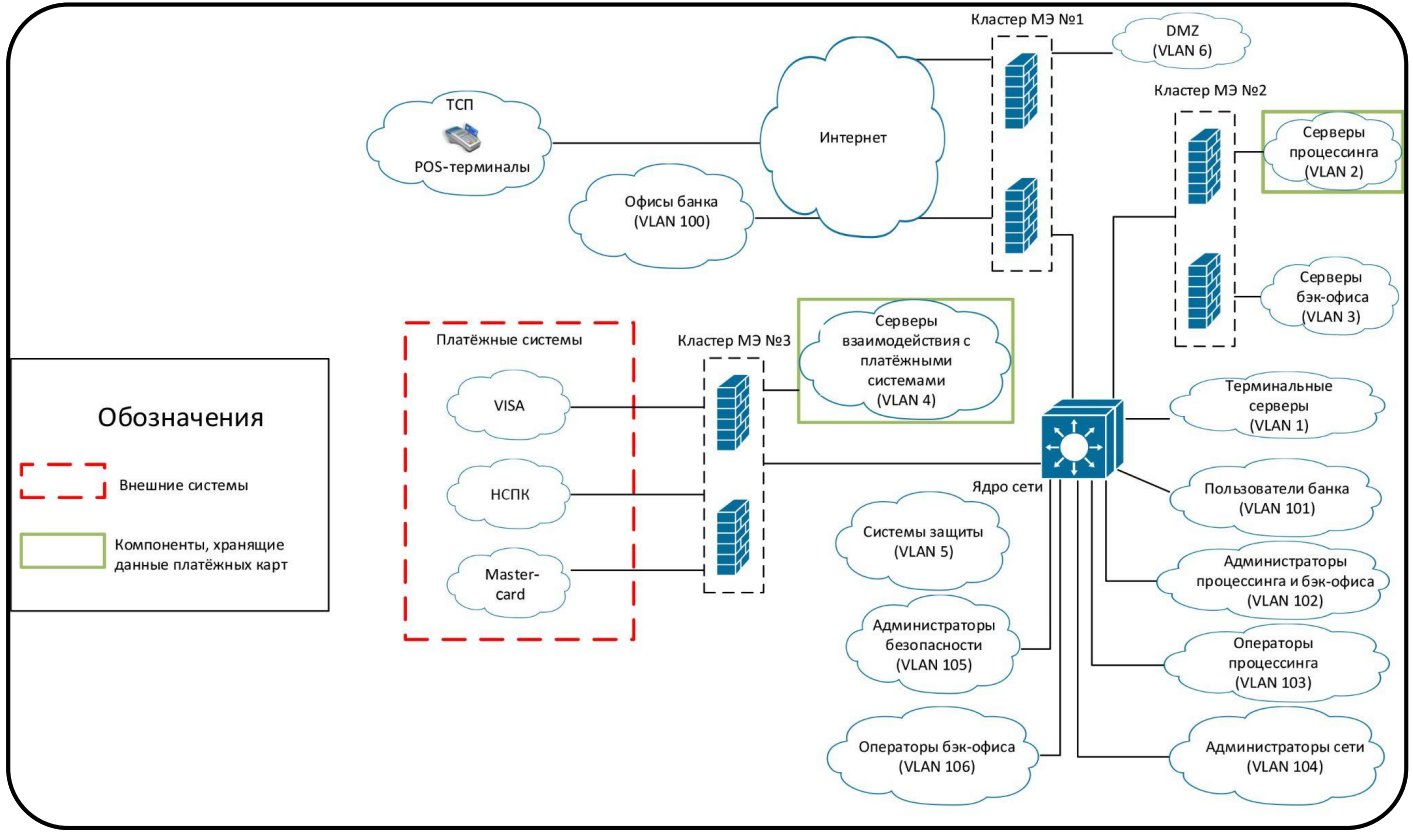
Аудит в банке по требованиям PCI DSS

Исходные данные

- Сертификационный аудит проводится в региональном банке, у которого:
  - есть сеть отделений по нескольким регионам (обслуживают только ТСП — торгово-сервисные предприятия)
  - есть сеть ТСП по нескольким регионам
  - нет ecommerce, ДБО (дистанционного банковского обслуживания), выпуска карт и банкоматов

- Для проведения этапа подготовки к оценке представитель банка прислал документы:
  - схему сети передачи данных банка
  - описание подсетей сети передачи данных банка (VLAN и их назначение)

Схема сети передачи данных банка



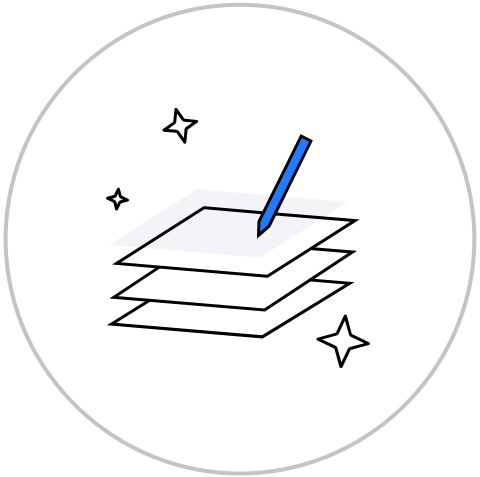
Описание подсетей сети передачи данных банка (VLAN и их назначение)

- VLAN 100 — офисы банка — не имеют доступа к CDE
- VLAN 101 — пользователи головного офиса банка — не имеют доступа к CDE
- VLAN 102 – администраторы процессинга и бэк-офиса – имеют доступ к приложению процессинга и бэк-офиса напрямую
- VLAN 103 — операторы процессинга — имеют доступ к приложению процессинга напрямую
- VLAN 104 — администраторы сети — имеют доступ только к сетевому оборудованию (МЭ и ядро сети)
- VLAN 105 — администраторы безопасности — не имеют доступа к системам в CDE, но имеют доступ к МЭ и средствам защиты (в том числе установленным в процессинге и бэк-офисе)
- VLAN 106 — операторы бэк-офиса — имеют доступ к приложению бэк-офиса
- VLAN 1 — терминальные серверы — используются пользователями головного офиса для доступа к приложениям
- VLAN 2 — серверы процессинга — обрабатывают транзакции от POS терминалов
- VLAN 3 — серверы бэк-офиса — взаимодействуют с серверами процессинга, но не хранят и не обрабатывают ДДК (данные держателей карт)
- VLAN 4 — серверы взаимодействия с платёжными системами — получают транзакции (содержащие ДДК) от процессинга и передают в платёжные системы
- VLAN 5 — системы защиты банка — используются в том числе и для защиты CDE
- VLAN 6 — DMZ сегмент — используется для доступа к сайту банка и CRM (не обрабатывают ДДК)

Задание 1

Напишите в чате номера подсетей (VLAN) компонентов ИТ-инфраструктуры, которые относятся к среде данных платёжных карт (CDE — cardholder data environment).

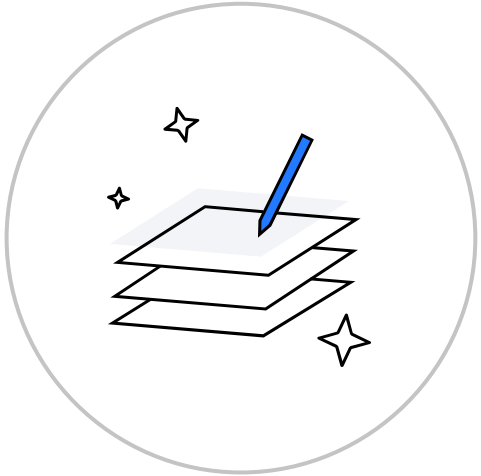
Ответ дайте в формате: **№ 1: VLAN 100 …**



Задание 2

Напишите в чате номера подсетей (VLAN) компонентов ИТ-инфраструктуры, которые попадают в область действия PCI DSS.

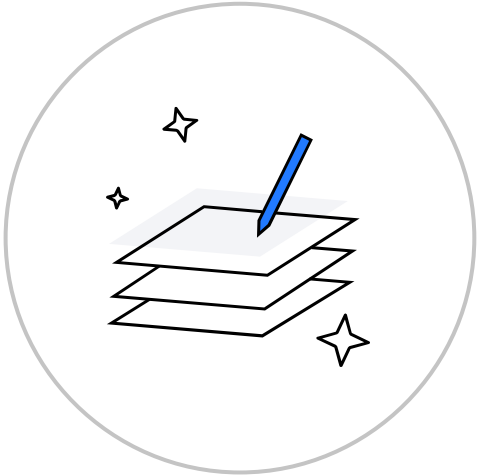
Ответ дайте в формате: **№ 2: VLAN 100 …, VLAN 100 …**



Задание 3

Напишите в чате, нужно ли проверять все три кластера межсетевых экранов или нет (например, используя принцип выборки компонентов в области аудита, проверить только один из них)

Ответ дайте в формате: **№ 3: да/нет**



Обсудим результаты

Задание 1

Номера подсетей (VLAN) компонентов ИТ-инфраструктуры, которые относятся к среде данных платежных карт (CDE - Cardholder Data Environment)

Правильный ответ: VLAN 2, 4, 102, 103

Задание 2

Номера подсетей (VLAN) компонентов ИТ-инфраструктуры, которые попадают в область действия PCI DSS

Правильный ответ: VLAN 102, 103, 104, 105, 2, 3, 4, 5

Задание 3

Нужно ли проверять все три кластера межсетевых экранов или нет?

(например, используя принцип выборки компонентов в области аудита проверить только один из них)

Правильный ответ: да

Ваши вопросы?

Перерыв

5 минут

Анализ выборочных требований стандарта PCI DSS

4

Вспоминаем материалы лекций

Вопрос: сколько всего доменов требований в стандарте PCI DSS?

Вспоминаем материалы лекций

Вопрос: сколько всего доменов требований в стандарте PCI DSS?

Ответ: 12

Из чего состоит Report of Compliance (отчёт о соответствии)

1. **Assessment Overview (обзор оценки)** — состоит из 6 разделов, содержащих область оценки, свидетельства и результаты оценки
2. **Findings and Observations (выводы и наблюдения)** — состоит из 12 разделов по 12 доменам требований PCI DSS
3. **Additional PCI DSS Requirements (дополнительные требования),** распространяющиеся на особые случаи
4. **Compensating Controls (компенсирующие меры)** — содержит описание компенсирующих мер и шаблон по их описанию
5. **Customized Approach (индивидуальный подход)** — содержит описание альтернативного подхода в реализации требований PCI DSS и шаблон по его описанию

Report of Compliance (RoC) заполняется QSA по шаблону, предоставляемому PCI SSC

RoC. Assessment Overview

Состоит из 6 разделов

1. Contact information and summary of results
2. Business overview
3. Description of scope of work and approach taken
4. Details about reviewed environments
5. Quarterly scan results
6. Evidence (assessment workpapers)

- Документация
- Интервью
- Наблюдения
- Конфигурации

RoC. Findings and Observations — 1.2.7

PCI DSS Requirement				
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.				
Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*			<Enter Response Here>	
Validation Method – Customized Approach				
Indicate whether a Customized Approach was used:			☐ Yes ☐ No	
If "Yes", Identify the aspect(s) of the requirement where the Customized Approach was used. ***Note:** The use of Customized Approach must also be documented in Appendix E.*			<Enter Response Here>	
Validation Method – Defined Approach				
Indicate whether a Compensating Control was used:			☐ Yes ☐ No	
If "Yes", Identify the aspect(s) of the requirement where the Compensating Control(s) was used. ***Note:** The use of Compensating Controls must also be documented in Appendix C.*			<Enter Response Here>	

RoC. Findings and Observations — 1.2.7

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.2.7.a Examine documentation to verify procedures are defined for reviewing configurations of NSCs at least once every six months.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	<Enter Response Here>
1.2.7.b Examine documentation of reviews of configurations for NSCs and interview responsible personnel to verify that reviews occur at least once every six months.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	<Enter Response Here>
	Identify the evidence reference number(s) from Section 6 for all **interview(s)** conducted for this testing procedure.	<Enter Response Here>
1.2.7.c Examine configurations for NSCs to verify that configurations identified as no longer being supported by a business justification are removed or updated.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	<Enter Response Here>

RoC. Findings and Observations — 6.3.3

PCI DSS Requirement
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).

Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*	<Enter Response Here>

Validation Method – Customized Approach	
Indicate whether a Customized Approach was used:	☐ Yes ☐ No
If "Yes", Identify the aspect(s) of the requirement where the Customized Approach was used. ***Note:** The use of Customized Approach must also be documented in Appendix E.*	<Enter Response Here>

Validation Method – Defined Approach	
Indicate whether a Compensating Control was used:	☐ Yes ☐ No
If "Yes", Identify the aspect(s) of the requirement where the Compensating Control(s) was used. ***Note:** The use of Compensating Controls must also be documented in Appendix C.*	<Enter Response Here>

RoC. Findings and Observations — 6.3.3

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.3.3.a Examine policies and procedures to verify processes are defined for addressing vulnerabilities by installing applicable security patches/updates in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	<Enter Response Here>
6.3.3.b Examine system components and related software and compare the list of installed security patches/updates to the most recent security patch/update information to verify vulnerabilities are addressed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system components and related software** examined for this testing procedure.	<Enter Response Here>

RoC. Additional PCI DSS Requirements (Приложение A)

Состоит из 3 разделов

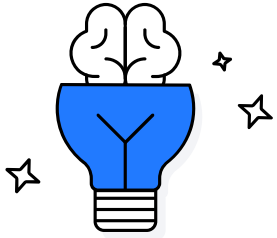
1. Appendix A1: Additional PCI DSS requirements for multi-tenant service providers*
2. Appendix A2: Additional PCI DSS requirements for entities using SSL/early TLS for card-present POS POI terminal connections
3. Appendix A3: Designated Entities Supplemental Validation (DESV)

Необходимость выполнения требований в Appendix A3 определяется или эквайером, или платежной системой

*** Multi-tenant service providers** — это тип стороннего поставщика услуг, у которого клиенты совместно используют системные ресурсы (например, физические или виртуальные серверы), инфраструктуру, приложения (SaaS) и/или базы данных

RoC. Compensating Controls

- Организация не может выполнить исходное требование PCI DSS (Defined Approach*)
- Реализуется, когда есть законодательные, технические ограничения или ограничения со стороны бизнеса
- Требует заполнения организацией шаблона компенсирующей меры и реализации данной меры
- Может использоваться только для Defined Approach*



Условия применения компенсирующих мер

*Понятие Defined Approach рассмотрим далее

RoC. Compensating Controls

Required Number and Definition: <Enter Response Here>

	Information Required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	<Enter Response Here>
2. Definition of Compensating Controls	Define the compensating controls, explain how they address the objectives of the original control and the increased risk, if any.	<Enter Response Here>
3. Objective	Define the objective of the original control (for example, the Customized Approach Objective).	<Enter Response Here>
	Identify the objective met by the compensating control (*note: this can be, but is not required to be, the stated Customized Approach Objective for the PCI DSS requirement*).	<Enter Response Here>
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	<Enter Response Here>
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	<Enter Response Here>
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	<Enter Response Here>

RoC. Customized Approach

В PCI DSS 4.0 есть два варианта реализации требований:

1. **Defined Approach**
   Исходное требование PCI DSS с определёнными PCI SCC процедурами проверки

2. **Customized Approach**
   Иной подход (защитная мера), не соответствующий формулировке исходного требования PCI DSS, но соответствующий её цели

RoC. Customized Approach

Не служит для:

- упрощения выполнения требования PCI DSS
- быстрого исправления несоответствия перед или в процессе аудита
- тех, кто проводит самооценку (заполняет SAQ)

! Не все требования стандарта PCI DSS можно реализовать в Customized Approach

! QSA, помогающий в разработке или документировании Customized Approach, не может выполнять сертификационный аудит в организации

Подумайте

Вопрос: можно ли использовать компенсирующую меру для Customized Approach?

Подумайте

Вопрос: можно ли использовать компенсирующую меру для Customized Approach?

Ответ: Нет — компенсирующая мера может использоваться только для Defined Approach

Выводы

1. Отчёт имеет структуру, определённую PCI SSC. Детализация свидетельств определяется аудитором, но должна быть достаточна для подтверждения выполнения требования

2. Для каждого требования определяется, что именно должен проверить аудитор:
   - наличие документации
   - наличие ответственных лиц и понимания выполняемых функций
   - наличие процесса и свидетельств его выполнения
   - наличие настроек в области действия PCI DSS

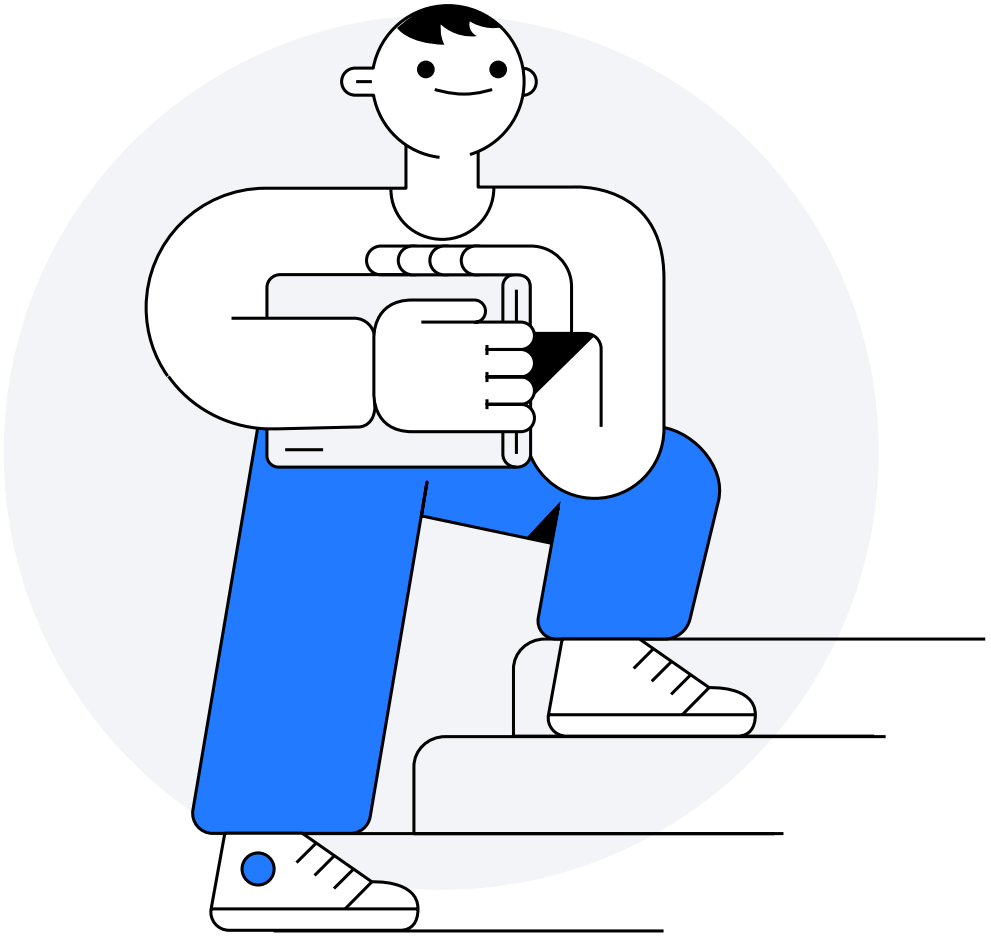
Ваши вопросы?

Итоги занятия

1. Узнали, что необходимо для того, чтобы стать сертифицированным аудитором по PCI DSS
2. Разобрались, как проходит сертификационный аудит по PCI DSS
3. Рассмотрели на практике, как аудитор определяет область действия стандарта PCI DSS
4. Узнали, как заполняется отчёт о соответствии требованиям PCI DSS и разобрали выборочные требования стандарта PCI DSS

Ваши вопросы?

Домашнее задание



Домашнее задание

Цель: проверить полученные знания по теме.

Формат выполнения: тест в LMS.

Результат: знание основных положений стандарта PCI DSS.

Описание: тест