

## Секция 6 Сертификационный QSA-аудит





Сертификационный QSA-аудит – это **внешняя независимая аудиторская проверка** соответствия организации требованиям стандарта PCI DSS, выполняемая QSA-аудиторами, сертифицированными Советом PCI SSC.

Являясь **наиболее серьезным вариантом подтверждения соответствия** организации требованиям стандарта PCI DSS, сертификационный QSA-аудит **дает наиболее объективные результаты** и пользуется **максимальным уровнем доверия** со стороны международных платежных систем, эквайеров и иных участников индустрии платежных карт.\*



\* - другими вариантами подтверждения соответствия стандарту PCI DSS являются заполнение листа самооценки (SAQ) и выполнение внутреннего ISA-аудита.



Вопрос	Да / Нет
<b>К сертификационному аудиту рекомендуется приступать, если дан ответ «Да» на все вопросы:</b>	
Выполнены ли все задачи, предусмотренные планом или рекомендациями по приведению организации в соответствие PCI DSS?	
Выполняются ли на практике все требования внутренних нормативных документов по информационной безопасности?	
Выполнено ли ASV-сканирование и тестирование на проникновение?	
Устранены ли уязвимости, если они были выявлены в ходе ASV-сканирования и тестирования на проникновение?	
Проведено ли повторное сканирование и тестирование после исправления, подтвердившее отсутствие критичных уязвимостей?	



Сертификационный QSA-аудит выполняется **при личном присутствии QSA-аудитора в офисе сертифицируемой компании**. Официальным статусом QSA должен обладать каждый аудитор, выполняющий проверки в процессе сертификационного QSA-аудита. Проверить действительный статус QSA-аудитора можно на официальном сайте Совета PCI SSC [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

В ходе аудита аудиторами выполняются следующие действия:

- Определение области аудита;
- Интервьюирование сотрудников;
- Изучение настроек конфигурации компонентов информационной инфраструктуры;
- Наблюдение за функционированием информационных систем;
- Изучение внутренних нормативных документов;
- Проверка наличия записей об исполнении регулярных процедур;
- Сбор свидетельств выполнения требований PCI DSS (копии документов и записей, снимки экрана, фотографии)\*.

\* - свидетельства сохраняются у QSA-компании в течение трех лет с момента аудита и могут быть в любой момент предоставлены Совету PCI SSC в рамках программы контроля качества услуг QSA.



Итог	Поставщик услуг (в т. ч. банк)	Торгово-сервисное предприятие
<p>Подтверждено 100% соответствие</p>	<p><b>QSA предоставляет заказчику:</b></p> <ul style="list-style-type: none"> <li>• Отчет о Соответствии (ROC);</li> <li>• Свидетельство о Соответствии (AOC);</li> <li>• Сертификат Соответствия.</li> </ul> <p><b>QSA предоставляет МПС:</b></p> <ul style="list-style-type: none"> <li>• Свидетельство о Соответствии;</li> <li>• Резюме Отчета о Соответствии;</li> <li>• Отчет о Соответствии (по запросу).</li> </ul>	<p><b>QSA предоставляет заказчику:</b></p> <ul style="list-style-type: none"> <li>• Отчет о Соответствии (ROC);</li> <li>• Свидетельство о Соответствии (AOC);</li> <li>• Сертификат Соответствия.</li> </ul> <p>Торгово-сервисное предприятие по запросу предоставляет Отчет о Соответствии своему банку-эквайеру.</p>
<p>Выявлены несоответствия</p>	<p><b>QSA предоставляет заказчику:</b></p> <ul style="list-style-type: none"> <li>• Отчет о соответствии (ROC)*.</li> </ul>	<p><b>QSA предоставляет заказчику:</b></p> <ul style="list-style-type: none"> <li>• Отчет о соответствии (ROC)*.</li> </ul>

\* - по желанию заказчика в случае несоответствия PCI DSS, QSA помогает заказчику заполнить форму отчетного документа «План действий по устранению несоответствий» для отправки его в МПС или банку-эквайеру.