deiteriy

Секция 6
Сертификационный QSA-аудит

 | 192236, Россия, Санкт-Петербург, ул. Софийская д. 8-1Б | +7 (812) 361-61-55 | www.deiteriy.com | info@deiteriy.com

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.*

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

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

Когда можно приступать к сертификационному QSA-аудиту?

Вопрос	Да / Нет
К сертификационному аудиту рекомендуется приступать, если дан ответ «Да» на все вопросы:	
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?	

Процедура сертификационного QSA-аудита

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.

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.

Результаты сертификационного QSA-аудита

Итог	Поставщик услуг (в т. ч. банк)	Торгово-сервисное предприятие
Подтверждено 100% соответствие	**QSA предоставляет заказчику:** • Отчет о Соответствии (ROC); • Свидетельство о Соответствии (AOC); • Сертификат Соответствия. **QSA предоставляет МПС:** • Свидетельство о Соответствии; • Резюме Отчета о Соответствии; • Отчет о Соответствии (по запросу).	**QSA предоставляет заказчику:** • Отчет о Соответствии (ROC); • Свидетельство о Соответствии (AOC); • Сертификат Соответствия. Торгово-сервисное предприятие по запросу предоставляет Отчет о Соответствии своему банку-эквайеру.
Выявлены несоответствия	**QSA предоставляет заказчику:** • Отчет о соответствии (ROC)*.	**QSA предоставляет заказчику:** • Отчет о соответствии (ROC)*.

* - 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.