Obowiązek zgodności ze standardem bezpieczeństwa PCI DSS

Od 1 stycznia 2013 roku wszyscy Akceptanci powinni być w pełni zgodni z wymogami standardu PCI DSS (wersja 2).

1. Kryteria określenia sposobów kontroli zgodności z PCI DSS

Grupa 1	**Metody weryfikacji zgodności z PCI DSS**
> roczna liczba transakcji powyżej 6 mln w systemie Visa lub MasterCard > inni Akceptanci o podwyższonym ryzyku wyznaczeni decyzją systemów płatniczych	> coroczny **Audyt PCI** > kwartalny **Zewnętrzny Skan Sieci**
Grupa 2	
> roczna liczba transakcji od 1 mln do 6 mln w systemie Visa lub MasterCard	> coroczna **Samoocena Zgodności PCI** lub coroczny **Audyt PCI** > kwartalny **Zewnętrzny Skan Sieci**
Grupa 3	
> roczna liczba transakcji eCommerce (handel elektroniczny) od 20 tys. do 1 mlnw systemie Visa lub MasterCard	> coroczna **Samoocena Zgodności PCI** > kwartalny **Zewnętrzny Skan Sieci**
Grupa 4	
> pozostali Akceptanci	> coroczna **Samoocena Zgodności PCI** (tylko na prośbę agenta rozliczeniowego) > kwartalny **Zewnętrzny Skan Sieci** (tylko na prośbę agenta rozliczeniowego)

2. Metody weryfikacji zgodności z PCI DSS, o których mowa powyżej:

> Audyt PCI – Audyt zgodności z PCI przeprowadzony przez zewnętrznego Certyfikowanego Audytora Bezpieczeństwa (ang. QSA – Qualified Security Agent).

> Lista firm oferujących usługi QSA w Polsce dostępna jest na stronie PCI DSS: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors.

3. Zewnętrzny Skan Sieci

> Zewnętrzny Skan Sieci wykonywany jest przez firmy wyznaczone przez PCI DSS. Lista takich firm (ang. ASV – Approved Scannign Vendors) dostępna jest na stronie PCI DSS: https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

4. Samoocena Zgodności PCI

Samoocena Zgodności PCI (ang. SAQ – Self-Assessment Questionnaire) jest dokumentowana w kwestionariuszu samooceny SAQ.
Rodzaj wypełnianego kwestionariusza SAQ zależy do rozwiązań technologicznych stosowanych przez Akceptanta:

Opis rozwiązań technologicznych stosowanych przez Akceptanta	**Typ kwestionariusza samooceny SAQ**
Akceptant, który przeprowadza transakcje bez fizycznej obecności karty płatniczej (eCommerce lub MO/TO) i który w całości przetwarzanie danych kart płatniczych powierza zewnętrznemu dostawcy usług posiadającemu certyfikat PCI DSS, przy czym Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej, nie przesyła ani nie przetwarza ich w swoich systemach informatycznych lub na swoim terenie (nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności w obecności posiadacza karty)	**A**
Akceptant przyjmujący transakcje za pośrednictwem Internetu (eCommerce), który w całości przetwarzanie danych kart płatniczych powierza zewnętrznemu dostawcy usług posiadającemu certyfikat PCI DSS, przy czym Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej, nie przesyła ani nie przetwarza ich w swoich systemach informatycznych lub na swoim terenie oraz nie pobiera danych kart płatniczych za pośrednictwem swojej strony internetowej, jednak stopień zabezpieczenia tej strony może mieć wpływ na bezpieczeństwo transakcji dokonywanych kartą płatniczą (stosuje się wyłącznie do przypadków, gdy Akceptant przyjmuje płatności za pośrednictwem Internetu)	**A-EP**
Akceptant korzystający wyłącznie z: • z urządzeń typu Imprinter i/lub • z wolnostojących terminali łączących się za pośrednictwem telefonii stacjonarnej, przy czym Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej (nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności za pośrednictwem Internetu)	**B**

Akceptant korzystający wyłącznie z wolnostojących terminali posiadających certyfikat PCI-PTS łączących się z użyciem protokołu IP, bez przechowywania danych kart płatniczych w formie elektronicznej (nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności za pośrednictwem Internetu)	**B-IP**
Akceptant, który wprowadza transakcje ręcznie do wirtualnego terminala udostępnianego przez Internet i zarządzanego przez zewnętrznego dostawcę usług, posiadającego certyfikat PCI DSS. Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej (nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności za pośrednictwem Internetu)	**C-VT**
Akceptant, który wykorzystuje aplikację płatniczą opartą na systemie informatycznym podłączonym do Internetu. Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej (nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności za pośrednictwem Internetu)	**C**
Akceptant korzystający wyłącznie z wolnostojących terminali wykorzystujących i zarządzanych przez zaakceptowane przez PCI SSC rozwiązanie P2PE Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej (nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności za pośrednictwem Internetu)	**P2PE**
Wszyscy pozostali Akceptanci, nie zakwalifikowani do kategorii wymienionej powyżej	**D**

- Kwestionariusze SAQ dostępne są na stronie: https://www.pcisecuritystandards.org/document_library?category=saqs#results
- Akceptanci z Grupy 3 i Grupy 4 mogą wypełnić formularz SAQ samodzielnie.
- Akceptanci z Grupy 2 muszą wypełnić formularz SAQ przy pomocy QSA lub swojego pracownika, który uzyskał tytuł ISA (Internal Security Assessor). Sposób uzyskiwania kwalifikacji ISA jest opisany na stronie PCI DSS: https://www.pcisecuritystandards.org/program_training_and_qualification/internal_security_assessor_certification.

5. Niezbędne informacje dotyczące PCI DSS

- PCI DSS – Wymagania – Dokument do pobrania w aktualnej wersji standardu: https://www.pcisecuritystandards.org/document_library

- PCI DSS – materiały edukacyjne dla Merchantów i Service Providerów: https://www.pcisecuritystandards.org/pci_security/educational_resources

- PCI DSS – formularze SAQ oraz Przewodnik do ich wypełnienia: https://www.pcisecuritystandards.org/document_library?category=saqs#results

- PCI DSS – lista kwalifikowanych audytorów: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

- PCI DSS – lista kwalifikowanych firm prowadzących skanowanie sieci: https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

- Stron główna PCI Council (PCI SSC): https://www.pcisecuritystandards.org/index.php