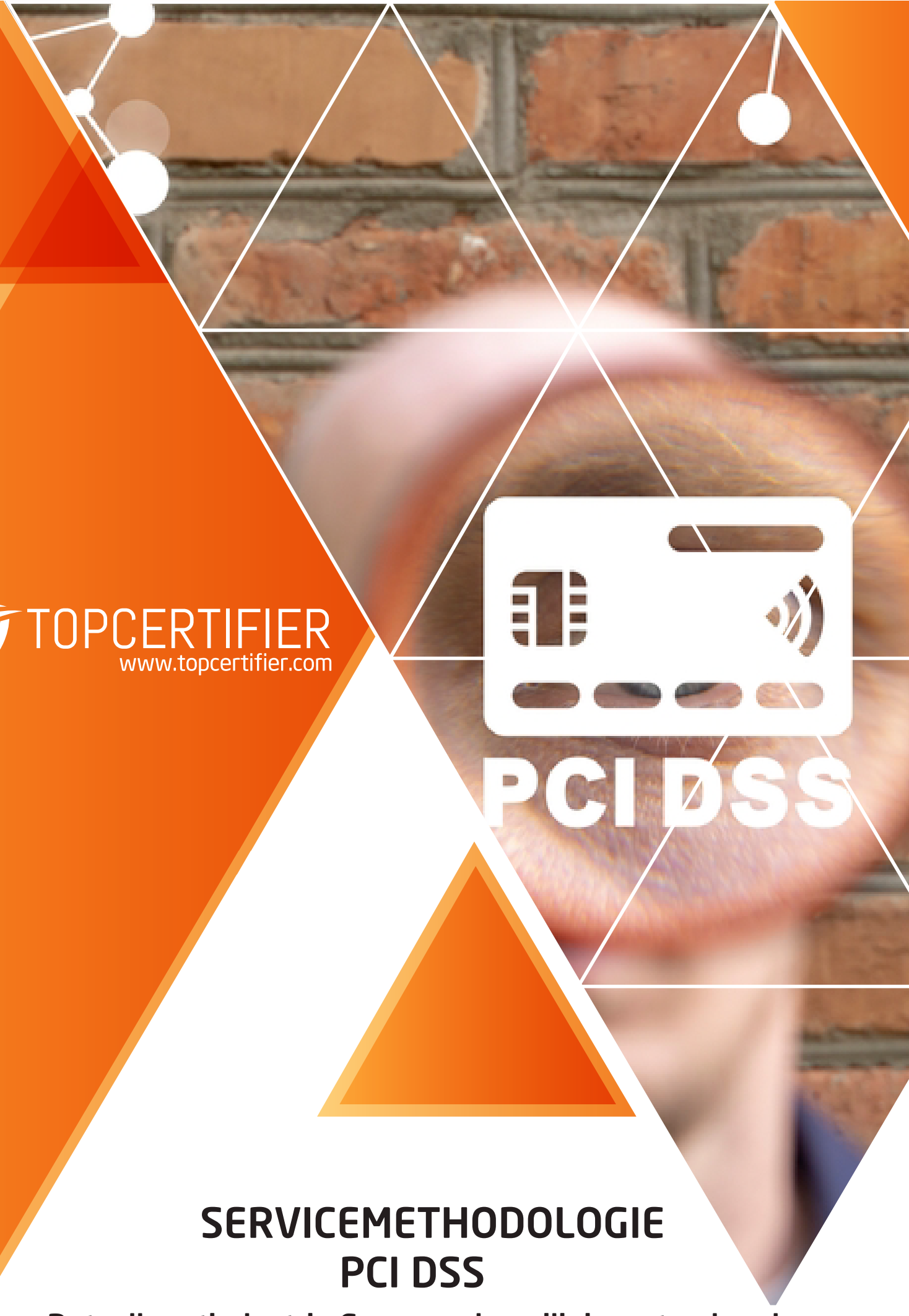
TOPCERTIFIER
www.topcertifier.com



SERVICEMETHODOLOGIE PCI DSS

Betaalkaartindustrie Gegevensbeveiligingsstandaard.

INLEIDING PCI DSS

TOPCertifier presenteert een vereenvoudigde PCI DSS Gap Analysis-checklist om u te helpen identificeren gebieden waar uw organisatie mogelijk verbeteringen nodig heeft om te voldoen aan PCI DSS (Payment Card Industry Data Security Standard) vereisten. Deze checklist biedt een basis raamwerk voor het evalueren van uw aansluiting bij PCI DSS en dient als een eerste stap hierin het beoordelen van uw naleving.

DEEL 1: GEGEVENSBEVEILIGING

- zijn betaalkaartgegevens correct gecodeerd tijdens verzending en opslag
- Worden gevoelige authenticatiegegevens, zoals CVV-nummers, na autorisatie niet opgeslagen
- Is er een beleid voor het beveiligen van kaarthoudergegevens en gevoelige authenticatiegegevens

DEEL 2: NETWERK- EN FIREWALLBEVEILIGING

- Worden netwerkconfiguraties en firewallregels regelmatig herzien en bijgewerkt
- Is er een netwerkdiagram dat de stroom van kaarthoudergegevens illustreert?
- Zijn er beveiligingsbeleid en -procedures aanwezig voor het beveiligen van de netwerkinfrastructuur

DEEL 3: TOEGANGSCONTROLE

- Zijn de toegangsrechten van gebruikers beperkt op basis van zakelijke 'need-to-know'
- is multi-factor authenticatie geïmplementeerd voor externe toegang tot het netwerk
- Worden gebruikersaccounts onmiddellijk gedeactiveerd bij beëindiging of rolwijzigingen

DEEL 4: BEHEER VAN KWETSBAARHEID

- Worden beveiligingspatches snel toegepast om kwetsbaarheden aan te pakken
- Is er een proces voor het scannen op kwetsbaarheden en het testen van penetratie
- Worden kritieke beveiligingspatches beoordeeld en geprioriteerd op basis van risico's

DEEL 5: VEILIGHEIDSBELEID EN PROCEDURES

- Zijn alomvattend beveiligingsbeleid en -procedures gedocumenteerd en verspreid
- bestaat er een security awareness trainingsprogramma voor medewerkers
- Wordt het beveiligingsbeleid herzien en indien nodig bijgewerkt

DEEL 6: MONITORING EN LOGGING

- Worden beveiligingsgebeurtenissen en logboeken regelmatig beoordeeld en gecontroleerd
- Is er een proces voor het uitvoeren van realtime waarschuwingen voor verdachte activiteiten
- Zijn er procedures voor respons op incidenten en rapportageprocedures vastgesteld?

SECTIE 7: REACTIE OP INCIDENT

- Is er een incidentresponsplan waarin de stappen worden beschreven voor het aanpakken van beveiligingsincidenten
- Zijn medewerkers getraind in het herkennen en melden van beveiligingsincidenten
- Is er een gedocumenteerd proces voor analyse en verbetering na een incident

SECTIE 8: FYSIEKE VEILIGHEID

- Zijn er fysieke toegangscontroles aanwezig om ongeautoriseerde toegang tot kaarthoudergegevens te voorkomen
- is de toegang tot beveiligde gebieden beperkt en bewaakt
- Are video surveillance and visitor logs maintained for sensitive areas

SECTIE 9: DERDE DIENSTVERLENERS

- Worden externe leveranciers beoordeeld op PCI DSS-naleving
- Zijn er schriftelijke overeenkomsten met dienstverleners om de bescherming van de gegevens van kaarthouders te garanderen
- Bestaat er een proces voor het monitoren en evalueren van beveiligingspraktijken van derden

Houd er rekening mee dat deze checklist een overzicht op hoog niveau biedt en dat het essentieel is om: grondige analyse specifiek voor de processen en context van uw organisatie. Bovendien is het aanbevolen om samen te werken met PCI DSS-experts of consultants om een alomvattend onderzoek uit te voeren gap-analyse voor uw organisatie