> Top 10 keys to PCI DSS success

THALES

www.thalesesecurity.com

UNDERSTAND WHAT YOU NEED TO DO

1. ANALYZE DATA FLOWS

Review and document in detail all processes involving capture, authorization and settlement of payment transactions where cardholder data is present to understand the components of your cardholder data environment (CDE). Ensure you identify all trusted, untrusted, and third-party connections and any mechanisms deployed to prevent unauthorized access to the CDE.

Establish where cardholder data is present and how you are protecting it on its journey

2. IDENTIFY CARDHOLDER DATA STORAGE

Document precisely what elements of cardholder data you are storing, all locations where it is stored and why your organization needs to store it. Recording how you have rendered the data unreadable and how access is logged are of critical importance. Knowing how long you need to retain the data and when you can securely delete it should involve business, legal and regulatory considerations in addition to the PCI DSS requirements.

Know where your stored data is located and how you rendered it unreadable

3. UNDERSTAND AND DOCUMENT SCOPE

The scope of assessment will always include those systems which process, transmit, and/or store cardholder data. It is also imperative to identify those systems which share a network segment with them, connect to them, or provide shared services to your CDE to avoid any issues or surprises that may affect your compliance.

Determine which components, software or connections impact the security of your CDE

MANAGE YOUR PROGRAM EFFECTIVELY

4. KNOW YOUR REPORTING REQUIREMENTS

PCI DSS compliance and reporting requirements are enforced by the payment brands. The various reporting category levels depend on your role and annual transaction volume. Ensure you review carefully all applicable reporting requirements to be absolutely certain of what is expected. An effective approach may involve verifying your assumptions with your acquiring bank, processor, and/or payment brand contact as appropriate.

Consult with your reporting contacts to ensure you get it right

5. DOCUMENT EVERYTHING

Organizational policies and procedures which are tightly aligned with the various PCI DSS requirements and sub-requirements are critical pieces of your compliance effort and require explicit documentation. It is also essential to remember to document other important activities including change management efforts, code reviews, security awareness programs, training sessions, and program authorizations to reflect your overall approach to security.

Use comprehensive documentation to support your compliance policies

6. CONSIDER BUSINESS REQUIREMENTS AND RISK

Practical application of the PCI DSS requirements means considering intent as well as business needs and assessed risk. Your efforts should include reviewing PCI DSS guidance, reading PCI Security Standards Council publications, and consulting with your QSAs to better understand how to reasonably apply required controls without harming defined business requirements.

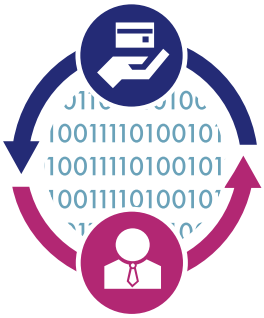
Ensure PCI DSS compliance complements your enterprise risk management efforts

7. CORRECT DEFICIENCIES

Throughout the assessment process and ensuing compliance management efforts, tracking deficiencies and remediation efforts through the use of a consolidated tracking mechanism can help to prioritize resources and make reporting status much easier. You may have a lot of items that you cannot fix immediately and understanding the overall assessment state of your environment may help you plan your activities more effectively.

Acknowledge and record all deficiencies while you focus diligently to mitigate them

ALIGN COMPLIANCE EFFORTS WITH BUSINESS GOALS



8. THINK CAREFULLY ABOUT COMPENSATING CONTROLS

Sometimes, business and/or technical constraints can prevent you from complying with one or more PCI DSS requirements. In these instances, compensating controls, which meet the intent and rigor of the affected requirement and go above and beyond other requirements can be deployed. However, the complexity of using compensating controls can prove daunting, often making it easier to comply with the affected requirement(s) as written.

Leverage existing cybersecurity strengths to reduce your need for compensating controls

9. REVIEW YOUR PROGRAM STRATEGY REGULARLY

Achieving and maintaining PCI DSS compliance can prove challenging. Establishing a defined program including documented roles and responsibilities can help to ensure that your CDE and supporting processes remain compliant. Manage your compliance efforts by establishing ongoing processes, regular team communications and staying abreast of developments within the industry.

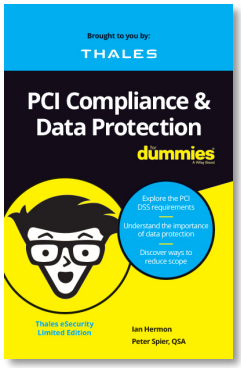
Promote greater team involvement in PCI SSC activities to expand your knowledge base

10. GET MANAGEMENT SUPPORT

Identifying program sponsors and stakeholders and ensuring their involvement and awareness can help to align your program with enterprise business goals and intra-organizational initiatives, and make you better prepared for changes in the threat environment.

Seek senior level buy-in to underpin your critical time and resource investments

For more detailed information please request a copy of our latest book, **PCI Compliance & Data Protection for Dummies**.



FORTREX TECHNOLOGIES

Follow us on:

Americas – 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101-03, 41/F., Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com