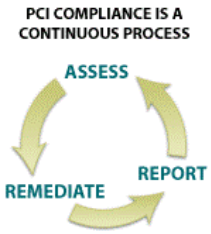
PCI DSS Security Regulations

Does your company process cardholder data?
Find Out What Your Organization Has to Do to Comply with PCI DSS Security Regulations!
The PCI Security Standards Council is an international organization that established the Payment Card Industry standards for securing cardholder data around the world.
The PCI Security Standards Council's mission is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

URS will assist the credit card company with PCI regulations. URS would start the PCI project with our Foundation Program, components including the cyber risk portal, compliance LMS training, plans & policies co-developed by URS & Mullen Coughlin plus compliance task monitoring and tracking, quarterly webinars, and a professional cyber insurance review. After this first phase is completed, URS will meet and determine next steps specifically speaking to the PCI regulation as described below.

The PCI 3-Step Process



- Assess. Identifying cardholder data, taking an inventory of IT assets and business processes for payment card processing, and analyzing them for vulnerabilities.
- Remediate. Fixing vulnerabilities and eliminating the storage of cardholder data unless absolutely necessary.
- Report. Compiling and submitting required reports to the appropriate acquiring bank and card brands.

The PCI Compliance Procedures

A. Card Brands

Specific questions about compliance validation levels and what you must do to validate should be directed to your acquiring financial institution or payment card brand.

- American Express
- Discover
- JCB International
- Mastercard
- UnionPay
- Visa / Visa Europe

B. PCI Data Security Standard Scooping

Implementing the PCI Data Security Standard starts with scoping. This process involves identifying all system components that are located within or connected to the cardholder data environment (such an environment is comprised of people, processes, and technology that handle cardholder data or sensitive authentication data). Scoping is an annual process and must occur prior to the annual assessment. Merchants and other entities must identify all locations and flows of cardholder data to ensure all applicable system components are included in scope for the PCI Data Security Standard.

C. Assessment

A Qualified Security Assessor is a data security firm that is qualified by the PCI Council to perform on-site PCI Data Security Standard assessments.

The Assessor will:

- Verify all technical information given by merchant or service provider
- Use independent judgment to confirm the standard has been met
- Provide support and guidance during the compliance process
- Be onsite for the duration of the assessment as required
- Adhere to the PCI Data Security Standard Assessment Procedures
- Validate the scope of the assessment
- Evaluate compensating controls
- Produce the final Report on Compliance

D. Reporting

Reports are the official method by which merchants and other entities report their compliance status with the PCI Data Security Standard to their respective acquiring financial institutions or payment card brand.

Quarterly submission of a report for network scanning may also be required. Individual payment card brands may require submission of other documentation; see their web sites for more information.

Depending on payment card brand requirements, merchants and service providers may need to submit a Self-Assessment Questionnaire for self-assessments, or a Report on Compliance for on-site assessments.

4 Levels of PCI

LEVEL 1

Merchants that handle:

- 6 million+ Visa, Mastercard, or Discover transactions per year
- 2.5 million+ American Express transactions per year
- 1 million+ JCB transactions per year

Merchants that have suffered a data breach or cyberattack resulting in compromised cardholder data or that have been identified by a card issuer as Level 1

REQUIREMENTS

- Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA)
- Quarterly network scan by an Approved Scan Vendor (ASV)
- Attestation of Compliance Form

LEVEL 2

Merchants that handle:

- 1-6 million Visa, Mastercard, or Discover transactions per year
- 50,000 to 2.5 million American Express transactions per year
- less than 1 million JCB transactions per year

REQUIREMENTS

- Annual Self-Assessment Questionnaire (SAQ)
- Quarterly network scan by an Approved Scan Vendor (ASV)
- Attestation of Compliance Form

LEVEL 3

Merchants that handle:

- 20,000 – 1 million Visa e-commerce transactions per year
- 20,000+ Mastercard e-commerce transactions per year,
  and up to to 1 million total Mastercard transactions per year
- 20,000 – 1 million Discover card-not-present transactions per year
- less than 50,000 American Express transactions

REQUIREMENTS

- Annual Self-Assessment Questionnaire (SAQ)
- Quarterly network scan by an Approved Scan Vendor (ASV)
- Attestation of Compliance Form

LEVEL 4

Merchants that handle:

- less than 20,000 Visa or Mastercard e-commerce transactions per year
- up to 1 million Visa or Mastercard transactions per year

REQUIREMENTS

- Established by the merchant's acquiring bank
- Usually include an SAQ and Quarterly Network Scan