nuvei

Payment Technology Network

PCI

Corporate Sales Training

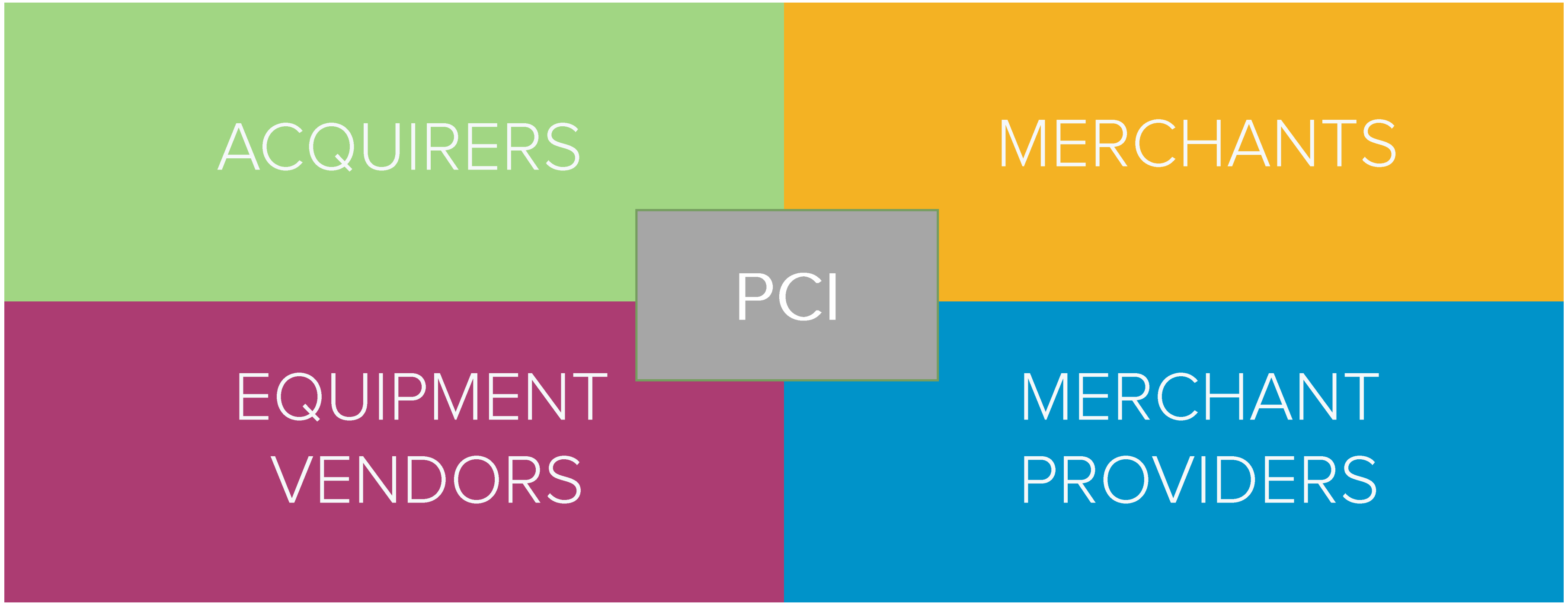
Agenda

- Introduction to PCI
- Levels of PCI
- 12 Requirements of PCI
- Validation (Conformance Technologies)

PCI

PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data.

The standards globally govern all merchants and organizations that store, process or transmit this data, and include specific requirements for software developers and manufacturers of applications and devices used in the transaction process.



ACQUIRERS

MERCHANTS

PCI

EQUIPMENT VENDORS

MERCHANT PROVIDERS

Compliance with the PCI security standards is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI

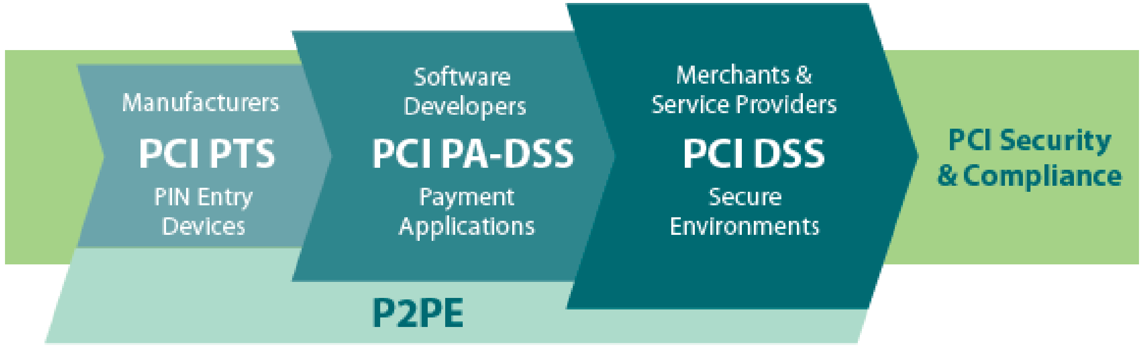
PCI Data Security Standard: The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If your business accepts or processes payment cards, it must comply with the PCI DSS.

Payment Application Data Security Standard: The PA-DSS is for software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement. It governs these applications that are sold, distributed or licensed to third parties.

PIN Transaction Security Requirements: The PCI PTS applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions.

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



Manufacturers

PCI PTS

PIN Entry Devices

Software Developers

PCI PA-DSS

Payment Applications

Merchants & Service Providers

PCI DSS

Secure Environments

PCI Security & Compliance

P2PE

Ecosystem of payment devices, applications, infrastructure and users

LEVELS OF PCI

Levels of PCI Compliance for Merchants

Level 1

"Big box" stores and major corporations

Minimum of 6 million transactions per year. Required to complete:

Annual internal audit conducted by a qualified PCI auditor

Quarterly PCI scans administered by an approved scanning vendor.

Level 2

Large businesses

Conduct between 1 million and 6 million transactions yearly. Required to complete:

Annual risk assessment using the appropriate SAQ.

Quarterly PCI scans, administered by an approved scanning vendor, may also be required.

Level 3

Mid-sized companies

Between 20,000 and 1 million transactions annually. Required to complete:

Annual risk assessment using the appropriate SAQ.

Quarterly PCI scans, administered by an approved scanning vendor, may also be required.

Level 4

Small businesses

Process less than 20,000 e-commerce transactions and less than 1 million other transactions annually. Required to complete:

Annual risk assessment using the appropriate PCI Self-Assessment Questionnaire (SAQ)

Quarterly PCI scans, administered by an approved scanning vendor, may also be required.

LEVELS OF PCI

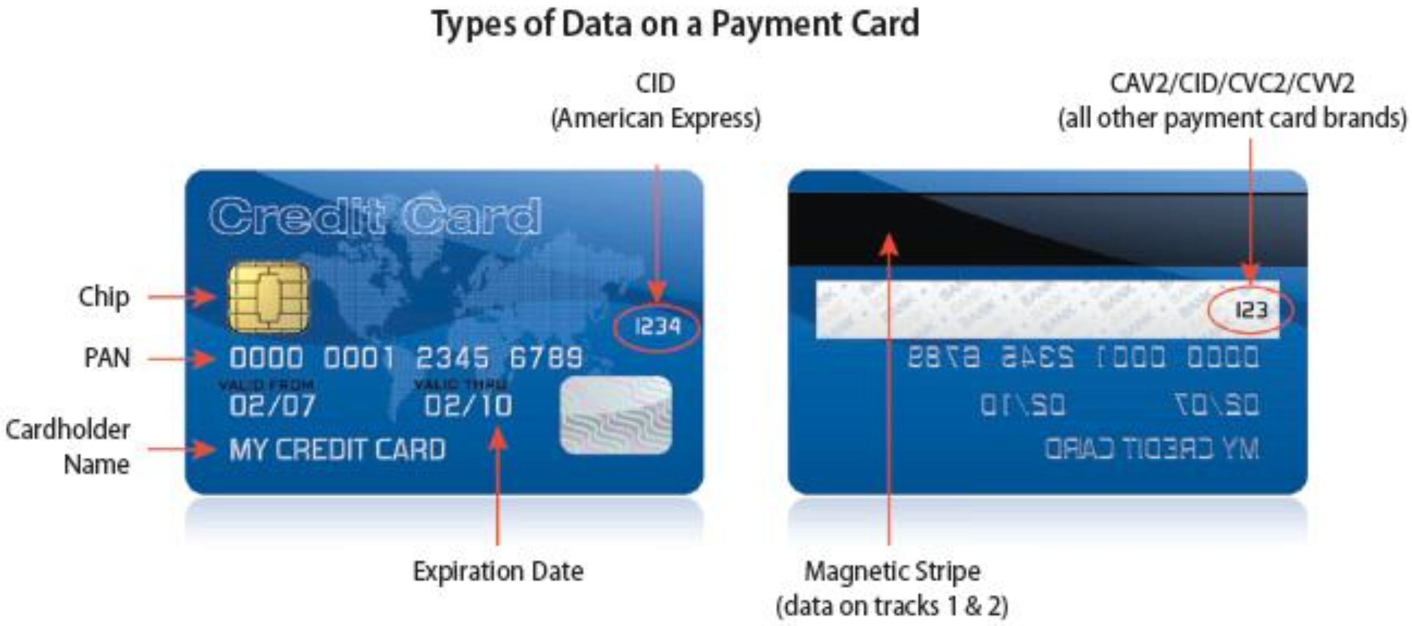
RISKY BEHAVIOR

A survey of businesses in the U.S. and Europe reveals activities that may put cardholder data at risk.

- 81% store payment card numbers
- 73% store payment card expiration dates
- 71% store payment card verification codes
- 57% store customer data on the payment card magnetic strip
- 16% store other personal data

Source: Forrester Consulting: The State of PCI

PCI

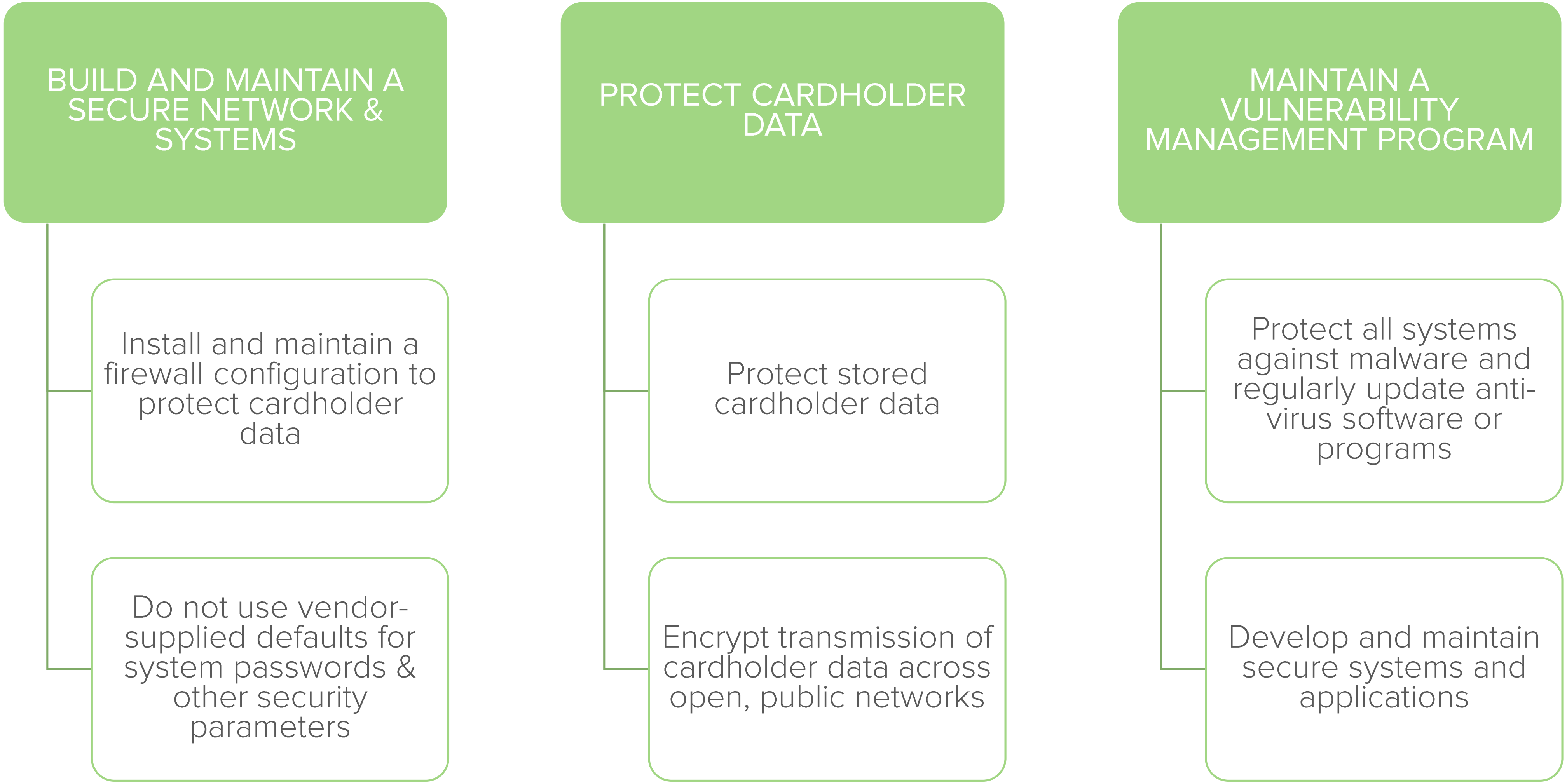


Businesses must physically secure or restrict access to printouts of cardholder data, to media where it is stored, and devices used for accessing or storing cardholder data. It's important to understand that PCI is about protecting both electronic data and paper receipts as well. (www.pcisecuritystandards.org)

The goal of the PCI DSS (PCI Data Security Standard) is to protect cardholder data and sensitive authentication data wherever it is processed, stored or transmitted.

nuvei
Payment Technology Network

12 REQUIREMENTS OF PCI



BUILD AND MAINTAIN A SECURE NETWORK & SYSTEMS

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords & other security parameters

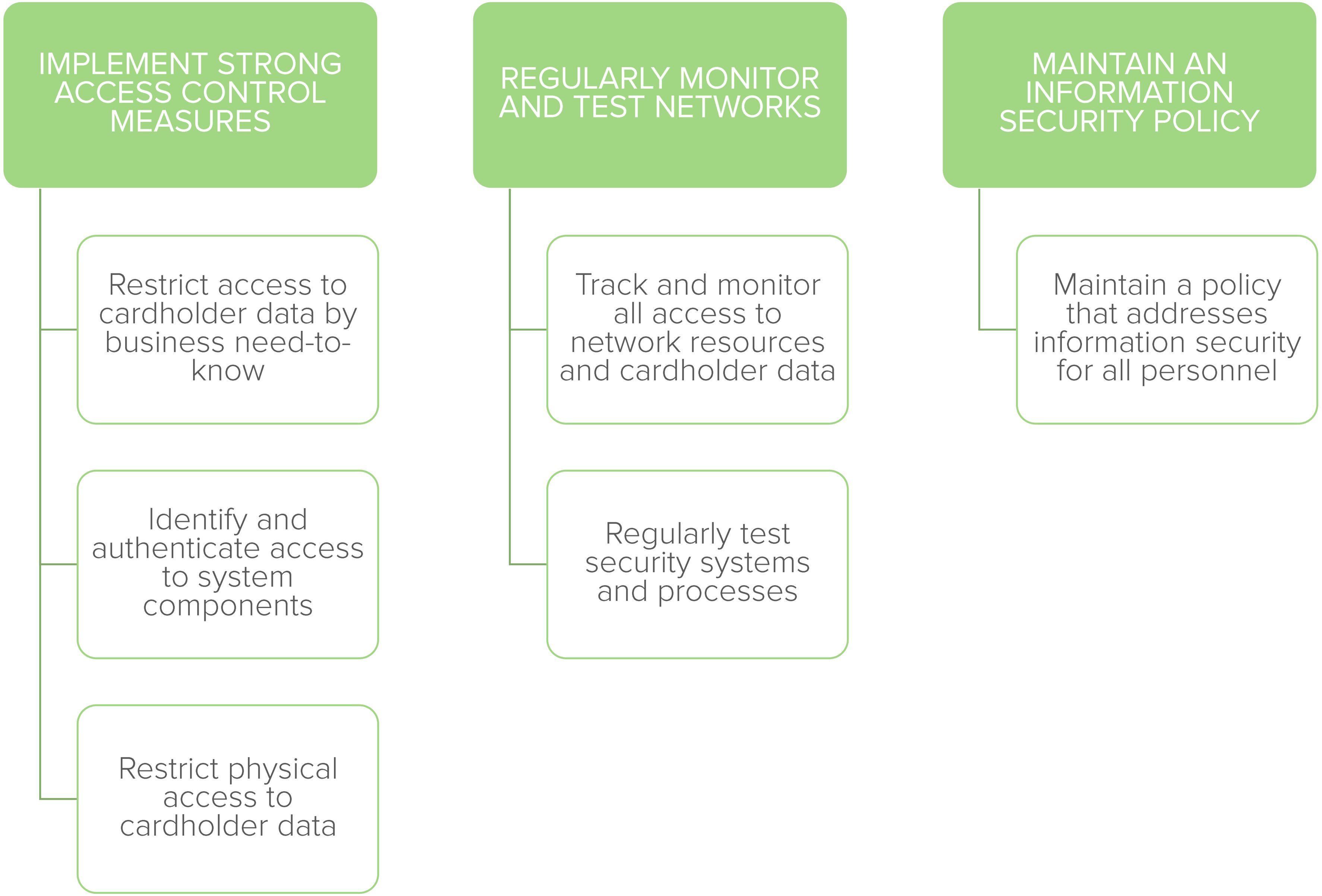
PROTECT CARDHOLDER DATA

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

- Protect all systems against malware and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

12 REQUIREMENTS OF PCI



IMPLEMENT STRONG ACCESS CONTROL MEASURES

- Restrict access to cardholder data by business need-to-know
- Identify and authenticate access to system components
- Restrict physical access to cardholder data

REGULARLY MONITOR AND TEST NETWORKS

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

MAINTAIN AN INFORMATION SECURITY POLICY

- Maintain a policy that addresses information security for all personnel

PCI – CONFORMANCE TECHNOLOGIES

The Nuvei PCI program is offered in partnership with Conformance Technologies.

Conformance Technologies offers the best in class virtual private Cloud solutions for the payment industry.

In addition to their ability to heighten compliance levels with minimum interruption, their PCI Compliance Suite is easy to use and offers excellent self-service tools.

Additional benefits of Nuvei's partnership with Conformance Technologies:

- The PCI compliance portal and all emails are branded as Nuvei.
- Registered sub-ISO's with Nuvei can create their own unique portal with their branding.
- Combined SAQ options for merchants with same TIN.
- Automatic scans with notification emails for attestation of a completed scan.

PCI

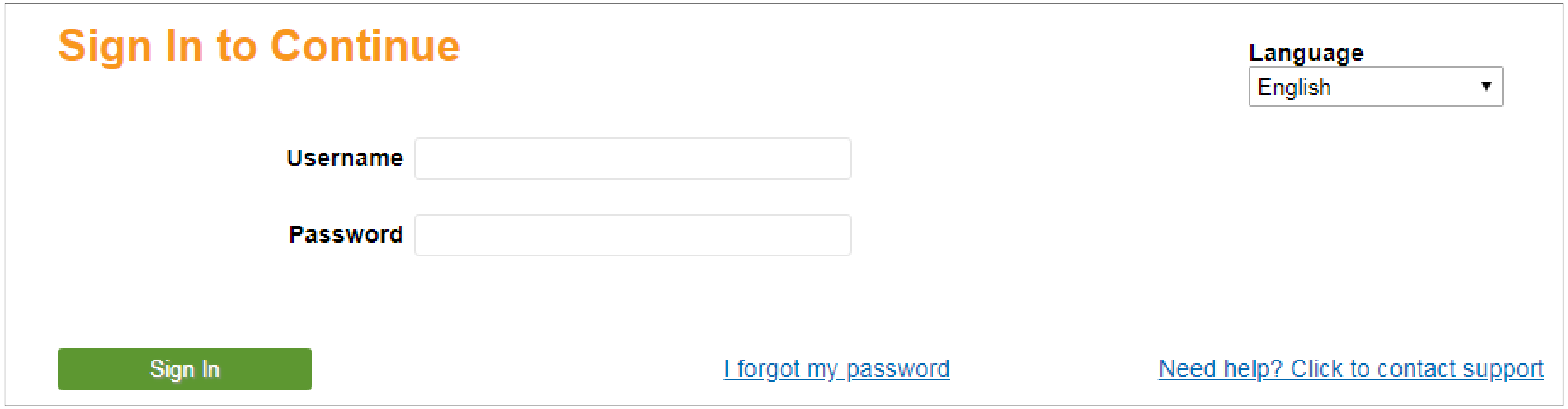
Our application will guide you through the completion of your PCI DSS Self-Assessment Questionnaire (SAQ) and includes (if applicable) the required quarterly scans of your processing systems.

To access the tool, simply logon: https://nuvei.pcitoolkit.com/version3/SignIn.aspx

Username: merchant's email
Password: provided in the welcome email.

Contact Us

Email: support@pcitoolkit.com
Phone: 1-833-445-3007



Sign In to Continue

Language: English

Username

Password

PCI

ADDITIONAL RESOURCES

https://www.pcisecuritystandards.org/index.php

nuvei
Payment Technology Network

nuvei

Payment Technology Network

THANK YOU