



Security  
Standards Council

# The PCI Security Standards Council

# What is PCI SSC?

- An independent standards body providing industry oversight of the development and management of Payment Card Industry Security Standards on a global basis.

# What will PCI SSC do?

PCI Security Standards Council will :

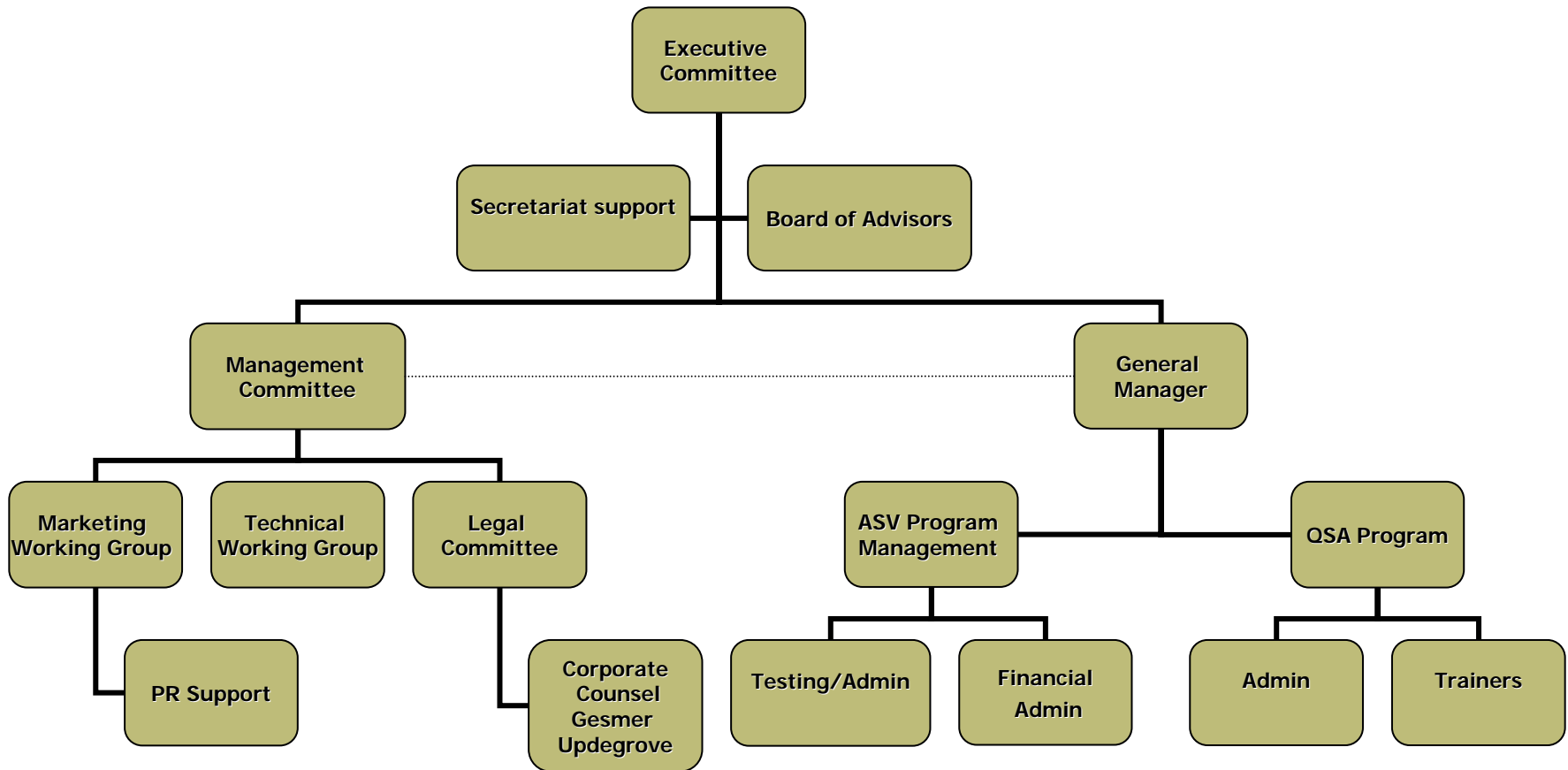
- Foster adoption of a single set of security standards by providing ongoing education and training to all key stakeholders (merchants, banks, TPPs, POS vendors).
- Create and manage a globally available, qualified pool of security solution providers to help stakeholders implement the standards and validate compliance
- Invite stakeholders to participate on the ongoing development of the PCI Data Security Standards

# How will PCI SSC do this?

## What resources does it have?

- Support from the five founding leading payment brands: American Express, Discover, JCB, MasterCard Worldwide and Visa international
- A full service PCI website
- An executive steering committee
- The feedback and support of participating organizations like yours!

# How is the organization structured?



# How can we get involved?

- **Become a Participating Organization**
  - Merchants, payment device and services vendors, processors and financial institutions are encouraged to join the PCI Security Standards Council as Participating Organizations
- **Stand for election to the Advisory Board**
  - The Advisory Board will provide strategic and technical guidance to the PCI Security Standards Council, reflecting different stakeholder perspectives
  - Two-thirds of the Advisory Board members will be elected to serve on the Advisory Board from within the ranks of Participating Organizations. The remaining one-third will be appointed by the Council's Executive Committee.

Qualified security assessors (QSAs) and approved scanning vendors (ASVs) are not eligible to be Participating Organizations, but will have an opportunity to comment on the standards. Please contact PCI Security Standards Council for additional details.

# Why get involved?

- Participating organizations may:
  - recommend changes and provide input on future initiatives
  - be eligible for election/appointment to the Board of Advisors
  - nominate representatives for election to the PCI Security Standards Council Advisory Board
  - have access to and ability to comment on drafts of potential changes to security standards in advance
  - attend annual PCI SSC community meeting
- Participating organizations will supply feedback on the next evolution of the Data Security Standard

## Next steps to participation:

1. Visit [PCISecurityStandards.org](https://PCISecurityStandards.org) or email [info@pcisecuritystandards.org](mailto:info@pcisecuritystandards.org)
2. complete and submit two copies of application to the PCI Security Standards Council, LLC.
  - *Annual dues for Participating Organizations are \$2,000*

Participation is open to any business, other than qualified security assessors (QSAs) and approved scanning vendors (ASVs), that participates in payment processing (merchants, banks, POS vendors) and that supports the mission, goals and activities of the organization.

# Security Solution Providers

- The PCI Security Standards Council manages global training and certification programs for qualified security assessors (QSAs) and approved scanning vendors (ASVs).
- Solution Providers will assist stakeholders implement the standard and validate compliance
  - The training, testing and certification programs will provide a uniform, global approach to account data protection.
  - Each of the five founding members will recognize the QSAs and ASVs certified as being qualified to validate compliance to the PCI DSS standards.

# How to Become a QSA

As of September 7, 2006, the PCI Security Standards Council will operate an in-depth program for security companies seeking to become Qualified Security Assessors (QSAs), and to be re-certified each year.

Prospective QSA companies must:

- Apply as a firm for qualification in the program;
- Provide documentation adhering to the Validation Requirements for Qualified Security Assessors (QSA) v. 1.1
- Qualify individual employees, through training and testing, to perform the assessments
- Execute an agreement with the PCI Security Standards Council governing performance

# How to Become an ASV

The PCI Security Standards Council will maintain a structured process for security solution providers to become Approved Scanning Vendors (ASVs), as well as to be re-approved each year.

- The major requirement of the process is a rigorous remote test conducted by each vendor on the PCI Security Standards Council's test infrastructure, which simulates the network of a typical security scan customer.
- Execute an agreement with the PCI Security Standards Council governing performance

# Information on QSA or ASV Programs

Visit [PCISecurityStandards.org](https://PCISecurityStandards.org) or email  
[info@pcisecuritystandards.org](mailto:info@pcisecuritystandards.org)



Security  
Standards Council

# PCI DSS VERSION 1.1

# How has the PCI Data Security Standard changed ?

Updates are designed to acknowledge partner and customer feedback, along with technical compliance constraints, and foster rapid adoption, while maintaining the robustness of the security measures

- The focus of the 1.1 revision has been to address questions about how to implement the standard.
  - The standard has been updated to provide clarification to certain requirements
  - Give guidance for compensating controls for complex requirements such as data encryption.
- Additional requirements have been added to address emerging threats related to application security.

# Security Improvements

- New Requirements:
  - 2.4 Added Hosting provider requirements
    - Appendix A – PCI DSS Applicability for Hosting Providers. Established requirements for providers that host merchant and service provider clients
  - 5.1.1 Malicious software, such as spyware and adware, are included in anti-virus software capabilities
  - 6.6 Requirement for application review or application firewall
    - This is a best practice until June 30,2008, after which it will be a requirement
  - 12.10 Added requirement for a policy to manage connected entities to which companies send cardholder data or allow to impact cardholder data, including maintaining a list, implementing appropriate due diligence, ensuring applicable connected entities are PCI DSS complaint and having an established process to connect and disconnect entities

# Implementation Changes

- Appendix B – Compensating Controls. Defines compensating Controls in general and discusses compensating controls when stored cardholder data cannot be rendered unreadable

# When is Version 1.1 Effective?

- Version 1.1 of the PCI Data Security Standard became effective with the launch of the PCI Security Standards Council.
  - Some of the more complex individual requirements contained in the new version of the standard have built-in lead time for implementation
- As of January 1, 2007 all new certifications and newly initiated re-certifications must be based on DSS version 1.1.



Security  
Standards Council

QUESTIONS?