Payment Card Industry
Data Security Standard (PCI DSS)

Payment Application
Data Security Standard (PA-DSS)

Summary of 2012 Feedback

**Summary of Feedback Received for PCI DSS v2.0
and PA-DSS v2.0**

August 2012

Feedback for PCI DSS v2.0 and PA-DSS v2.0

Objective

This document presents a summary of the feedback that was provided to the Payment Card Industry Security Standards Council (PCI SSC) relating to v2.0 of the *PCI Data Security Standard (PCI DSS)* and *PCI Payment Application Data Security Standard (PA-DSS)*.

Context

As part of the documented Feedback Lifecycle for PCI DSS and PA-DSS, the PCI Security Standards Council (PCI SSC) solicits input for proposed changes to the standards from PCI SSC stakeholders – Participating Organizations, including merchants, banks, processors, hardware and software developers, Board of Advisors, point-of-sale vendors, and the assessment community (QSAs, PA-QSAs, & ASVs). Changes to the PCI standards follow a defined 36-month lifecycle with eight stages, described on the Council's website. This report depicts the results of stages 4 and 6 of the lifecycle:

> **Stage 4 (Feedback Begins):** The fourth stage initiates a period of systematic feedback from stakeholders on the new standards. Stakeholders will have the opportunity to formally express their views on the new standards and provide suggestions for changes and improvements. Stage 4 occurs during November to March of Year 2. *Note: PCI DSS/PA-DSS v2.0 feedback deadline was extended to April 15*.
>
> **Stage 6 (Feedback Review):** The sixth stage is for collecting and evaluating feedback from Participating Organizations, and occurs during April through August of Year 2.

Note for Stage 5 (Old Standards Retired): This stage occurs on December 31 of year 2, when the prior versions of PCI DSS and PA-DSS are retired. Both PCI DSS version 1.2 and PA-DSS version 1.2 were retired December 31, 2011.

During **Stage 7 (Draft Revisions)** through April of year 3, and **Stage 8 (Final Review**) through July of year 3, the feedback will continue to be analyzed as draft content is written and reviewed. The final disposition of the feedback will be determined during stage 8.

Approach

Upon conclusion of the feedback collection period, contributor comments and suggested solutions were collated and grouped into their respective categories for PCI DSS and PA-DSS as well as for supporting documents. The Technical Working Group, consisting of the PCI SSC and payment brand subject matter experts, reviewed each item to determine how the proposed solution may enhance the Standard(s) or supporting documents, and to determine the response category. Each item was categorized into one of the feedback categories represented in Table 1, and the resultant response category, as listed in Table 2.

Table 1: Feedback Categories	
Category	**Explanation**
Request for clarification	To clarify intent of existing content, identify typographical errors, formatting issues, unclear messaging, etc.
Request for additional guidance	To request new information supplements or other guidance on specific technology or issue
Request change to existing requirement /testing procedure	To identify where an existing requirement or testing procedure does not provide adequate coverage
Request new requirement / testing procedure	To address a gap in the existing requirements or testing procedures – e.g. a new security risk is not currently addressed
Feedback only – no change requested	To express opinion or provide comment – no changes to the standards or supporting documents

Table 2: Resultant Response Category	
Response	**Explanation**
Accepted for current consideration	Some or all of the suggested solution has been accepted for consideration to be incorporated into the standard(s) or other supporting documentation (e.g., navigation guide, FAQ, etc.). *Note: a comment may indicate a need for clarification which results in a different outcome than suggested in the feedback item. The actual/final actions are also subject to change during the course of the update process as mentioned above.*
No Action Requested (comment/feedback only)	The reviewer provided a comment and/or and opinion only and did not request a change. *Note: comment-only items may also be considered for adoption even though no action was requested.*
Not Considered for Adoption	The suggested solution is not being considered for adoption. Reasons for this may include: • Suggested solution applies only to a specific industry sector or technology platform • Suggested solution is not practical to implement in different environments or regions • The author misinterpreted the requirement • Suggested solution is already addressed in the PCI DSS, PA-DSS or other supporting documents • Suggested solution may reduce the effectiveness of the PCI DSS or other programs • Suggested solution is unclear • Suggested solution was considered out of scope
Brand Compliance Topic	The suggested solution is not being considered for adoption by PCI SSC since the feedback was directly related to one or more of the payment brands' compliance programs.
Retained for later consideration	The suggested solution may still be addressed, but not as part of this lifecycle update.

***Note:** While Table 2 denotes the initial response (proposed action to be taken), the actual/final actions are subject to change during the course of the update process in Stages 7 and 8 as mentioned above.*

Results

The majority of the feedback received during the feedback lifecycle pertained to PCI DSS as illustrated in Figure 1. Similarly, notable trends that emerged during review were predominantly related to PCI DSS. The majority of this report is therefore focused on PCI DSS.

Figures 1 illustrates how feedback was distributed between PCI DSS and PA-DSS.

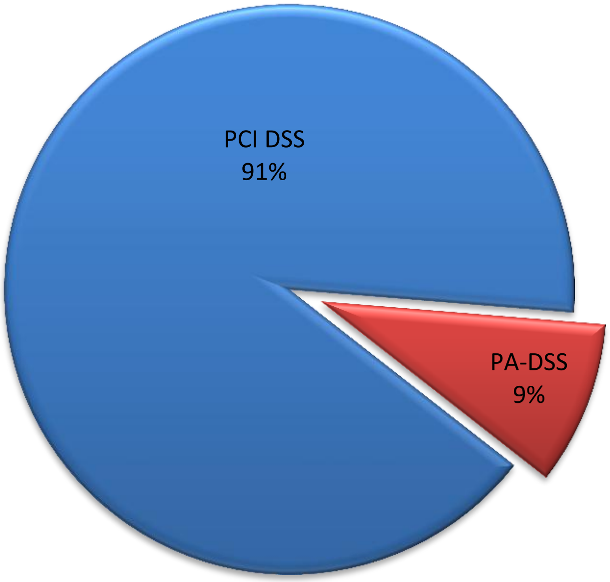
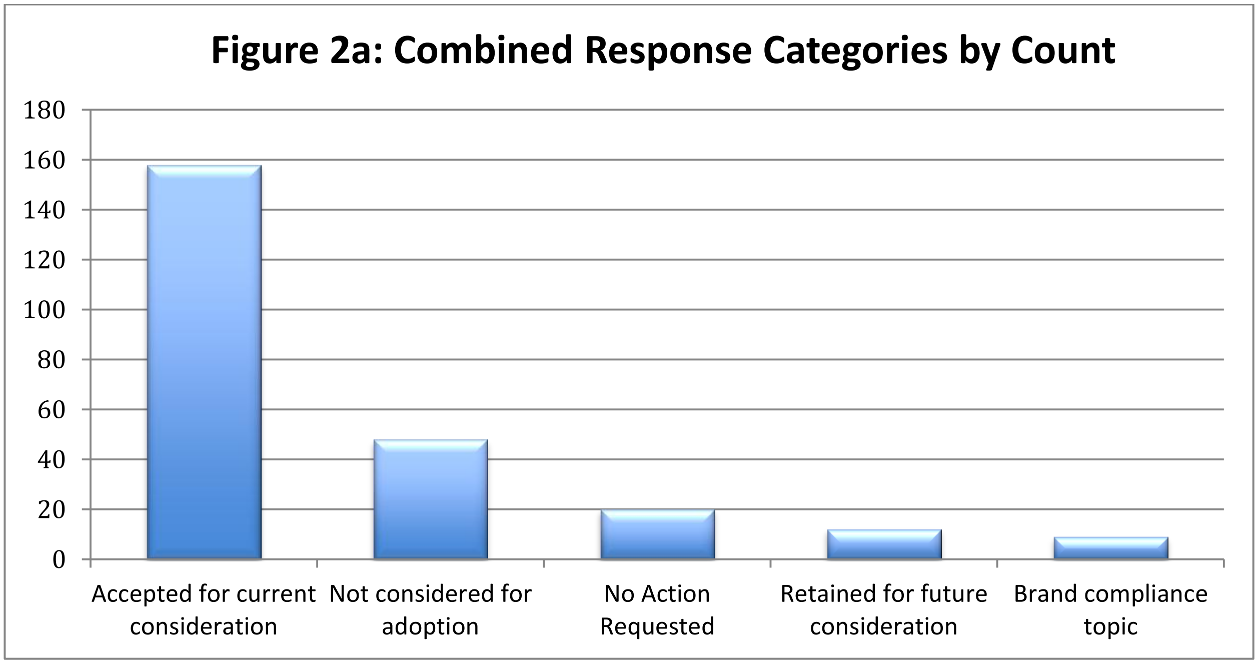


Figure 1: Total Feedback Received

Note that Figures 2 through 6 below illustrate the combined PCI DSS and PA-DSS feedback data.

The majority of PCI DSS and PA-DSS combined feedback consisted of items relating to technical content. As shown in figures 2a and 2b, 64% of all feedback was accepted for current consideration, with 19% not being considered for adoption. The remaining feedback is either being retained for future consideration, relates to a brand compliance topic, or there was no action requested (comment/feedback only).



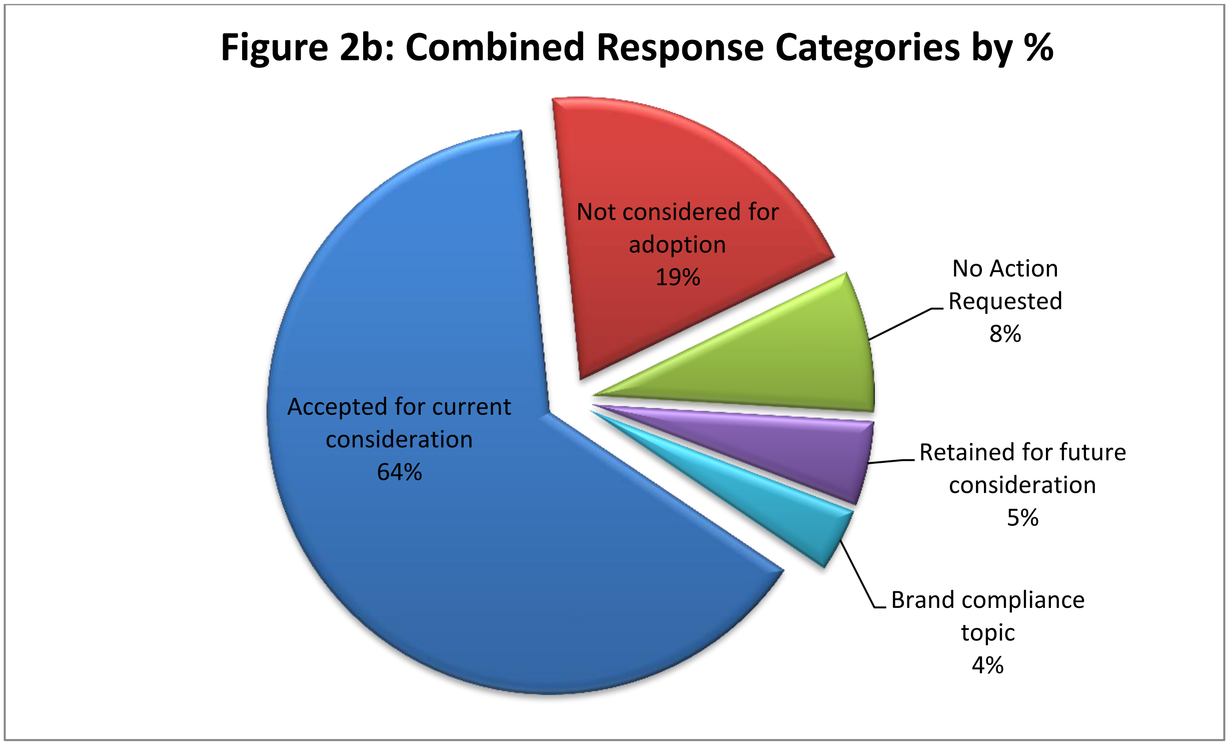
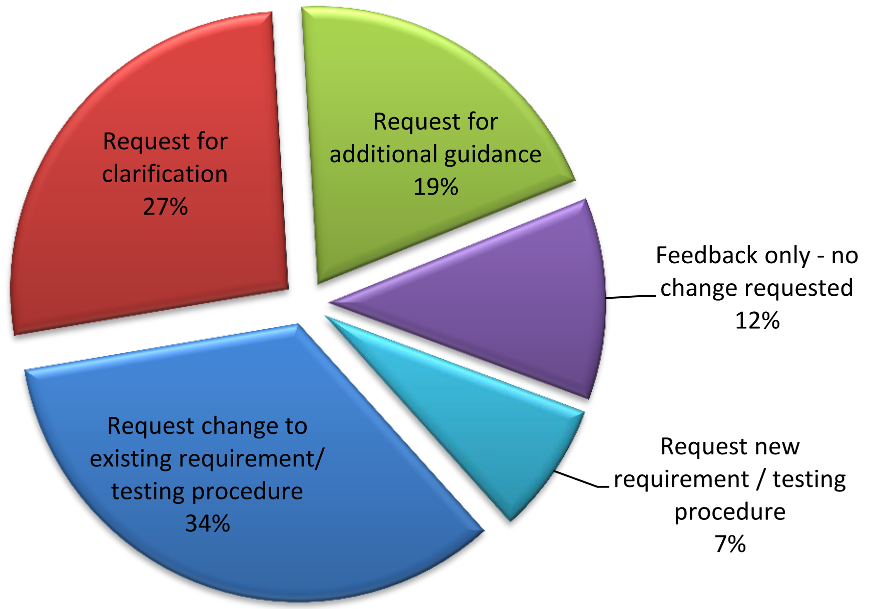
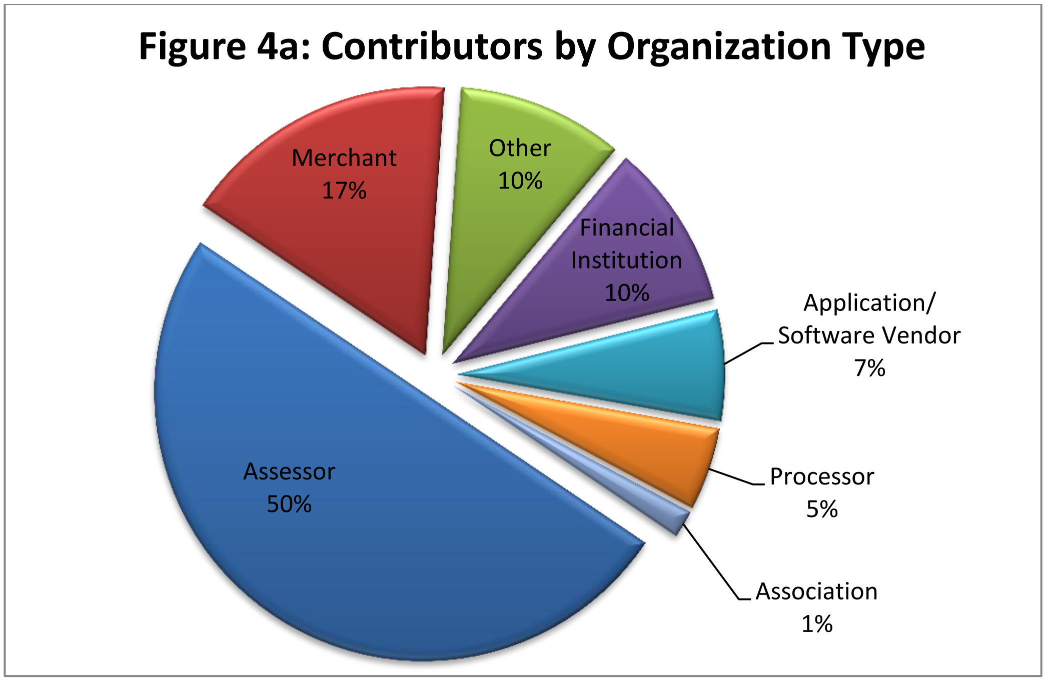


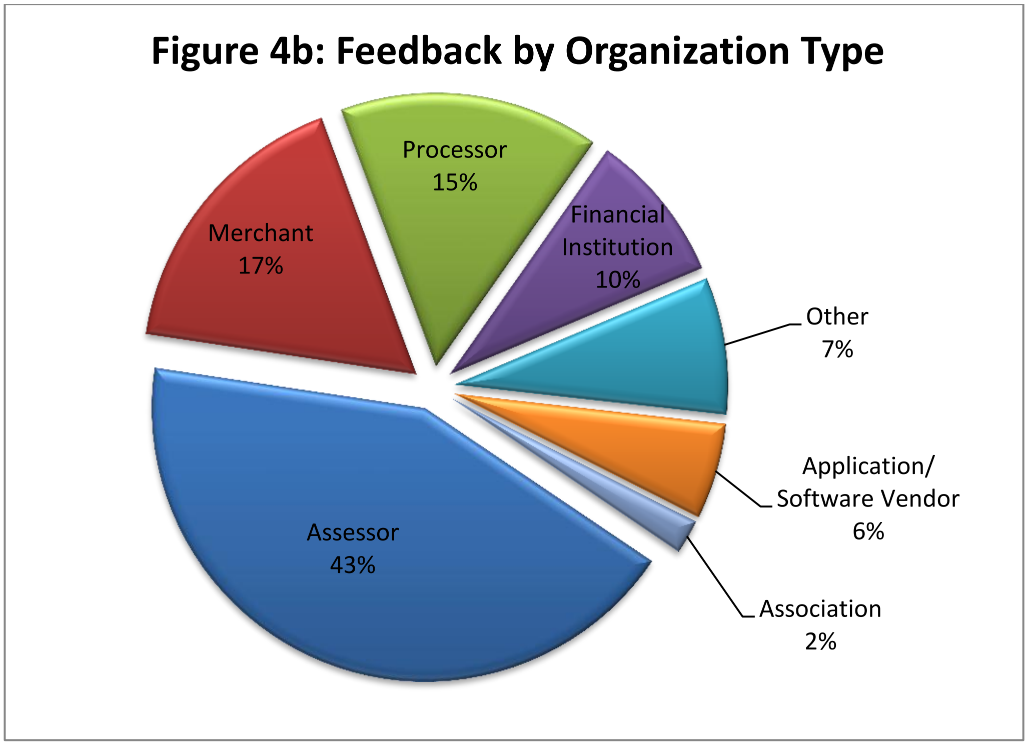
Figure 3 illustrates the relative breakdown of combined feedback categories by percentage. While requests to change an existing requirement/testing procedure accounted for 34% of all feedback received, requests for clarification and requests for additional guidance were also expressed at 27% and 19%, respectively. The remaining 19% were either comment-only feedback with no request for action (12%), or requests for new requirements/testing procedures (7%).

Figure 3: Combined Breakdown by Feedback Category



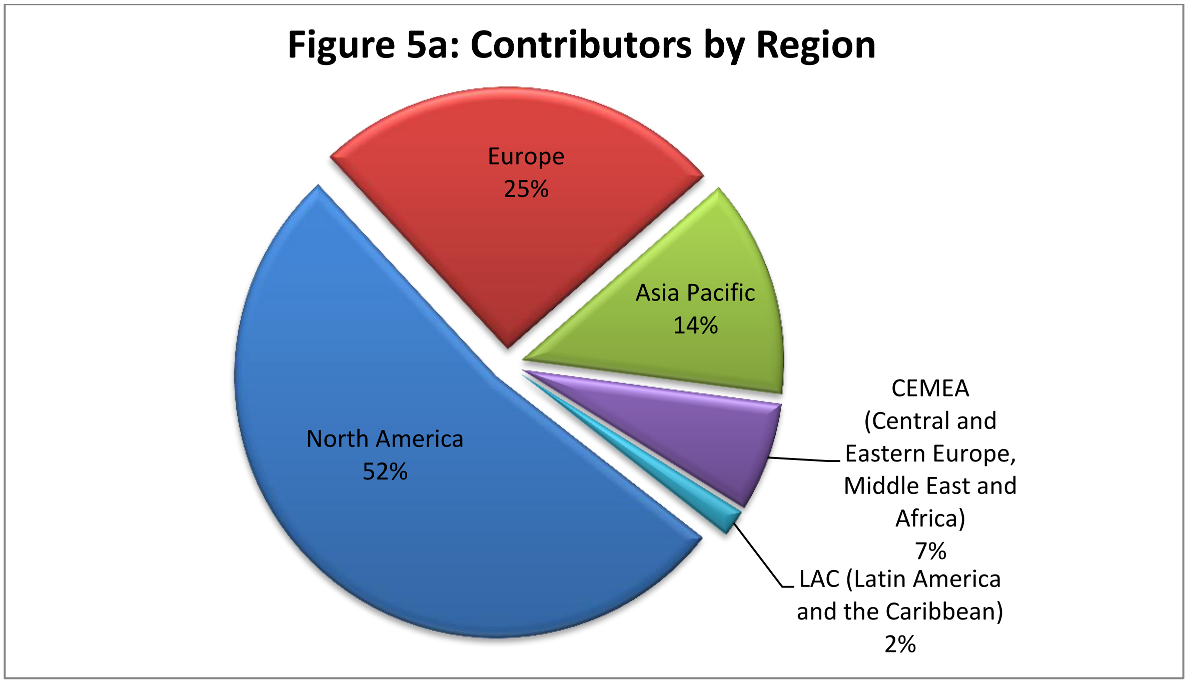
Assessors (QSAs, PA-QSAs, & ASVs) represented 50% of all contributing organizations (Figure 4a), and provided 43% of all feedback (Figure 4b). Merchant and Financial Institution representation was consistent with the percentage of all feedback provided, at 17% and 10%, respectively. While Processors represented just 5% of the contributing organizations, they provided 15% of all feedback. Representation by Application/Software Vendors and Associations was consistent with the percentage of all feedback provided.

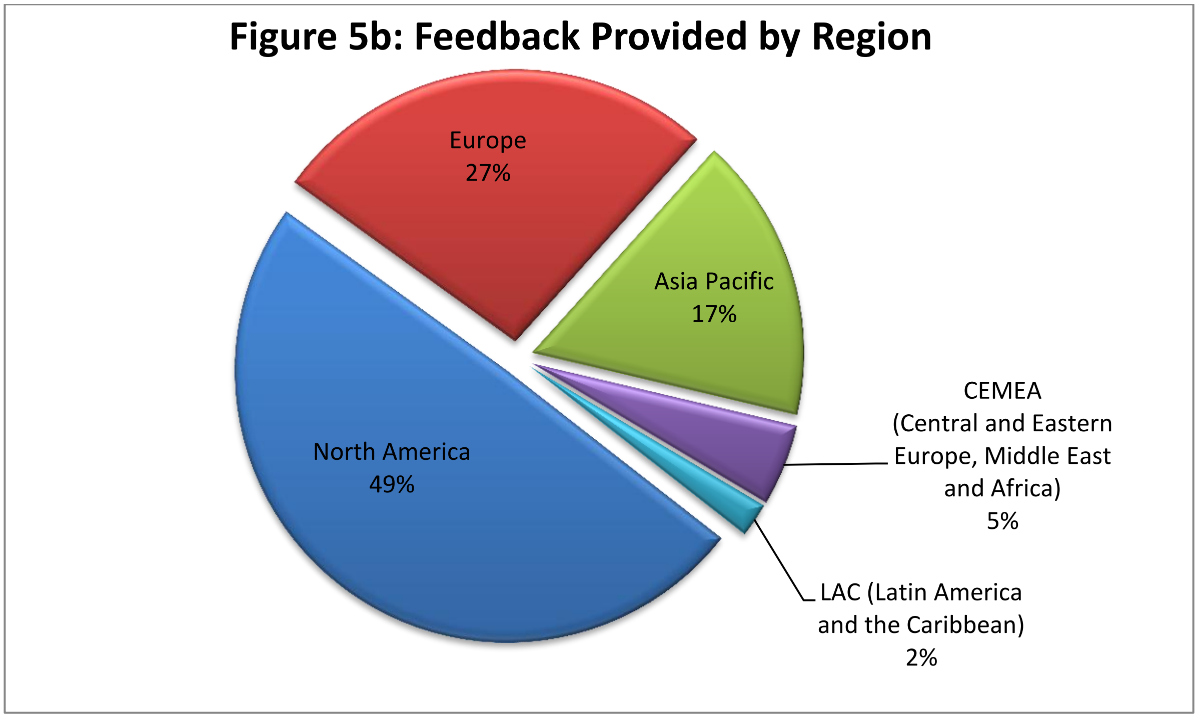




Feedback was distributed across different regions as follows:

- 52% of all contributing organizations were based in North America, and provided 49% of all feedback.
- 25% of the contributing organizations were based in Europe, and provided 27% of all feedback.
- 14% of all contributing organizations were based in Asia Pacific, and provided 17% of all feedback.
- 7% of all contributing organizations were based in CEMEA, and provided 5% of all feedback.
- 2% of all contributing organizations were based in LAC, and provided 2% of all feedback.





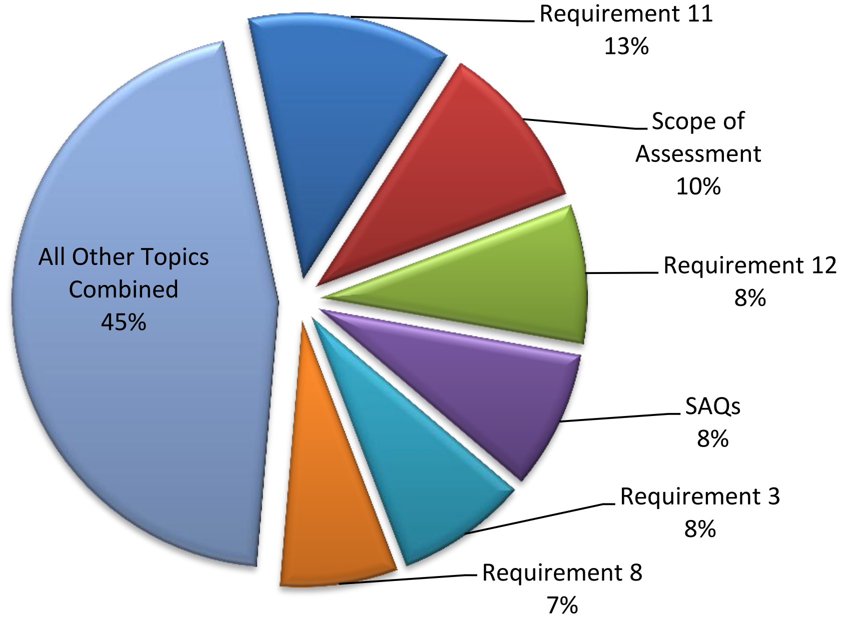
PCI DSS Trends

During feedback review, some noticeable trends were evident; more than half of all PCI DSS feedback was comprised of the following topics:

Table 3: PCI DSS Feedback Trends

Topic	Feedback Suggestions
PCI DSS Requirement 11.2	Prescribe use of specific tools, require ASVs to perform internal scans, and define what constitutes a "significant change".
PCI DSS Scope of Assessment	Provide detailed guidance on scoping and segmentation.
PCI DSS Requirement 12.8	Clarify the terms "service provider" and "shared," and provide more prescriptive requirements regarding written agreements that apply to service providers.
PCI DSS SAQs	Consider updating the SAQs; they are either too complex (difficult to understand) or not detailed enough. Either include more requirements, or do not include so many requirements.
PCI DSS Requirement 3.4	Encryption and key management (e.g., keys tied to user accounts) are complex requirements; provide further clarification. Truncation/hashing/tokenization is not a convenient method to store and retrieve data; provide further guidance.
PCI DSS Requirement 8.5	Consider updating password requirements (expand authentication beyond just passwords). The current password requirements are either too strict or not strict enough; be either less prescriptive or more prescriptive.

Figure 6: Top PCI DSS Feedback Topics



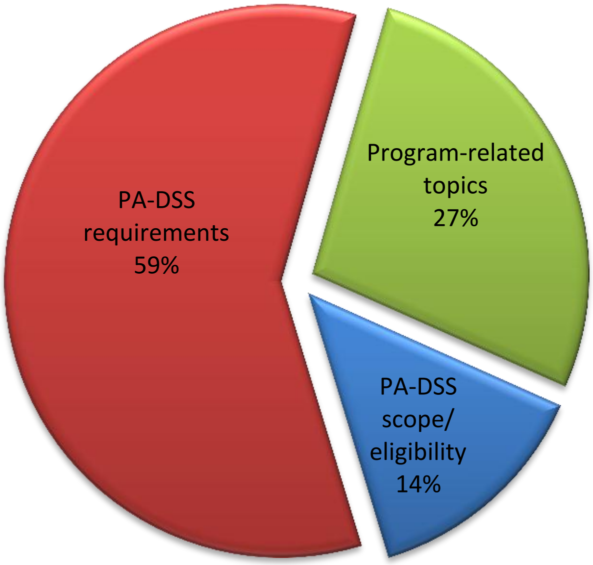
PA-DSS Themes

While less overall feedback was received for PA-DSS, the following themes were noticeable:

Table 4: PA-DSS Feedback Themes

Topic	Feedback Suggestions
PA-DSS Requirements	Develop additional PA-DSS requirements for different technologies, such as mobile, EMV, tokenization, etc.
PA-DSS Program	Streamline PA-QSA submission and assessment processes, as well as application updates and listing processes.
PA-DSS scope/eligibility	Expand applicability of PA-DSS to non-payment applications, bespoke applications, payment terminals, etc.

Figure 7: PA-DSS Feedback Themes


PA-DSS requirements 59%
Program-related topics 27%
PA-DSS scope/ eligibility 14%