# Appendix C. Sample QSA Feedback Form

This form is used to review QSAs and their work product, and is intended to be completed after a PCI audit by the QSA client. While the primary audience of this form are QSA audit clients (merchants or service providers), there are several questions at the end, under “QSA Feedback Form for Payment Brands and Others,” to be completed as needed by Payment Brand participants, banks, and other relevant parties. This form can be obtained directly from the QSA during the audit, or can be found online in a useable format at www.pcisecuritystandards.org. The client, not the QSA, should submit this form to PCI SSC. Please send this completed form to PCI SSC at: qsa@pcisecuritystandards.org

| | |
|---|---|
| **QSA FEEDBACK FORM** | |
| **Client Name (merchant or service provider)** | **Qualified Security Assessor company (QSA)** |
| *NAME* | *NAME* |
| *CONTACT* | *CONTACT* |
| *TELEPHONE* | *TELEPHONE* |
| *E-MAIL* | *E-MAIL* |
| **Business location where assessment took place** | **QSA employee who performed assessment** |
| *STREET* | *NAME* |
| *CITY* | *TELEPHONE* |
| *STATE/ZIP* | *E-MAIL* |
| For each question, please indicate the response that best reflects your experience and provide comments.<br>**4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree** | |
| **1) During the initial engagement, did the QSA explain the objectives, timing, and review process, and address your questions and concerns?** | |
| Response: | |
| Comments: | |
| **2) Did the QSA employee(s) understand your business and technical environment, and the payment card industry?** | |

| |
|---|
| Response: |
| Comments: |
| **3) Did the QSA employee(s) have sufficient security and technical skills to effectively perform this audit?** |
| Response: |
| Comments: |
| **4) Did the QSA sufficiently understand the PCI Data Security Standard and the PCI Security Audit Procedures?** |
| Response: |
| Comments: |
| **5) Did the QSA effectively minimize interruptions to operations and schedules?** |
| Response: |
| Comments: |
| **6) Did the QSA provide an accurate estimate for time and resources needed?** |
| Response: |
| Comments: |
| **7) Did the QSA provide an accurate estimate for report delivery?** |
| Response: |
| Comments: |
| **8) Did the QSA attempt to market products or services for your company to attain PCI compliance?** |
| Response: |
| Comments: |
| **9) Did the QSA imply that use of a specific brand of commercial product or service was necessary to achieve compliance?** |

| |
|---|
| Response: |
| Comments: |
| **10) In situations where remediation was required, did the QSA present product and/or solution options that were not exclusive to their own product set?** |
| Response: |
| Comments: |
| **11) Did the QSA use secure transmission to send any confidential reports or data?** |
| Response: |
| Comments: |
| **12) Did the QSA demonstrate courtesy, professionalism, and a constructive and positive approach?** |
| Response: |
| Comments: |
| **13) Was there sufficient opportunity for you to provide explanations and responses during the audit?** |
| Response: |
| Comments: |
| **14) During the review wrap-up, did the QSA clearly communicate findings and expected next steps?** |
| Response: |
| Comments: |
| **15) Did the QSA provide sufficient follow-up during your company's remediation efforts, until eventual compliance was achieved?** |
| Response: |
| Comments: |
| **Please provide any additional comments here about the QSA, your audit, or the PCI documents.** |

| | |
|---|---|
| **QSA FEEDBACK FORM FOR PAYMENT BRANDS AND OTHERS** | |
| Name of QSA Client (merchant or service provider reviewed): | QSA Company name:) |
| Payment Brand Reviewer | QSA employee who performed assessment |
| *NAME* | *NAME* |
| *TELEPHONE* | *TELEPHONE* |
| *E-MAIL* | *E-MAIL* |
| For each question, please indicate the response that best reflects your experience and provide comments.<br>**4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree** | |
| | |
| **1) Does the QSA clearly understand how to notify your payment brand about compliance and non-compliance issues, and the status of merchants and service providers?** | |
| Response: | |
| Comments: | |
| **2) Did you receive any complaints about QSA activities related to this audit?** | |
| Response: | |
| Comments: | |
| **3) Did the QSA demonstrate sufficient understanding of the PCI Data Security Standard and the PCI Security Audit Procedures?** | |
| Response: | |
| Comments: | |