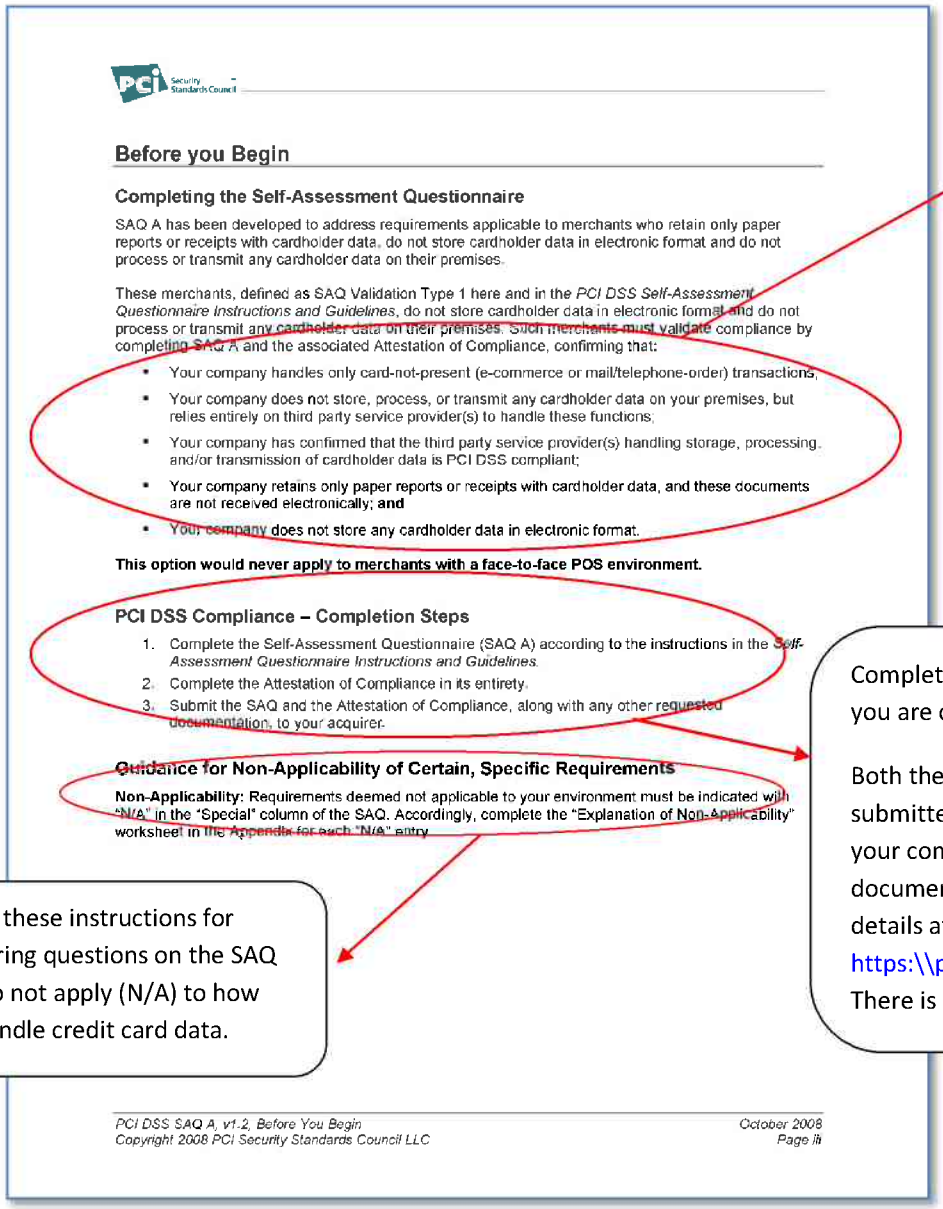
Attestation of Compliance (AOC)
&
Self Assessment Questionnaire A (SAQ A) Help Guide

This document is designed to provide you addition assistance in completing the Attestation of Compliance (AOC) and Self-Assessment Questionnaire A (SAQ A). It identifies some common mistakes and attempts to clarify for you what information the document is asking for. It is not representative of the entire AOC or SAQ A and does not include all pages of the AOC or SAQ A.

This document is not a comprehensive or complete guide to the Payment Card Industry Data Security Standard (PCI DSS), any Attestation of Compliance, or any Self-Assessment Questionnaire. For complete information on PCI DSS including the AOC's and SAQ's you can visit the Payment Card Industry Security Standards Council web site at https://www.pcisecuritystandards.org.

Your first step in completing the AOC and SAQ A is to determine your eligibility to complete SAQ A. To do so you must read "**Before you Begin**" (page iii).



PCI Security Standards Council

Before you Begin

Completing the Self-Assessment Questionnaire

SAQ A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises.

These merchants, defined as SAQ Validation Type 1 here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises. Such merchants must validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that:

- Your company handles only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your premises, but relies entirely on third party service provider(s) to handle these functions;
- Your company has confirmed that the third party service provider(s) handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant;
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; **and**
- Your company does not store any cardholder data in electronic format.

This option would never apply to merchants with a face-to-face POS environment.

PCI DSS Compliance – Completion Steps

1. Complete the Self-Assessment Questionnaire (SAQ A) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
2. Complete the Attestation of Compliance in its entirety.
3. Submit the SAQ and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

Guidance for Non-Applicability of Certain, Specific Requirements

Non-Applicability: Requirements deemed not applicable to your environment must be indicated with "N/A" in the "Special" column of the SAQ. Accordingly, complete the "Explanation of Non-Applicability" worksheet in the Appendix for each "N/A" entry.

PCI DSS SAQ A, v1.2, Before You Begin *October 2008*
Copyright 2008 PCI Security Standards Council LLC *Page iii*

You must meet all 5 of these conditions to be eligible for to complete SAQ A. If you do not meet all 5 of these conditions you must complete SAQ B, C, or D.

IMPORTANT: If you use the Authorize.Net virtual terminal or the CyberSource virtual terminal to process credit cards you are NOT eligible to complete SAQ A.

Complete these 3 steps to validate that you are compliant with PCI DSS.

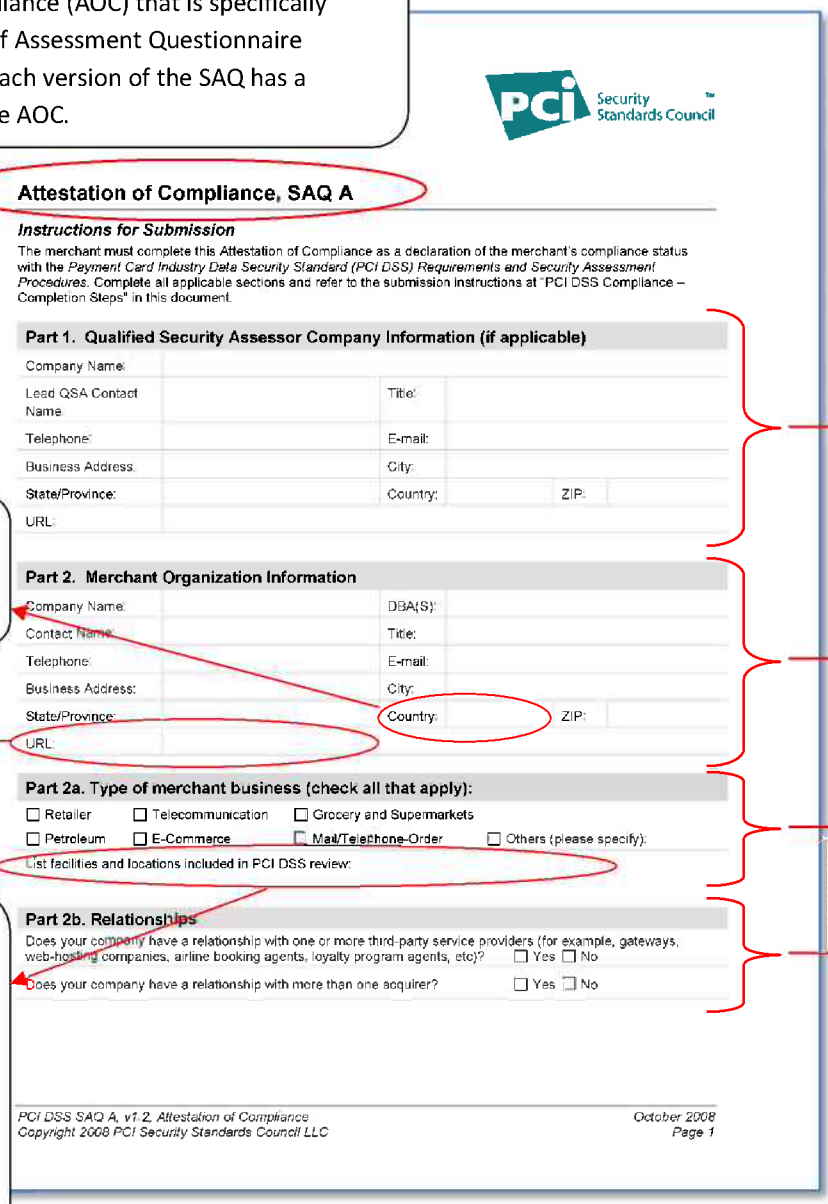
Both the signed AOC and SAQ must be submitted to CyberSource to validate your compliance. You must upload these documents and register you compliance details at to our secure portal… https:\\pci.trustwave.com\cybersource. There is no charge for you to do this.

Follow these instructions for answering questions on the SAQ that do not apply (N/A) to how you handle credit card data.

Attestation of Compliance (AOC)
&
Self Assessment Questionnaire A (SAQ A) Help Guide

Attestation of Compliance (AOC)

Here you can see that you are completing the Attestation of Compliance (AOC) that is specifically associated to the Self Assessment Questionnaire version A (SAQ A). Each version of the SAQ has a related version of the AOC.



PCI Security Standards Council

Attestation of Compliance, SAQ A

Instructions for Submission

The merchant must complete this Attestation of Compliance as a declaration of the merchant's compliance status with the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Complete all applicable sections and refer to the submission instructions at "PCI DSS Compliance – Completion Steps" in this document.

Part 1. Qualified Security Assessor Company Information (if applicable)

Company Name:			
Lead QSA Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	ZIP:
URL:			

Part 2. Merchant Organization Information

Company Name:		DBA(S):	
Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	ZIP:
URL:			

Part 2a. Type of merchant business (check all that apply):

☐ Retailer ☐ Telecommunication ☐ Grocery and Supermarkets
☐ Petroleum ☐ E-Commerce ☐ Mail/Telephone-Order ☐ Others (please specify):

List facilities and locations included in PCI DSS review:

Part 2b. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)? ☐ Yes ☐ No

Does your company have a relationship with more than one acquirer? ☐ Yes ☐ No

PCI DSS SAQ A, v1.2, Attestation of Compliance *October 2008*
Copyright 2008 PCI Security Standards Council LLC *Page 1*

This field is asking for Country (i.e. USA) not County.

This field is for your website address and is required.

This field is required. Provide addresses of any locations that were included in the PCI review. This includes any home offices where your business is operated from.

Part 1. This section should be completed if you engaged the services of a Qualified Security Assessor (QSA). If you did not work with a QSA to validate your compliance with PCI DSS then this part should be left blank.

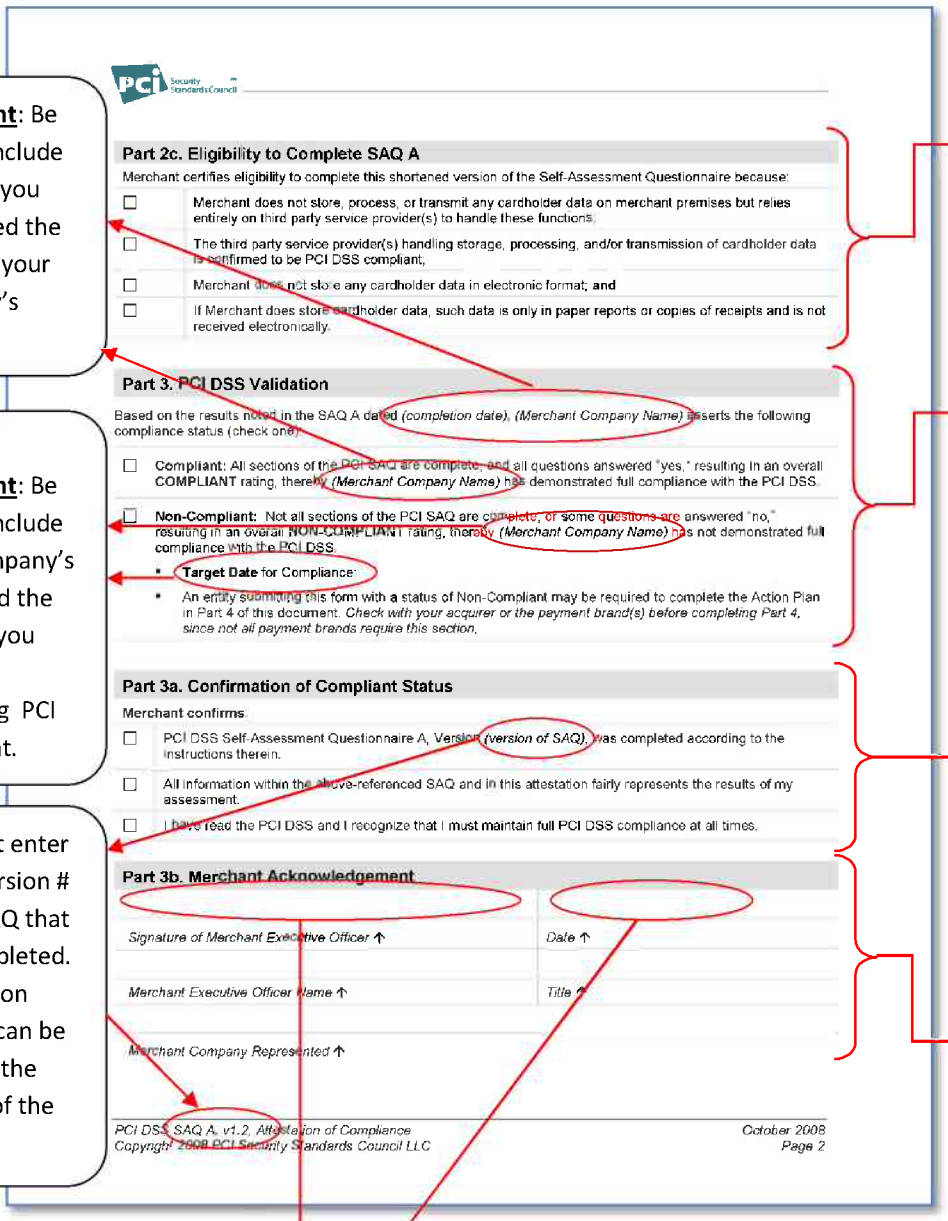
Part 2. This section is to be completed with your company and contact information. You are the Merchant Organization. All fields are required including URL.

Part 2a. In this section you check all the boxes that apply to your type of business. If necessary check "Others" and provide a description (e.g. Church, School, etc.). Be sure to include the addresses of any offices or facilities that were included in the PCI DSS review. This would include any home offices where the business is operated.

Part 2b. This section is asking if you work with more than one third-party service provider and if you work with more than one merchant acquirer. A service provider is a company that would have access to the credit card data of payments you accept. Web-hosting companies and payment gateways are examples of these. Authorize.Net and CyberSource are examples of payment gateways. An acquirer is a financial institution or other organization that provided you with a merchant account. CyberSource is an example of a

Attestation of Compliance (AOC)
&
Self Assessment Questionnaire A (SAQ A) Help Guide

Attestation of Compliance (AOC)



Part 2c. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

- ☐ Merchant does not store, process, or transmit any cardholder data on merchant premises but relies entirely on third party service provider(s) to handle these functions;
- ☐ The third party service provider(s) handling storage, processing, and/or transmission of cardholder data is confirmed to be PCI DSS compliant;
- ☐ Merchant does not store any cardholder data in electronic format; and
- ☐ If Merchant does store cardholder data, such data is only in paper reports or copies of receipts and is not received electronically.

Part 3. PCI DSS Validation

Based on the results noted in the SAQ A dated *(completion date)*, *(Merchant Company Name)* asserts the following compliance status (check one):

- ☐ **Compliant:** All sections of the PCI SAQ are complete, and all questions answered "yes," resulting in an overall **COMPLIANT** rating, thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS.
- ☐ **Non-Compliant:** Not all sections of the PCI SAQ are complete, or some questions are answered "no," resulting in an overall **NON-COMPLIANT** rating, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS.
  - **Target Date** for Compliance:
  - An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

Merchant confirms:

- ☐ PCI DSS Self-Assessment Questionnaire A, Version *(version of SAQ)*, was completed according to the instructions therein.
- ☐ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment.
- ☐ I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.

Part 3b. Merchant Acknowledgement

Signature of Merchant Executive Officer ↑	*Date* ↑
Merchant Executive Officer Name ↑	*Title* ↑
Merchant Company Represented ↑	

PCI DSS, SAQ A, v1.2, Attestation of Compliance *October 2008*
Copyright 2008 PCI Security Standards Council LLC *Page 2*

Compliant: Be sure to include the date you completed the SAQ and your company's name.

Non-Compliant: Be sure to include your company's name and the date for you plan on becoming PCI compliant.

You must enter in the version # of the SAQ that you completed. The version number can be found at the bottom of the page.

Part 2c. This section is where you confirm that you are eligible to complete SAQ A. You must be able to check all of the boxes confirming that you meet all four conditions otherwise you are not eligible to complete SAQ A.

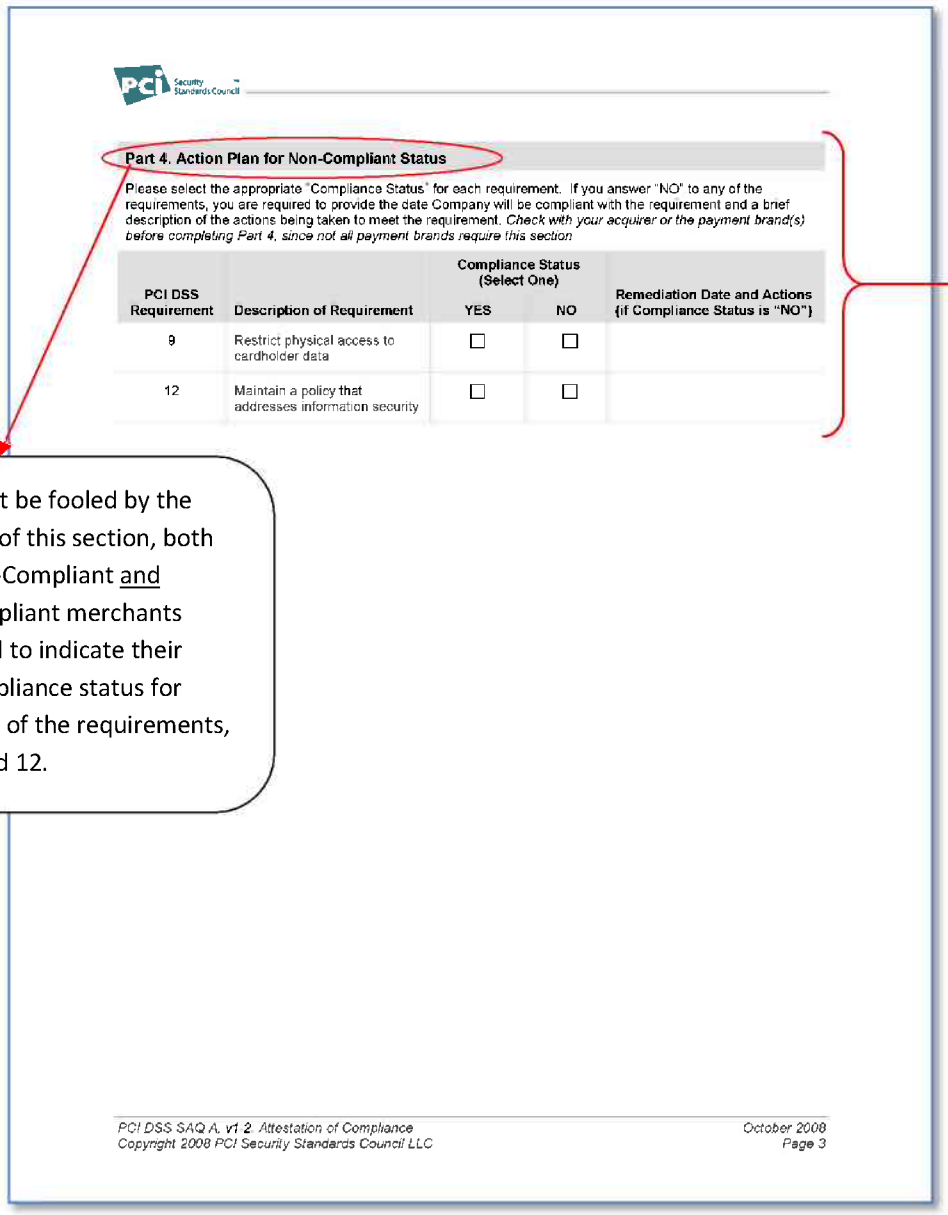
Part 3. This section is where you are validating your PCI DSS status as either Compliant or Non-Compliant.

Part 3a. In this section, if you have stated to be Compliant in Part 3 above you must check the three boxes affirming why you have deemed your company to be Compliant with PCI DSS.

Part 3b. This section is where you provide the Name, Title, and Signature of the person authorized to verify the information and statements made in the AOC. The Date is also required.

Signature and Date along with the Name and Title of the authorize signer are required.

Attestation of Compliance (AOC)



Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "NO" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section*

PCI DSS Requirement	Description of Requirement	Compliance Status (Select One) YES	NO	Remediation Date and Actions (if Compliance Status is "NO")
9	Restrict physical access to cardholder data	☐	☐	
12	Maintain a policy that addresses information security	☐	☐	

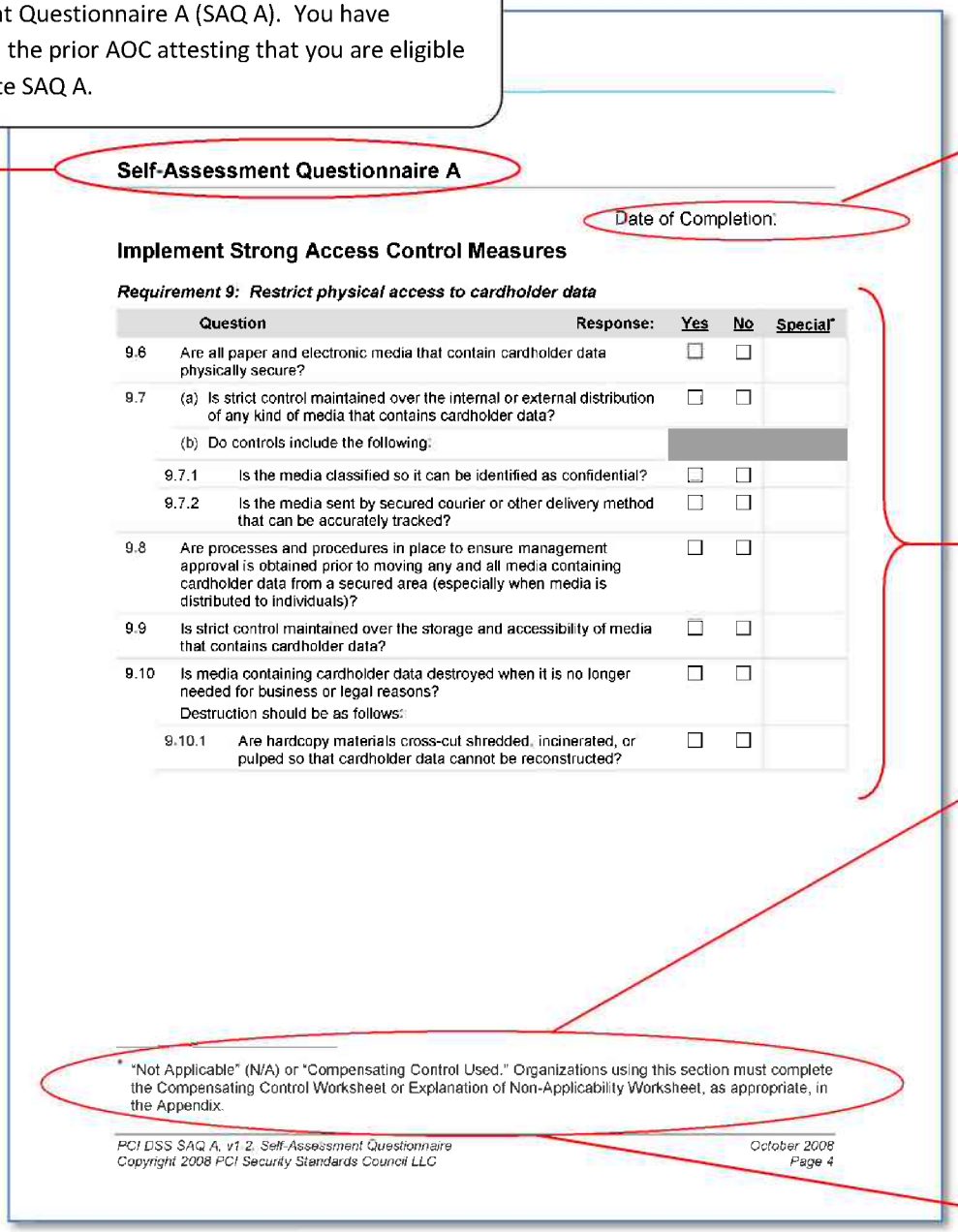
PCI DSS SAQ A, v1.2 Attestation of Compliance *October 2008*
Copyright 2008 PCI Security Standards Council LLC *Page 3*

Don't be fooled by the title of this section, both Non-Compliant and Compliant merchants need to indicate their compliance status for each of the requirements, 9 and 12.

Part 4. The title of this section is deceiving because both Compliant and Non-Compliant merchants must complete this section. You must answer "Yes" or "No" to whether or not you are compliant with PCI DSS requirement 9 and 12. If you answer "No" you must provide an explanation of what you are doing to become compliant with the requirement and the date of when you will be compliant with the requirement.

Self Assessment Questionnaire A (SAQ A)

Here you can see that you are now completing the Self Assessment Questionnaire A (SAQ A). You have completed the prior AOC attesting that you are eligible to complete SAQ A.



Self-Assessment Questionnaire A

Date of Completion:

Implement Strong Access Control Measures

Requirement 9: Restrict physical access to cardholder data

	Question	Response:	Yes	No	Special*
9.6	Are all paper and electronic media that contain cardholder data physically secure?		☐	☐	
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?		☐	☐	
	(b) Do controls include the following:				
9.7.1	Is the media classified so it can be identified as confidential?		☐	☐	
9.7.2	Is the media sent by secured courier or other delivery method that can be accurately tracked?		☐	☐	
9.8	Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals)?		☐	☐	
9.9	Is strict control maintained over the storage and accessibility of media that contains cardholder data?		☐	☐	
9.10	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows:		☐	☐	
9.10.1	Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		☐	☐	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS SAQ A, v1.2, Self-Assessment Questionnaire *October 2008*
Copyright 2008 PCI Security Standards Council LLC *Page 4*

Enter the date that you completed the SAQ questions.

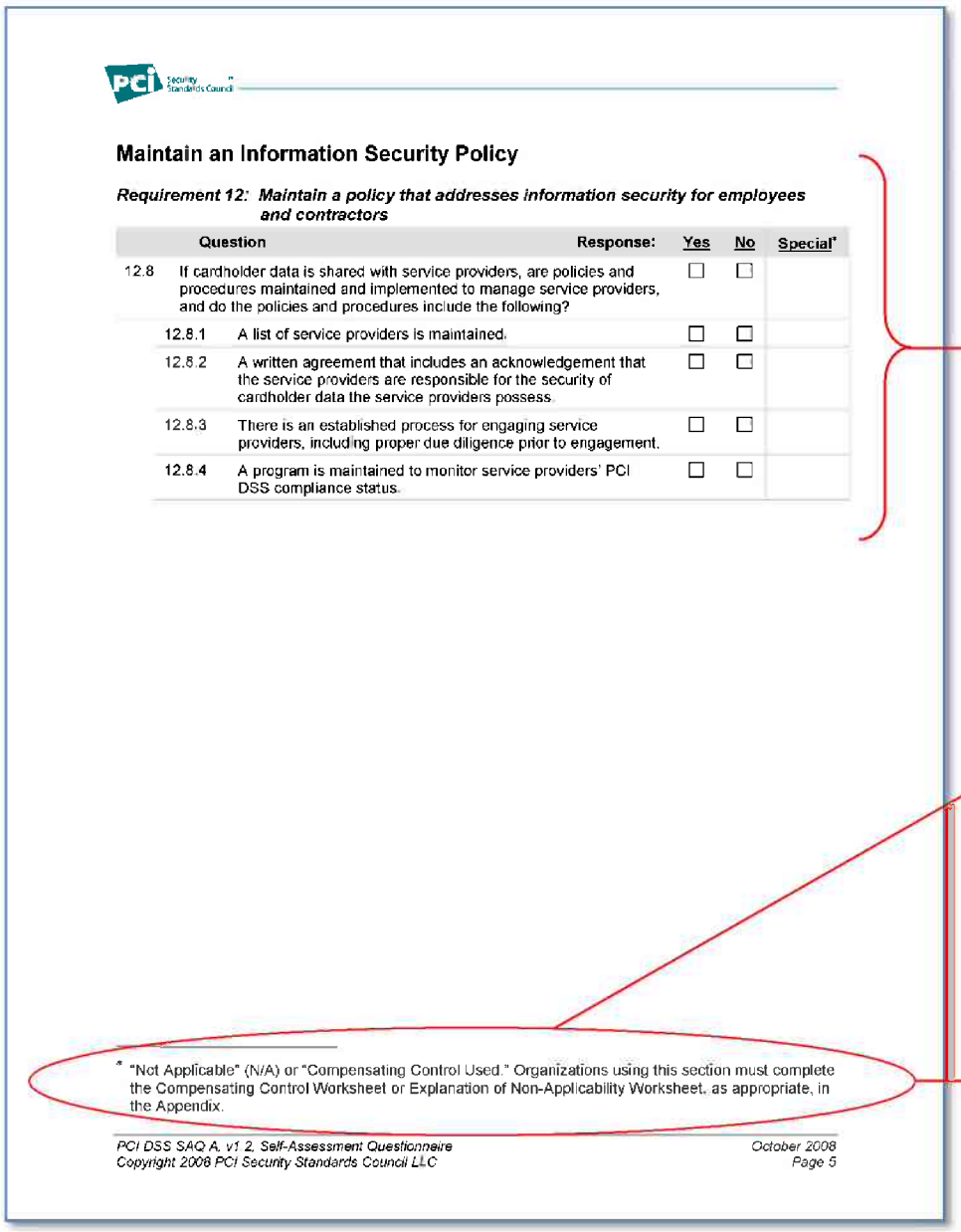
Requirement 9. In this section **ALL** questions and sub-questions must be answered with "Yes", "No", or in the Special column, with "N/A" for Not Applicable or with "Compensating Control Used".

If you enter "N/A" in the Special column you must complete Appendix D: Explanation of Non-Applicability for each question and sub-question.

If you enter "Compensating Control Used" in the Special column you must complete Appendix C: Compensating Controls Worksheet.

Appendix B: Compensating Controls explains what an acceptable compensating control is.

Self Assessment Questionnaire A (SAQ A)



PCI Security Standards Council

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

	Question	Response:	Yes	No	Special*
12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, and do the policies and procedures include the following?		☐	☐	
12.8.1	A list of service providers is maintained.		☐	☐	
12.8.2	A written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.		☐	☐	
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement.		☐	☐	
12.8.4	A program is maintained to monitor service providers' PCI DSS compliance status.		☐	☐	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS SAQ A, v1.2, Self-Assessment Questionnaire *October 2008*
Copyright 2008 PCI Security Standards Council LLC *Page 5*

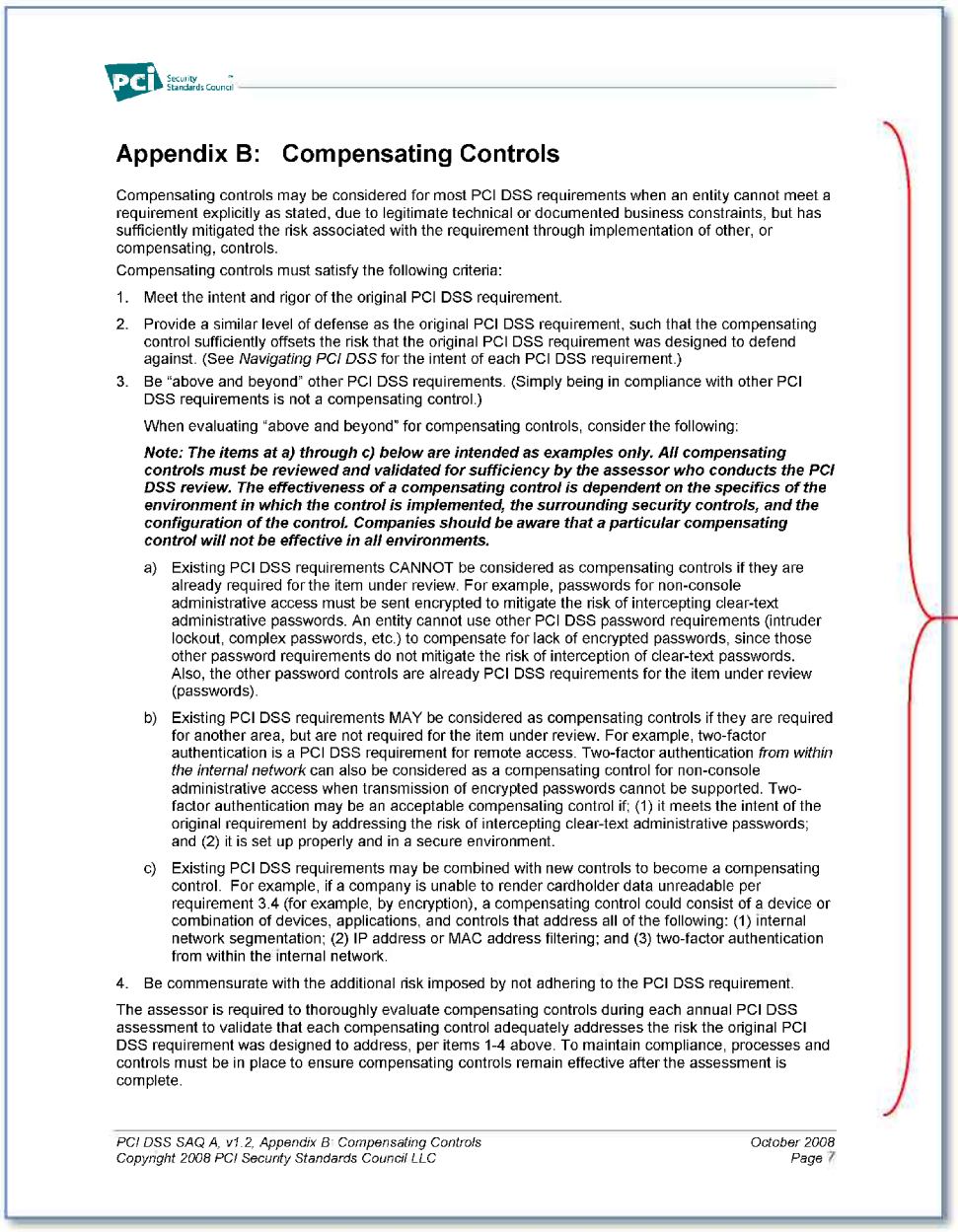
Requirement 12. In this section **ALL** questions and sub-questions must be answered with "Yes", "No", or in the Special column, with "N/A" for Not Applicable or with "Compensating Control Used".

If you enter "N/A" in the Special column you must complete Appendix D: Explanation of Non-Applicability for each question and sub-question.

If you enter "Compensating Control Used" in the Special column you must complete Appendix C: Compensating Controls Worksheet.

Appendix B: Compensating Controls defines what an acceptable compensating control is.

Self Assessment Questionnaire A (SAQ A)



PCI Security Standards Council

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

   Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

   b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if; (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.

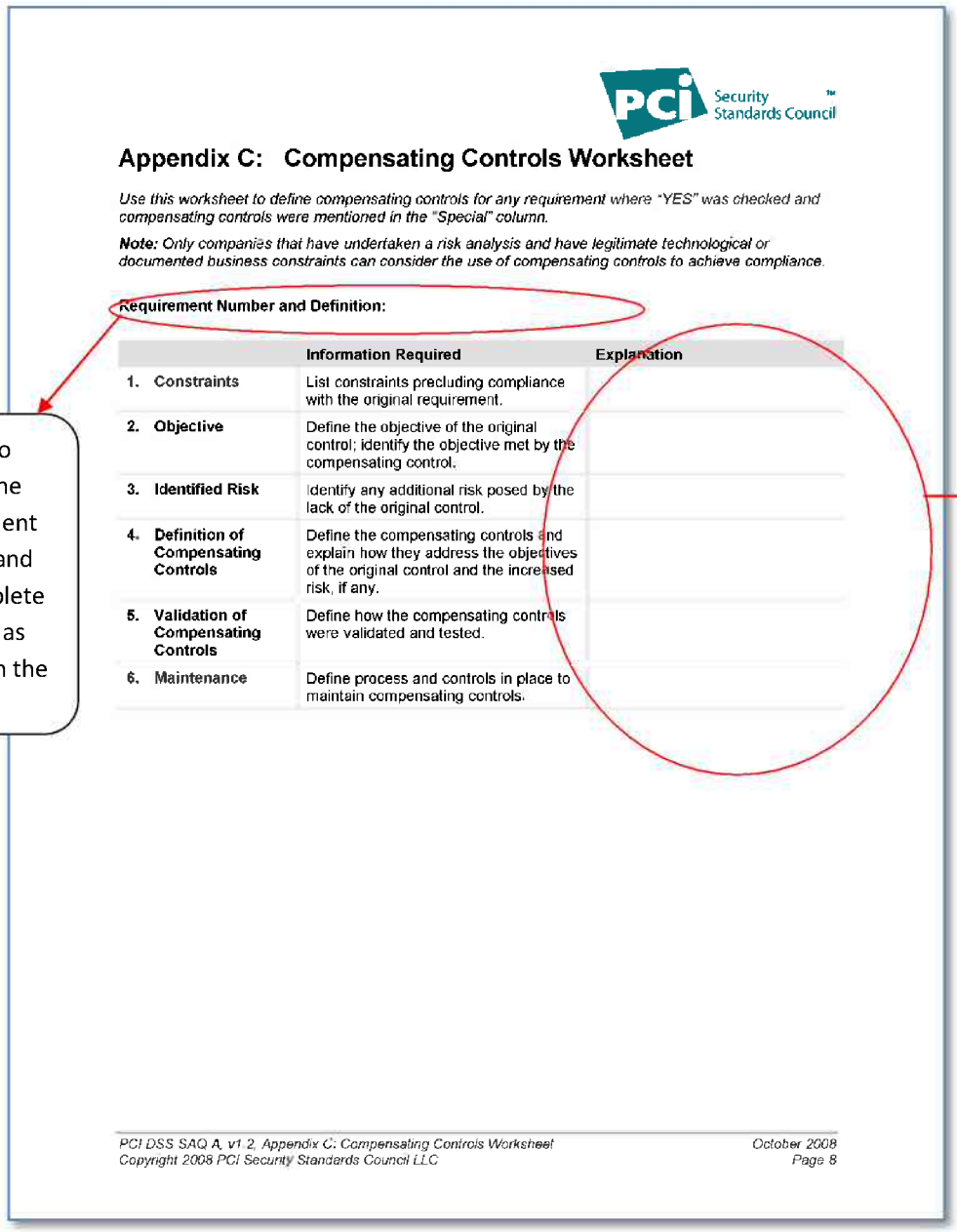
   c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix B is a must read for any company using compensating controls to secure credit card data instead of implementing the exact requirement and/or sub-requirement as defined in the questions of the SAQ.

Self Assessment Questionnaire A (SAQ A)



PCI Security Standards Council

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES" was checked and compensating controls were mentioned in the "Special" column.

***Note:** Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	Explanation
1. **Constraints**	List constraints precluding compliance with the original requirement.	
2. **Objective**	Define the objective of the original control; identify the objective met by the compensating control.	
3. **Identified Risk**	Identify any additional risk posed by the lack of the original control.	
4. **Definition of Compensating Controls**	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. **Validation of Compensating Controls**	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

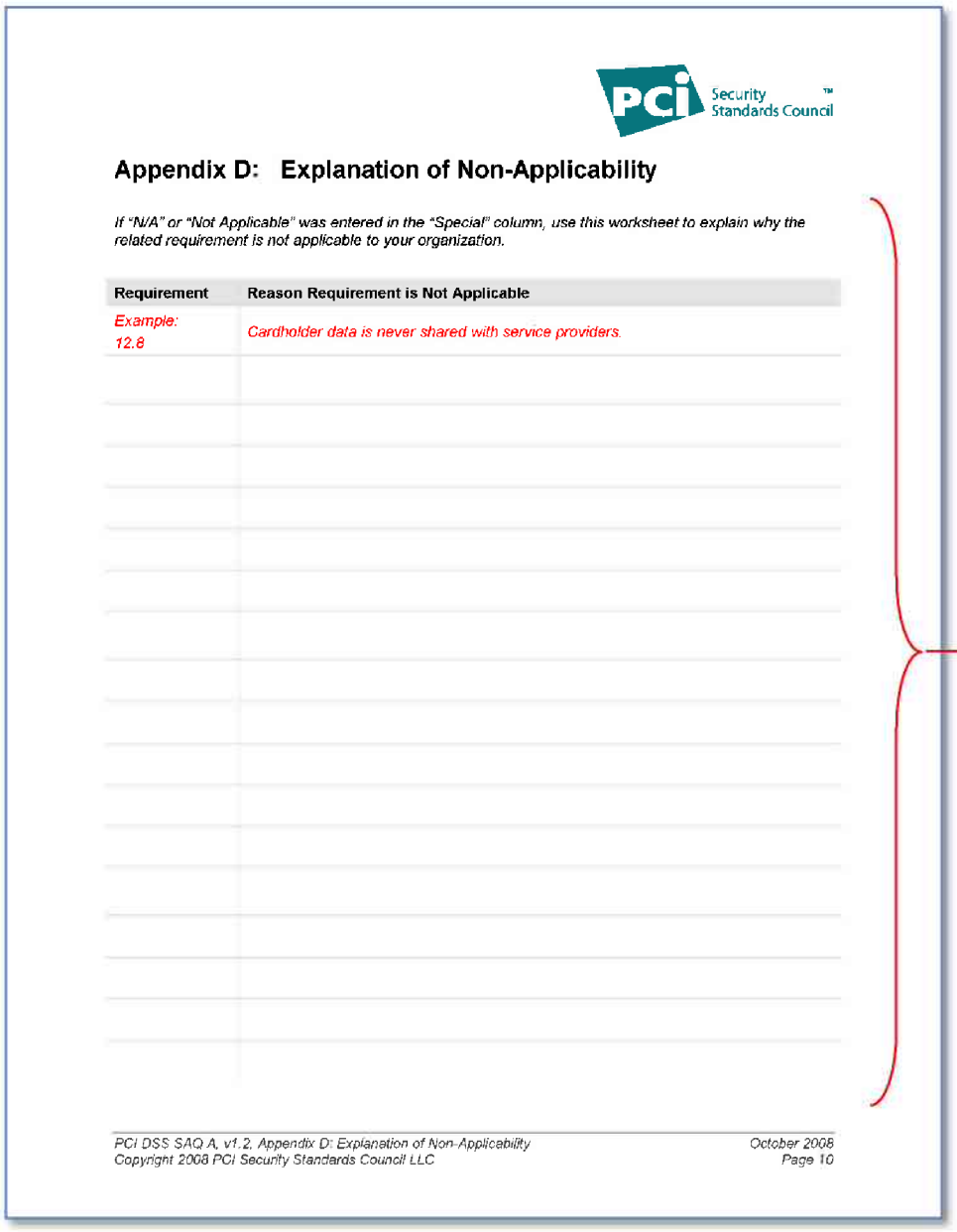
PCI DSS SAQ A, v1.2, Appendix C: Compensating Controls Worksheet *October 2008*
Copyright 2008 PCI Security Standards Council LLC *Page 8*

Be sure to include the requirement number and the complete question as shown on the SAQ.

Appendix C must be completed if you have indicated for any of the requirements or sub-requirements of the SAQ that you use compensating controls.

You must complete one worksheet for each requirement or sub-requirement for which you indicated you are using compensating controls.

Self Assessment Questionnaire A (SAQ A)



PCI Security Standards Council

Appendix D: Explanation of Non-Applicability

If "N/A" or "Not Applicable" was entered in the "Special" column, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example: 12.8	*Cardholder data is never shared with service providers.*

PCI DSS SAQ A, v1.2, Appendix D: Explanation of Non-Applicability *October 2008*
Copyright 2008 PCI Security Standards Council LLC *Page 10*

Appendix D must be completed if you indicated "N/A" for any of the requirements or sub-requirements of the SAQ. You must provide an explanation for each requirement and sub-requirement that you note as not applicable.