



Payment Card Industry (PCI) Qualified Security Assessors

Associate QSA Mentor Manual Template

Version 1.0

January 2018

Document Changes

Date	Version	Description
January 2018	1.0	This is the first release of the Associate QSA Mentor Manual Template.

TABLE OF CONTENTS

DOCUMENT CHANGES	2
1 INTRODUCTION	4
2 RELATED PUBLICATIONS	4
3 INSTRUCTIONS FOR USE	4
4 QSA COMPANY MENTOR PROGRAM OVERVIEW	7
4.1 DOCUMENT CONTROL/ANNUAL REVIEW	7
4.2 QSA COMPANY SUMMARY	7
4.3 ASSOCIATE QSA PROGRAM	8
APPENDIX A: AQSA-MENTOR ASSIGNMENT LOG	10
APPENDIX B: MENTOR RESPONSIBILITIES ACKNOWLEDGMENT FORM	11
APPENDIX C: AQSA SKILLS SUMMARY FORM	13
APPENDIX D: AQSA ENGAGEMENT SUMMARY	16
APPENDIX E: AQSA DEVELOPMENT TRACKING LOG	18

1 Introduction

The goal of the Associate QSA Program is to provide a path to enable QSA Companies to develop new resources into fully qualified QSA Employees, through formal mentorship and monitored skills development. Associate QSA Employees are qualified by PCI SSC to support QSA Employees on PCI DSS Assessments.

QSA Companies participating in the Associate QSA Program are required to implement and maintain a formal mentor program to support development of the Associate QSA Employee's assessment skills and techniques and provide numerous opportunities for discussing growth and setting new objectives. The mentor program must be documented in the QSA Company's Mentor Manual.

The *Associate QSA Mentor Manual Template* is provided by PCI SSC for use by a QSA Company in creating and maintaining the required Mentor Manual. This template is available on the Website, with an editable version available in the Portal.

The Primary Contact for the QSA Company is ultimately responsible for providing oversight of the mentor program to ensure the QSA Company's continued adherence to the QSA Requirements, including maintaining the Mentor Manual and performing associated audit activities.

Refer to the QSA Qualification Requirements and the QSA Program Guide on the Website for a full explanation of all requirements that must be adhered to when an eligible QSA Company participates in the Associate QSA (AQSA) Program.

2 Related Publications

This document should be reviewed in conjunction with other relevant PCI SSC publications, including but not limited to current publically available versions of the following, each available on the Website:

- *CPE Maintenance Guide*
- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures* ("PCI DSS")
- *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (the "Glossary")
- *PCI DSS Qualification Requirements for Qualified Security Assessors (QSAs)*
- *PCI DSS Template for Report on Compliance* ("ROC Reporting Template")
- *QSA Feedback Form*

3 Instructions for use

This document is the required template for the QSA Company's Mentor Manual and represents the minimum required content defined within the PCI DSS Qualification Requirements for Qualified Security Assessors (QSAs) for a mentor manual. Refer to the Portal for the most up-to-date version of this template in an editable format.

All sections of the template must be thoroughly and accurately completed, with sufficient detail to ensure the usefulness of the mentor manual for affected QSA employees.

Changes to the template are permitted as follows:

- Deletion of any content from the Associate QSA Mentor Manual Template is strictly prohibited.
- Minimal personalization changes, such as the addition of company logos, are allowed.
- Insertion of additional content is allowed, either by inserting additional rows or sections within the template or by adding appendices to the template. Please maintain the appendix numbering when making such additions.
- PCI SSC recognizes that QSA Companies may have implemented processes and/or technology for tracking mentor and/or training activities and that those processes and/or technologies may produce reporting consistent with some of the appendices of this document. Repurposing of such reporting to meet the intent of certain appendices is allowed only under the following conditions:
 - PCI SSC will allow alternate reporting documentation to be used to meet the intent for these appendices only:
 - *AQSA-Mentor Assignment Log* (Appendix A)
 - *AQSA Engagement Summary* (Appendix D)
 - *AQSA Development Tracking Log* (Appendix E)
 - The QSA Company must document the alternate reporting approach within Section 4 *QSA Company Mentor Program Overview* and provide supporting documentation for the approach as indicated (for example, a blank copy of the alternate reporting log).
 - The QSA Company is responsible for ensuring that the alternate reporting log includes all content required in the PCI SSC template.

The mentor manual content includes, but is not limited to, the following:

Document name:	Purpose:	Completed by and minimally reviewed:	Location:
<i>QSA Company Mentor Program Overview</i>	For recording QSAC-specific content such as contingency plan(s) for when mentors leave, internal audit processes	To be completed/maintained by the Primary Contact or formal designee at least once every 365 days	QSA Company Mentor Manual (Section 4 <i>QSA Company Mentor Program Overview</i>)
<i>AQSA-Mentor Assignment Log</i>	For documenting assignments of eligible mentor QSA Employees to Associate QSA Employees	To be completed/maintained by the Primary Contact or formal designee at least once every 30 days	QSA Company Mentor Manual (Appendix A)

Document name:	Purpose:	Completed by and minimally reviewed:	Location:
<i>Mentor Responsibilities Acknowledgment Form</i>	For acknowledgment of Mentor Responsibilities by Mentor QSA. Includes acknowledgment of completion of mentor training module.	To be signed by the mentor before starting mentor responsibilities and updated with the onboarding of each Associate QSA Employee	QSA Company Mentor Manual (Appendix B) Executed forms are retained with the <i>AQSA-Mentor Assignment Log</i>
<i>AQSA Skills Summary Form</i>	To ensure the Lead QSA with whom the Associate QSA Employee is working on a PCI DSS Assessment understands the level of expertise the Associate QSA Employee possesses	To be completed at onboarding with the Mentor and Associate QSA Employee and updated at least once every 90 days to reflect the Associate QSA Employee's quarterly progress	QSA Company Mentor Manual (Appendix C) Executed forms are retained by the Lead QSA as part of Workpaper Retention, as well as by the AQSA.
<i>AQSA Engagement Summary</i>	To allow the Lead QSA with whom the Associate QSA Employee is working on a PCI DSS Assessment to acknowledge receipt and review of the most current <i>AQSA Skills Summary Form</i> , assign any tasks to the Associate QSA, and provide the Associate QSA with feedback and/or opportunities for improvement	To be completed by the Lead QSA; The Lead QSA must update the summary with feedback and/or opportunities for improvement and return the completed <i>AQSA Engagement Summary</i> to the Associate QSA Employee within 30 days of the assigned tasks being completed.	QSA Company Mentor Manual (Appendix D) Executed forms are retained by the Lead QSA as part of Workpaper Retention, as well as by the AQSA.
<i>AQSA Development Tracking Log</i>	For self-tracking PCI DSS Assessment work, learning opportunities, CPEs, etc.	To be completed/maintained by the Associate QSA Employee at least once every 30 days	QSA Company Mentor Manual (Appendix E) Retained by AQSA.

4 QSA Company Mentor Program Overview

4.1 Document Control/Annual Review

The QSA Company Mentor Program Overview is to be completed/maintained by the Primary Contact or formal designee at least once every 365 days. Use this table for revision management and to document annual review.

Note: This section only needs to be updated to reflect changes to Section 4 QSA Company Mentor Program Overview of the QSA Company Mentor Manual. This section does not need to be updated to reflect changes or additions to the appendices and executed appendices for which retention in the QSA Company Mentor Manual is required.

Name	Date	Description

4.2 QSA Company Summary

QSA Company	
▪ Company name:	
▪ Company address:	
▪ Company website:	
▪ Date QSA Company initially began participating in the AQSA Program	

QSA Primary Contact							
▪ Contact name:							
▪ Contact email::							
▪ Has the Primary Contact delegated any required AQSA monitoring tasks to a formal designee?	<input type="checkbox"/> Yes <input type="checkbox"/> No If 'yes,' explain below. Note: The Primary Contact for the QSA Company is ultimately responsible for providing oversight of the mentor program to ensure the QSA Company's continued adherence to the QSA Requirements, including maintaining the Mentor Manual and performing associated audit activities.						
	<table> <tr> <th>Name of Formal Designee</th><th>Assigned monitoring tasks</th></tr> <tr> <td></td><td></td></tr> <tr> <td></td><td></td></tr> </table>	Name of Formal Designee	Assigned monitoring tasks				
Name of Formal Designee	Assigned monitoring tasks						

4.3 Associate QSA Program

The goal of the Associate QSA Program is to provide a path to enable QSA Companies to develop new resources into fully qualified QSA Employees, through formal mentorship and monitored skills development. In support of that, ensure responses are specific and relevant to the QSA Company and Associate QSA. Responses must focus on concise quality of detail rather than generic language.

For each of the following Associate QSA Program requirements, describe the process and/or methods the QSA Company has defined to ensure program requirements are adhered to:

The QSA Company must inform the applicable Customer when an Associate QSA Employee has been assigned to work in connection with the PCI DSS Assessment of that Customer, and what parts of the PCI DSS Assessment the Associate QSA Employee will be participating in.	
The QSA Company is expected to arrange sufficient back-up of Assessor-Employee resources so as not to impact a Customer's validation deadlines in the event an assigned Assessor-Employee is unable to complete a PCI DSS Assessment.	
Monitoring tasks and/or associated audit activities performed by the Primary Contact or formal designee to ensure the QSA Company's continued adherence to the QSA Requirements for the Associate QSA Program supported by Assessor-Employee roles, as follows:	
The Associate QSA Employee's on-going completion, retention and delivery to relevant parties of the <i>AQSA Skills Summary</i> , <i>AQSA Engagement Summary</i> and <i>AQSA Development Tracking Log</i> .	
<p>The Lead QSA's completion and retention of the <i>AQSA Engagement Summary</i> in the workpapers for each PCI DSS Assessment.</p> <p>Note: if more than one AQSA is assisting on a PCI DSS Assessment, an AQSA Engagement Summary must be completed for each Associate QSA Employee. Similarly, the Lead QSA must complete an AQSA Engagement Summary for each separate PCI DSS Assessment if working with an Associate QSA Employee on multiple PCI DSS Assessments.</p>	
The Mentor's on-going guidance and development to each Associate QSA Employee assigned to them.	

AQSA-Mentor Assignment

How are mentors identified before the application for an Associate QSA is submitted to PCI SSC?	
Describe contingency plan(s) for when a Mentor withdraws from the QSA Company's mentor program	
Note:	

<ul style="list-style-type: none"> ○ If a Mentor withdraws from the QSA Company's Mentor program, affected Associate QSA Employees must be reassigned to another Mentor <i>within 90 days</i>. ○ The QSA Company must notify the QSA Program Manager via email if Associate QSA Employees cannot be reassigned to an eligible mentor <i>within 90 days</i>. ○ A QSA Company must have at least one QSA Employee at all times. If a QSA Company has only Associate QSAs, contact the QSA Program Manager <i>immediately</i> via email. 	
Additional comments	

Existing Processes/Technology for Tracking Mentor and/or Training Activities		
Does the QSA Company currently implement processes and/or technologies for mentor and/or training activities that will be utilized to support the mentoring of Associate QSAs?		<input type="checkbox"/> Yes <input type="checkbox"/> No If 'no,' mark the remainder of this section as 'not applicable.'
If yes, will the QSA Company be repurposing resulting reporting for eligible appendices?		<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Applicable If 'yes,' complete the table below and include a blank copy/sample of the alternate reporting log within the corresponding appendix.
Eligible appendices:	Repurposed reporting?	Description of how intent of appendix is met by the repurposed reporting:
AQSA-Mentor Assignment Log (Appendix A)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Applicable	
AQSA Engagement Summary (Appendix D)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Applicable	
AQSA Development Tracking Log (Appendix E)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Applicable	

Appendix A: AQSA-Mentor Assignment Log

The *AQSA-Mentor Assignment Log* is for documenting assignments of eligible mentor QSAs to Associate QSA Employees and is to be completed/maintained by the Primary Contact or formal designee at least once every 30 days. With this log, the QSA Company should retain all corresponding executed copies of the Mentor Responsibilities Acknowledgment Form.

Note: a QSA Company must have at least one QSA Employee at all times. If a QSA Company has only Associate QSAs, contact the QSA Program Manager immediately via email. If a Mentor withdraws from the QSA Company's Mentor program, affected Associate QSAs must be reassigned to another Mentor within 90 days. Notify the QSA Program Manager via email if Associate QSAs cannot be reassigned within 90 days.

Complete the below table **for each Associate QSA** at certification (duplicate table as necessary, including additional rows for subsequently assigned Mentor QSAs as needed):

Associate QSA Mentor Assignment			
Associate QSA Name:			
Mentor QSA Information (assigned immediately upon Associate QSA certification)			
Mentor QSA Name:			
Start date of mentoring:		End date:	
Has the executed Mentor Responsibilities Acknowledgement Form that includes this assignment been retained with this log in the QSA Company Mentor Manual?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Subsequent Assignment Mentor QSA Information (if applicable)			
Mentor QSA Name:			
Start date of mentoring:		End date:	
Has the executed Mentor Responsibilities Acknowledgement Form that includes this assignment been retained with this log in the QSA Company Mentor Manual?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Subsequent Assignment Mentor QSA Information (if applicable)			
Mentor QSA Name:			
Start date of mentoring:		End date:	
Has the executed Mentor Responsibilities Acknowledgement Form that includes this assignment been retained with this log in the QSA Company Mentor Manual?		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Appendix B: Mentor Responsibilities Acknowledgment Form

The *Mentor Responsibilities Acknowledgment Form* must be signed by the mentor before starting mentor responsibilities and updated with the onboarding of each Associate QSA Employee; executed forms should be retained in the QSA Company Mentor Manual within the *AQSA-Mentor Assignment Log* (Appendix A).

Refer to Section 3.3.3 of the *QSA Qualification Requirements* for Mentor Requirements. Additionally, consider that a mentor's role in supporting the development of mentees requires a commitment in time and resources. The Associate QSA relies on their mentor to share experience, help set goals, give honest feedback in a supportive manner and remain accessible, committed and engaged in the process of developing the Associate QSA's skills.

Company Information			
Company Name:			
Mentor QSA Information			
Name:		Job Title:	
Telephone:		E-mail:	
Date of Mentor's completion of mentor training module			

Assigned Associate QSA Mentees (no more than three (3) Associate QSAs at one time):			
Associate QSA Name:			
Start date of mentoring:		End date:	
Associate QSA Name:			
Start date of mentoring:		End date:	
Associate QSA Name:			
Start date of mentoring:		End date:	
Associate QSA Name:			
Start date of mentoring:		End date:	
Associate QSA Name:			
Start date of mentoring:		End date:	

Signature

By signing below, I hereby acknowledge and agree that:

- (a) The information provided above is true, accurate and complete;
- (b) I have read and understand the Mentor Responsibilities as defined in Section 3.3.3 of the QSA Qualification Requirements and will comply with the terms thereof; and
- (c) I have completed the requisite mentor training module required by PCI SSC

Mentor Name:		Title:	
Mentor signature ↑		Date ↑	

Appendix C: AQSA Skills Summary Form

The *AQSA Skills Summary Form* is to be completed at onboarding with the Mentor and Associate QSA Employee and updated together at least once every 90 days to reflect the Associate QSA Employee's quarterly progress. Retained by the Associate QSA Employee, a current copy must be provided to any Lead QSA with whom the Associate QSA Employee is working on a PCI DSS Assessment.

The purpose of the *AQSA Skills Summary Form* is to ensure that any Lead QSA working with an Associate QSA understands the level of expertise the Associate QSA possesses. This prepares the Lead QSA to assign tasks appropriately and supports the on-going development of the Associate QSA's skills.

This form's structure aligns with the QSA Employee Application to support the Associate QSA's path to qualification as a QSA.

Associate QSA Employee			
Name:		Job Title:	
Telephone:		E-mail:	
Current Mentor QSA			
Name:		Job Title:	
Telephone:		E-mail:	
Initial completion at on-boarding			
Name of Mentor QSA:		Date:	
Subsequent review/update (at least once every 90 days)			
Name of Mentor QSA:		Date:	
Name of Mentor QSA:		Date:	
Name of Mentor QSA:		Date:	

Associate QSA Employee Skills, Experience and Education
Provide description and examples of the Candidate's initial educational and/or experience in the following areas of expertise, as well as description and examples of subsequent experience and relevant skills development. Insert additional rows as needed.

Description of education related to **information security** at on-boarding:

From (date):	To (date):	Total time: Years	Months
--------------	------------	-------------------	--------

Examples of work and/or description of experience in **information security** at on-boarding:

From (date):	To (date):	Total time: Years	Months
--------------	------------	-------------------	--------

Description of subsequent education, work, and/or experience related to information security :	
Date:	Description:
Date:	Description:

Description of education related to **information technology** at on-boarding:

From (date):	To (date):	Total time: Years	Months
--------------	------------	-------------------	--------

Examples of work and/or description of experience in **information technology** at on-boarding:

From (date):	To (date):	Total time: Years	Months
--------------	------------	-------------------	--------

Description of **subsequent** education, work, and/or experience related to **information technology**:

Date:	Description:
Date:	Description:

Examples of work and/or description of experience in **network security** (for example, administration of firewalls, intrusion prevention systems, etc.) at on-boarding:

From (date):	To (date):	Total time: Years	Months
--------------	------------	-------------------	--------

Description of **subsequent** education, work, and/or experience related to **network security**:

Date:	Description:
Date:	Description:

Examples of work and/or description of experience in **application security** at on-boarding:

From (date):	To (date):	Total time: Years	Months
--------------	------------	-------------------	--------

Description of **subsequent** education, work, and/or experience related to **application security**:

Date:	Description:
Date:	Description:

Examples of work and/or description of experience in **systems integration and security** at on-boarding:

From (date):	To (date):	Total time: Years	Months
--------------	------------	-------------------	--------

Description of **subsequent** education, work, and/or experience related to **systems integration and security**:

Date:	Description:
Date:	Description:

Examples of work and/or description of experience in **auditing information systems and processes** at on-boarding:

From (date):	To (date):	Total time: Years	Months
Description of subsequent education, work, and/or experience related to auditing information systems and processes :			
Date:	Description:		
Date:	Description:		

Examples of work and/or description of experience in **information security risk assessment or risk management** at on-boarding:

From (date):	To (date):	Total time: Years	Months
Description of subsequent education, work, and/or experience related to information security risk assessment or risk management :			
Date:	Description:		
Date:	Description:		

Professional Certifications (check all that apply):

<input type="checkbox"/> (ISC) ² CISSP	Certification number:	Expiry date:
<input type="checkbox"/> ISACA CISM	Certification number:	Expiry date:
<input type="checkbox"/> ISACA CISA	Certification number:	Expiry date:
<input type="checkbox"/> SANS GIAC/GSNA	Certification number:	Expiry date:
<input type="checkbox"/> IRCA Auditor	Certification number:	Expiry date:
<input type="checkbox"/> IIA CIA	Certification number:	Expiry date:
<input type="checkbox"/> ISO 27001, Lead Auditor/Implementer, Internal Auditor	Certification number: Accredited certification body:	Date achieved:

Associate QSA Employee – Goals

Based on the information provided above as well as growth planning with the Mentor QSA, the following goal(s) have been identified as priorities for learning: (add rows as needed)

Description of **short-term** goal and/or learning priority:

Date:	Milestone achieved/progress made:
-------	-----------------------------------

Description of **long-term** goal and/or learning priority:

Date:	Milestone achieved/progress made:
-------	-----------------------------------

Appendix D: AQSA Engagement Summary

The *AQSA Engagement Summary* is to be completed by the Lead QSA with whom the Associate QSA Employee is working on a PCI DSS Assessment; Lead QSA must also retain a copy of the completed *AQSA Engagement Summary* as part of the PCI DSS Assessment workpapers. If more than one Associate QSA is contributing to the assessment, an AQSA Engagement Summary must be completed for each Associate QSA Employee. Similarly, the Lead QSA must complete an AQSA Engagement Summary for each separate PCI DSS engagement if working with an Associate QSA Employee on multiple engagements.

Additionally, a copy of the completed *AQSA Engagement Summary* should be retained by the Associate QSA Employee for every PCI DSS Assessment the Associate QSA Employee completed tasks for; Associate QSA Employee is responsible for providing the summary to the Mentor QSA at least once every 90 days for use when updating the *AQSA Skills Summary Form*

The QSA Company must inform the applicable Customer when an Associate QSA Employee has been assigned to work in connection with the PCI DSS Assessment of that Customer, and what parts of the PCI DSS Assessment the Associate QSA Employee will be participating in. The QSA Employee leading a PCI DSS Assessment (the “Lead QSA”) and providing supervision to an Associate QSA Employee:

1. Is responsible for understanding the level of expertise of the Associate QSA Employee and their ability to perform any assigned part of the assessment independently.
2. Is responsible to review all notes and/or evidence collected by the Associate QSA Employee
3. Is responsible to make the actual compliance determination.

Associate QSA Employee			
Name:		Email:	
Lead QSA			
Name:		Email:	
Did the Lead QSA receive and review the most current <i>AQSA Skills Summary</i> from the Associate QSA?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
PCI DSS Customer Information			
Customer Name:		Date:	

The Lead QSA must assign any tasks to the Associate QSA Employee using this form. The Lead QSA must update the summary with feedback and/or opportunities for improvement and return the completed *AQSA Engagement Summary* to the Associate QSA Employee within 30 days of the assigned tasks being completed.

	Tasks Assigned to Associate QSA (add rows as needed)	Due Date	Status of Task	Feedback and/or Opportunities for Improvement from Lead QSA
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Note: PCI SSC does not qualify Associate QSA Employees to support any standard other than the PCI DSS.

An Associate QSA Employee is restricted from performing the following duties:

- Leading a PCI DSS assessment
- Confirming PCI DSS compliance to Customers
- Signing AOCs
- Validating the scope of a PCI DSS assessment.
- Selection of systems and systems components where sampling is used
- Evaluating compensating control
- Initiating and leading compliance discussions with payment brands or acquirers

Appendix E: AQSA Development Tracking Log

The *AQSA Development Tracking Log* for self-tracking PCI DSS Assessment work, learning opportunities, CPEs, etc. and is to be completed/maintained by the Associate QSA Employee at least once every 30 days This log is to be retained by the AQSA, who must provide executed log to the Mentor QSA for use when updating the AQSA Skills Summary Form at least once every 90 days

- In order to remain “in Good Standing,” all Assessor-Employees must provide proof of information systems audit training within the last 12 months of the requalification date in accordance with the current version of the *PCI SSC CPE Maintenance Guide*.
- An Assessor-Employee must also earn a minimum of 20 CPE credits per year and a minimum of 120 CPE credits per rolling three-year period.

Year	Title or Name of Program Course	Location	Type of CPE * or learning opportunity	Start Date	End Date	Total	Annual Total
ONE							0
TWO							0

THREE							0
			* Type of CPE Earned should indicate how the CPE was attained, i.e., Authored a published document, Attended a training class, Presented at a conference, etc.		3-Year Running Total:		0