Payment Card Industry (PCI)

Qualification Requirements

For Internal Security Assessors (ISA)

Version 2.0

April 2015

Document Changes

Date	Version	Description
November 2012	1.2	Minor administrative revisions
April 2015	2.0	▪ Various minor clarifications and grammar improvements ▪ Terminology aligned with PCI DSS v3.0 ▪ Clarification that Payment Brands determine whether an ISA can validate their Sponsor Company's compliance ▪ Clarification that an individual's ISA qualification applies only for their Sponsor Company, and not for any other organization ▪ Clarification that the scope of function as an ISA is limited to business units internal to the ISA's Sponsor Company ▪ Processes updated to reflect Attestation acceptance and other program features moved to the Portal ▪ Addition of the PCI SSC Code of Professional Responsibility ▪ Clarification of recommended ISA experience

1 Introduction

The PCI SSC Internal Security Assessor Program ("ISA Program") provides an opportunity for employees of qualifying organizations to receive PCI DSS training and qualification, to improve the organization's understanding of the PCI DSS, facilitate the organization's interactions with QSAs, enhance the quality, reliability, and consistency of the organization's internal PCI DSS self-assessments, and support the consistent and proper application of PCI DSS measures and controls. Capitalized terms used herein and not otherwise defined shall have the meanings set forth in Section 4.

The ISA Qualification Requirements document should be used in conjunction with the following other PCI SSC publication(s), each available through the Website:

- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures* (defined in Section 4)
- *PCI SSC Code of Professional Responsibility*

1.1 Qualification Process Overview

This document describes the conditions under which an eligible organization or individual may qualify to participate in the ISA Program as a "Sponsor Company" or "ISA" (as applicable).

The qualification process involves the following three primary steps (described further below):

1. Sponsor Company Qualification: The candidate organization must apply for qualification as a Sponsor Company. Application requires submission of a complete Sponsor Company Application Package (defined in Section 1.2.1 below), including executed Sponsor Attestation. Sponsor Company qualification occurs once the above have been processed and the applicant has been notified by PCI SSC.
2. ISA Qualification: The process whereby employees of Sponsor Companies may be trained, tested and ultimately qualified as PCI SSC-approved "Internal Security Assessors" or "ISAs." Successful ISA qualification requires application on behalf of the ISA candidate by its supporting Sponsor Company employer (by submitting a training request through the Portal), payment of applicable ISA Program training fees by the Sponsor Company (see Website for ISA Program Fees), successful completion of applicable ISA training and examinations, and the ISA candidate accepting the ISA Attestation as part of the exam.
3. Annual Re-Qualification and Good Standing: In order to maintain "Good Standing," a Sponsor Company must satisfy the requirements set forth in Section 2.2, including but not limited to annual renewal of its Sponsor Attestation and payment of applicable ISA training fees. In order to maintain "Good Standing," an ISA must satisfy the requirements set forth in Section 3.3, including but not limited to successful completion of all required ISA requalification training and exams.

IMPORTANT:

Any full-time employee of a Sponsor Company may be qualified as an ISA by successfully completing all required training and examinations and satisfying all other ISA requirements. Nonetheless, due to the technical nature of the training materials and in order to help increase the efficiency of ISA training sessions, PCI SSC generally recommends that ISA candidates possess the ISA experience described in Section 3.4 below. Individuals with significantly less experience or who are looking for a more general overview of the PCI DSS may wish to consider a different PCI SSC training program.

ISA qualification signifies only that an individual has met all applicable ISA requirements as set forth in the ISA Qualification Requirements document, including successful completion of required ISA Program training and passing all required ISA Program examinations. ISA qualification may not entitle an ISA to perform special functions or conduct PCI DSS Assessments; whether a Sponsor Company can use an ISA for its own compliance validation for a given payment card brand is determined by that payment card brand.

ISA qualification is not transportable, and qualification as an ISA or Sponsor Company is not assignable or transferable. An individual's ISA qualification applies only for their Sponsor Company (and not for any other organization), and only while that individual remains employed by the Sponsor Company that employed him or her when initially qualified as an ISA (the "Initiating Sponsor Company"). Additionally, qualification as an ISA only permits an ISA to perform PCI DSS Assessments of his or her Initiating Sponsor Company, and again, whether a Sponsor Company can use an ISA for its own compliance validation for a given payment card brand is determined by that payment card brand. Individual ISA qualification immediately and automatically terminates upon interruption of employment with the Initiating Sponsor Company or any other failure to comply with the requirements of or satisfy the eligibility requirements of the ISA Program. Except as otherwise specified herein, an individual who loses ISA qualification and later satisfies applicable requirements may reapply for ISA qualification at any time.

1.2 Application Process

1.2.1 Sponsor Company Application

ISA Company registration is accessed through the ISA Training page on the Website. After the candidate submits its company and contact information, the ISA Program Manager will provide access to the Portal. The candidate can then log into the Portal to complete its application submittal.

The candidate Sponsor Company must submit the following materials (collectively, a "Sponsor Company Application Package") to PCI SSC in order to apply for initial qualification as a Sponsor Company:

a) Sponsor Attestation, executed by a duly authorized executive officer of the candidate Sponsor Company, attesting to the matters set forth therein;

b) Training request for each ISA candidate for whom the Sponsor Company is seeking ISA qualification; and

c) Copy of current company formation document or equivalent approved by PCI SSC (the "Business License") including year of incorporation and location(s) of offices. (Refer to the

Document Library on the Website—Business License Requirements—for more information.)

d) To facilitate preparation of the Sponsor Company Application Package, please refer to Appendix C.

1.2.2 Initial Sponsor Company Qualification

PCI SSC will notify the Sponsor Company candidate in writing if it has been qualified. A successful Sponsor Company applicant is considered qualified as a Sponsor Company for a period of one (1) year from the date of its initial qualification, subject to continued satisfaction of applicable Sponsor Company Requirements.

1.2.3 ISA Application and Qualification

A Sponsor Company in Good Standing may apply to qualify any of its full-time employees as an ISA at any time by submitting to PCI SSC (on behalf of its ISA candidate) an ISA training request through the Portal. This submission can occur in connection with the Sponsor Company's initial qualification or thereafter. Once the ISA training request has been received and approved by PCI SSC, the individual is eligible to receive ISA training and qualification as described further herein. ISA candidates who successfully complete training and related examinations are considered qualified as ISAs for a period of one (1) year from the date of initial ISA qualification, subject to continued satisfaction of all other applicable qualification requirements by the ISA and its Initiating Sponsor Company.

***IMPORTANT**: PCI SSC will notify candidate Sponsor Companies that do not meet applicable requirements or otherwise fail to qualify, and all such candidates may appeal within 30 days from the date of notification. Appeals must be addressed to the PCI SSC General Manager and will follow applicable procedures as determined by PCI SSC.*

PCI SSC reserves the right to reject any applicant (ISA or Sponsor Company) if PCI SSC determines in its discretion, or has reason to believe, that the applicant fails to satisfy applicable ISA Program requirements or has, within two (2) years prior to the application date, engaged in any conduct that would have entitled PCI SSC to revoke qualification.

1.2.4 Delivery Instructions

Sponsor Company Application Packages and all other materials required hereunder must be submitted in English, include all required documentation, and be submitted via the Portal. Contact the ISA Program Manager at isa@pcisecuritystandards.org for questions or requests for Portal access.

1.3 Requests for Additional Information

PCI SSC reserves the right to require Sponsor Companies or ISAs to provide additional documentation or information in order to confirm adherence to the ISA Qualification Requirements, Sponsor Attestation, and/or any other requirements of the ISA Program. All such additional documentation and information must be submitted in English or with a certified English translation. Responses must be received by PCI SSC no later than three (3) weeks from the date of the corresponding PCI SSC request. Failure to timely respond may result in disqualification or other action by PCI SSC.

2 Sponsor Company Qualification

This section describes ISA Program requirements for Sponsor Companies. Subsections address Initial Sponsor Company Qualification Requirements, Sponsor Company Good Standing and Annual Re-qualification Requirements, ISA Program Fees and Sponsor Attestations.

2.1 Initial Sponsor Company Qualification Requirements

In order for an organization to be initially qualified as a Sponsor Company, the organization must satisfy the following basic eligibility requirements ("Sponsor Company Eligibility Requirements"):

a) The organization must be a legal entity (not an individual) and provide to PCI SSC a copy of the organization's business license (or equivalent), year of organization and location(s) of office(s);

b) The organization must be a merchant, processor, service provider or other organization required to comply with the PCI DSS;

c) The organization must process credit, debit or other payment transactions with members of the general public;

d) The organization must have a dedicated internal audit department, group or division;

e) The organization must execute and deliver to PCI SSC a completed Sponsor Company Application Package; and

f) The organization must either (i) not be, and not have any Affiliate, division, department or unit that is a QSA, an Approved Scanning Vendor (ASV), an ASV Test Lab, or any other entity engaged in the business of offering services to any third party for purposes of establishing or achieving compliance with any PCI SSC standard (each such QSA, ASV, ASV Test Lab and other entity, a "PCI Standards Assessor") or (ii) if the organization has one or more divisions, subsidiaries or Affiliates that function as a PCI Standards Assessor: (A) ensure at all times that the Sponsor Company and ISA activities, functions, personnel, management, decision-making and operations of the organization ("ISA Functions and Decision-Making") are sufficiently separate and independent from the activities, functions, personnel, management, decision-making and operations of such PCI Standards Assessors to avoid all conflicts of interest between such PCI Standards Assessors and such ISA Functions and Decision-Making, and (B) take all reasonable steps to avoid any such conflicts of interest and any undue influence of such PCI Standards Assessors on such ISA Functions and Decision-Making. For purposes hereof, "Affiliate" means, with respect to a given organization, any separate legal entity that directly or indirectly controls, is controlled by, or is under common control with such organization; and the term "control" (and each derivate thereof) means the direct or indirect beneficial ownership, right to exercise a majority of the voting power, or power to direct the activities or operations of, such separate legal entity.

2.2 Sponsor Company Good Standing and Annual Re-qualification Requirements

An organization is deemed to be in "Good Standing" as a Sponsor Company as long as the following requirements ("Sponsor Company Good Standing Requirements") are satisfied:

a) The organization is initially qualified by PCI SSC as a Sponsor Company and continues to satisfy all Sponsor Company Eligibility Requirements;

b) The organization complies with the terms of its Sponsor Attestation;

c) To the extent that the Sponsor Company and any of its ISA Employees wish to renew that ISA Employee's certification, the organization submits to PCI SSC, within thirty (30) days prior to that individual ISA's certification expiration date (as indicated by the PCI SSC notification to the Sponsor Company that it has been qualified as a Sponsor Company), a request to enroll that ISA employee in requalification training[1]; and

d) The organization pays all applicable ISA Program Fees in the manner described in the ISA Qualification Requirements document or as otherwise required by PCI SSC.

Note: *A Sponsor Company may still be in Good Standing even if they have no ISAs on staff; failure to have an ISA on staff alone does not impact Good Standing status as long as the Sponsor Company continues to satisfy all Sponsor Company Eligibility Requirements.*

2.3 ISA Program Fees

The following fees must be paid by the applicable Sponsor Company in order for that Sponsor Company and its ISAs to participate in the ISA Program:

- Initial ISA Training Fee for each ISA candidate, which must be paid in full[2] for each ISA candidate prior to the applicable initial ISA training session in which that candidate will participate; and
- Annual ISA Re-qualification Training Fee for each re-qualifying ISA must be paid in full for each ISA prior to the applicable annual ISA re-qualification training session in which that ISA will participate.

[1] Where training instruction is provided by an authorized third party, all ISA sponsorship paperwork must be fully submitted and approved by PCI SSC and all ISA candidate pre-requisite coursework and examinations (for example, PCI Fundamentals) satisfactorily completed prior to the ISA candidate being permitted to attend or otherwise obtain ISA instruction from an authorized third-party training delivery provider.

[2] Where training is obtained from a PGTN Provider via the PCI Global Training Network (PGTN) or from any other PCI SSC-authorized third-party provider, payment terms must be satisfied with the provider prior to training instruction.

All fees associated with the ISA Program as specified on the Website—*PCI SSC Programs Fee Schedule* (collectively, "ISA Program Fees")—are non-refundable and are subject to change upon posting of revised fees by PCI SSC.

2.4 Sponsor Attestation

Each candidate Sponsor Company must submit to PCI SSC, as part of its completed Sponsor Company Application Package, a Sponsor Attestation in unmodified form, accepted by a duly authorized executive officer of the candidate Sponsor Company, attesting and agreeing to the matters set forth therein. Sponsor Companies must annually re-accept a Sponsor Attestation via the Portal on an annual basis in order to re-qualify as a Sponsor Company.

3 ISA Qualification

This section describes ISA Program Requirements for ISAs. Subsections address ISA Eligibility Requirements, ISA Good Standing Requirements, and Recommended ISA Experience. While a Sponsor Company is in Good Standing, PCI SSC will recognize as ISAs each eligible employee of the Sponsor Company who has successfully completed all required ISA training and examinations and satisfies applicable ISA Qualification Requirements (defined below).

3.1 ISA Eligibility Requirements

In order for an individual to be considered for qualification as an ISA, the following requirements ("ISA Eligibility Requirements") must be satisfied:

a) The ISA candidate must be a full-time employee of a Sponsor Company that is in Good Standing at the time when the application for the employee's ISA qualification is considered by PCI SSC (the "Application Time");

b) PCI SSC must have on file an executed and effective Sponsor Attestation from the ISA's Initiating Sponsor Company; and

3.2 Initial ISA Qualification Requirements

In order for an individual to be initially qualified as an ISA, the following requirements ("Initial ISA Qualification Requirements") must be satisfied:

a) All applicable ISA Eligibility Requirements must continue to be satisfied, the ISA candidate must continue to be a full-time employee of its Initiating Sponsor Company, and the Initiating Sponsor Company must continue to be in Good Standing;

b) The ISA candidate must successfully complete all required initial ISA Program training and legitimately pass, of his or her own accord, each examination conducted as part of that training;

c) The ISA candidate must read and agree to adhere to the PCI SSC Code of Professional Responsibility; and

d) The ISA candidate must accept the ISA Attestation as part of the training and exam process.

3.3 ISA Good Standing and Annual Re-qualification Requirements

An ISA is deemed to be in "Good Standing" as long as all of the following requirements ("ISA Good Standing Requirements", and together with the ISA Eligibility Requirements and the Initial ISA Qualification Requirements, the "ISA Qualification Requirements") are satisfied:

a) The ISA must successfully complete all required annual ISA Program training and legitimately pass, of his or her own accord, each examination conducted as part of such training. The existing ISA qualification of one who fails to pass a required exam will immediately be revoked until they successfully pass the exam. Re-qualification training and a new ISA Attestation must be completed on an annual basis, on or before the applicable anniversary of their original ISA qualification date;

b) The ISA must continue to be employed by his or her Initiating Sponsor Company* and that Initiating Sponsor Company must remain in Good Standing as a Sponsor Company; and

c) The ISA must comply with the terms of his or her ISA Attestation.

Note:

Failure to satisfy any of the above requirements (e.g., due to failure to pass required ISA training examinations, change of employer, or failure of the Initiating Sponsor Company to maintain Good Standing) will result in immediate termination of ISA qualification. Except as otherwise specified herein, an individual who has lost ISA qualification may re-apply at any time.

3.4 Recommended ISA Experience

ISA training is intended for individuals who already possess significant relevant technical and security audit and assessment experience. Candidates will ideally possess the following or equivalent experience:

a) Sufficient information security knowledge and experience to conduct technically complex security assessments;

b) Emphasis on internal information systems and security audit work as Sponsor Company employee;

c) Strong understanding of payment processes, related systems, and PCI DSS;

d) Annual information systems audit training to support applicable continuing professional education requirements (for example, 20 hours of such training annually and 120 hours of such training over the immediately preceding rolling three-year period); and

e) The following additional qualifications:

- University or undergraduate degree;
- Five years' applicable work experience;
- One year of experience performing information security audits similar to QSA Assessments, or three separate such audits, or other equivalent as determined by the Sponsor Company;
- Demonstrated expertise in at least three relevant areas including network security, application security and consultancy, system integration; and
- One or more of the following industry-recognized professional certifications (possessing one certification from each list is recommended, but not required):

  List A – Information Security

  - Certified Information System Security Professional (CISSP)
  - Certified Information Security Manager (CISM)

  List B – Audit

  - Certified Information Systems Auditor (CISA)
  - GIAC Systems and Network Auditor (GSNA)
  - Certified ISO 27001, Lead Auditor, Internal Auditor
  - International Register of Certificated Auditors (IRCA)
  - Information Security Management System (ISMS) Auditor

4 Terminology

Throughout this document, the following terms shall have the following meanings:

Term	Reference / Meaning
Good Standing	With respect to a Sponsor Company is defined in Section 2.2, and with respect to an ISA is defined in Section 3.3.
Initial ISA Qualification Requirements	Defined in Section 3.2.
Initiating Sponsor Company	Defined in Section 1.1.
Internal Security Assessor (ISA)	An individual who has satisfied and continues to satisfy all requirements applicable to ISAs as set forth in the ISA Qualification Requirements document.
ISA Attestation	The most current version of the document attached as Appendix B to the ISA Qualification Requirements document.
ISA Eligibility Requirements	Defined in Section 3.1.
ISA Good Standing Requirements	Defined in Section 3.3.
ISA Program Fees	Defined in Section 2.3.
ISA Qualification Requirements	Defined in Section 3.
ISA Qualification Requirements document	The then-current version of the *Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Internal Security Assessors* as made publicly available through the Website.
PCI SSC Code of Professional Responsibility	The then-current version of the PCI SSC Code of Professional Responsibility as made publicly available on the Website.
PCI DSS or Payment Card Industry Data Security Standard	The then-current (or successor) version of the *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures* as made publicly available on the Website.
PCI SSC	PCI Security Standards Council, LLC.
Portal	The then-current PCI SSC Assessor Portal (and its accompanying web pages), which is currently available at https://programs.pcissc.org.
QSA	Acronym for “Qualified Security Assessor.” QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the QSA Qualification Requirements for details about requirements for QSA Companies and Employees.
QSA Assessment	The on-site assessment of any cardholder data environment by a QSA for purposes of validating PCI DSS compliance.
Sponsor Attestation	The then-current version of the “Sponsor Attestation” document made available by PCI SSC via the Portal.

Term	Reference / Meaning
Sponsor Company	An organization that has satisfied and continues to satisfy all Sponsor Company Requirements.
Sponsor Company Application Package	Defined in Section 1.2.1.
Sponsor Company Eligibility Requirements	Defined in Section 2.1.
Sponsor Company Good Standing Requirements	Defined in Section 2.2.
Sponsor Company Requirements	Collectively, the Sponsor Company Eligibility Requirements and the Sponsor Company Good Standing Requirements.
Website	The then-current PCI SSC website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.

Appendix A: Sponsor Attestation

PCI SECURITY STANDARDS COUNCIL, LLC
SPONSOR ATTESTATION

1. Instructions:

This Sponsor Attestation is to be completed and submitted to the PCI Security Standards Council, LLC ("PCI SSC") via the Portal (included in this Appendix for reference) by each organization applying to participate as a "Sponsor Company" in the PCI SSC Internal Security Assessor Program ("ISA Program"), and is effective as of the date of such submission. Please do not submit this Sponsor Attestation to PCI SSC other than through the Portal.

For purposes of this Sponsor Attestation, "Company" means the company, organization or other legal entity that, through its individual representative(s): (a) was previously identified to PCI SSC as part of the Sponsor Company Registration Form information submitted to PCI SSC through the online Sponsor Company registration page on Website (the "Sponsor Company Registration Page"), (b) received from PCI SSC or its representative(s) an e-mail link providing access to this Sponsor Attestation, and (c) clicks "ACCEPT" below.

2. Agreement:

By clicking "ACCEPT," the individual doing so hereby: (i) represents and warrants to PCI SSC that s/he is authorized to legally bind Company to the terms and conditions of this Sponsor Attestation and (ii) acknowledges, agrees, and represents and warrants to PCI SSC, by and on behalf of Company, as follows:

a) Company has read and understands this Sponsor Attestation and the ISA Qualification Requirements document and agrees to and accepts the terms, provisions, and requirements hereof and thereof.

b) Capitalized terms used but not otherwise defined in this Sponsor Attestation shall have the meanings ascribed to them in the then-current version of the *Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Internal Security Assessors* as made publicly available through the Website.

c) Company is currently in compliance with all Sponsor Company Eligibility Requirements and all applicable Sponsor Company Good Standing Requirements and understands that Sponsor Company qualification is subject to annual re-qualification and payment of applicable ISA Program Fees.

d) Company has not and will not submit any ISA Attestation to PCI SSC unless Company believes in good faith that the applicable ISA candidate satisfies all applicable ISA Qualification Requirements.

e) Company will comply with all Sponsor Company Requirements and will promptly notify PCI SSC (in each instance) of any failure of Company or any ISA thereof to satisfy any Sponsor Company Requirement or Individual ISA Requirement, as applicable.

f) To the Company's knowledge, all information provided to PCI SSC in connection with the ISA Program is and will be true, accurate and complete in all material respects as of the date provided.

g) Company shall not (and shall not permit any of its ISAs or Affiliates to) misrepresent or make any false, misleading or incomplete statement regarding any requirement of the ISA Program, PCI SSC, or any of the standards or programs offered or managed by PCI SSC.

h) The ISA Program is intended solely as a tool to assist Sponsor Companies in working to: improve their own understanding of the PCI DSS, better prepare for interaction with QSAs, enhance the quality, reliability, and consistency of their internal PCI DSS self-assessments, and support the consistent and proper application of PCI DSS measures and controls.

i) PCI SSC does not verify compliance of Sponsor Companies or ISAs with applicable ISA Program requirements or recommendations, and relies solely on Sponsor Attestations and ISA Attestations, and in the case of ISAs, ISA Program examination results, in determining eligibility to participate in the ISA Program. ISA qualification signifies only that an individual has met applicable ISA Qualification Requirements and passed applicable ISA training examinations as of the applicable qualification date, and does not constitute any guarantee, warranty or endorsement, whether express or implied, of (i) any Sponsor Company, (ii) any ISA, (iii) PCI DSS compliance, (iv) the ability of a given ISA to competently perform self-assessment work on a given occasion, or (v) freedom from security vulnerabilities.

j) WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW: (I) PCI SSC PROVIDES THE PCI DSS, ISA PROGRAM, ISA QUALIFICATION REQUIREMENTS DOCUMENT, WEBSITE AND ALL RELATED AND OTHER MATERIALS AND SERVICES PROVIDED OR OTHERWISE MADE ACCESSIBLE IN CONNECTION WITH THE ISA PROGRAM (COLLECTIVELY, THE "PCI MATERIALS") ON AN "AS IS" BASIS AND WITHOUT WARRANTY OF ANY KIND, AND COMPANY ASSUMES THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE ARISING OUT OF ITS USE OF ANY OF THE FOREGOING, (II) PCI SSC DISCLAIMS, AND COMPANY HEREBY EXPRESSLY WAIVES, ANY AND ALL REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE ISA PROGRAM, PCI MATERIALS OR ANY PORTION OF EITHER OF THE FOREGOING, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND (III) IN NO EVENT SHALL PCI SSC OR ANY EMPLOYEE, REPRESENTATIVE, CONTRACTOR OR STATUTORY MEMBER THEREOF BE LIABLE TO COMPANY OR TO ANY OTHER PERSON OR ENTITY FOR ANY DAMAGES IN CONNECTION WITH THE ISA PROGRAM OR ITS ACTIVITIES IN CONNECTION THEREWITH, INCLUDING WITHOUT LIMITATION, DIRECT, CONSEQUENTIAL, INCIDENTAL, INDIRECT OR SPECIAL DAMAGES, HOWEVER CAUSED, WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EVEN IF PCI SSC OR SUCH EMPLOYEE, REPRESENTATIVE, CONTRACTOR OR STATUTORY MEMBER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; PROVIDED THAT IN THE EVENT SUCH DISCLAIMER OF DAMAGES IS NOT PERMITTED UNDER APPLICABLE LAW, THE MAXIMUM AGGREGATE LIABILITY OF PCI SSC AND EACH EMPLOYEE, REPRESENTATIVE, CONTRACTOR OR STATUTORY MEMBER THEREOF, COLLECTIVELY, TO COMPANY IN CONNECTION WITH THE ISA PROGRAM SHALL NOT EXCEED $500.

k) Without the prior written consent of PCI SSC in each instance, Company shall not (i) use the name or any mark of PCI SSC for any purpose, (ii) use any other information or materials of PCI SSC other than for its intended purpose or (iii) make any statement that might constitute an implied or express endorsement, recommendation or warranty by PCI SSC regarding Sponsor Company, any of its ISAs, any Sponsor Company product or service, or the functionality, quality

or performance of any aspect of any of the foregoing. Company grants PCI SSC the right to use Company's name and trademarks, as designated by Company, to identify Company as a participant in the ISA Program.

l) This Sponsor Attestation is governed by, and any dispute arising out of or in connection herewith that cannot be amicably settled within thirty (30) days of the written notice of the dispute given to the other party by exercising the best efforts and good faith of the parties, shall be finally settled by the courts of Delaware (United States of America) in accordance with Delaware law, without resort to its conflict of laws provisions. Company irrevocably submits to the nonexclusive jurisdiction of the United States District Courts for the State of Delaware and the local courts of the State of Delaware and waives any objection to venue in said courts.

m) This Sponsor Attestation, including the ISA Qualification Requirements document and appendices thereto (each of which is incorporated herein by this reference), constitutes the exclusive statement of the agreement between the parties with respect to the ISA Program and supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the parties with respect to such subject matter. This Sponsor Attestation may be modified, altered or amended only (i) by written instrument duly executed by both parties or (ii) by PCI SSC upon thirty (30) days' written notice to Company, provided, however, that if Company does not agree with such unilateral modification, alteration or amendment, Company shall have the right, exercisable at any time within the aforementioned thirty (30) day period, to terminate this Sponsor Attestation upon written notice of its intention to so terminate to PCI SSC. Any such unilateral modification, alteration or amendment will be effective as of the end of such 30-day period. The waiver or failure of either party to exercise in any respect any right provided for in this Sponsor Attestation shall not be deemed a waiver of any further right under this Sponsor Attestation. Any notice required or permitted under this Sponsor Attestation or the ISA Qualification Requirements document shall be (i) in writing, (ii) addressed, if to PCI SSC, to the PCI SSC ISA Program Manager at isa@pcisecuritystandards.org or 401 Edgewater Place, Suite 600, Wakefield, MA 01880 or, if to Company, to Company's primary contact as identified to PCI SSC on the Sponsor Company Registration Page, and (iii) deemed to be effective and in writing either upon delivery by hand, five (5) days after deposit in the mails, one (1) day after deposit with overnight courier, upon electronic transmission confirmation if by facsimile, or upon transmission if by electronic mail.

n) PCI SSC may reject this Sponsor Attestation in accordance with applicable policies and procedures, and may terminate this Sponsor Attestation and Company's status as a Sponsor Company upon notice to Company if Company fails to satisfy applicable Sponsor Company Requirements.

o) PCI SSC may share Company information with contracted training providers in connection with ISA training registration and examination activities.

Appendix B: ISA Attestation

Each ISA is required to accept and agree to the terms and conditions of this ISA Attestation via the Portal (included here for reference) prior to the ISA qualification training examination. Please do not submit this ISA Attestation to PCI SSC other than through the Portal.

PCI SECURITY STANDARDS COUNCIL, LLC
INDIVIDUAL SECURITY ASSESSOR ATTESTATION

By clicking "ACCEPT" below, I hereby acknowledge, agree, and certify to PCI Security Standards Council, LLC (the "Council"), in connection with my qualification for and participation in the Internal Security Assessor (ISA) program managed by the Council (the "Program"), that (A) I have read, understand, and agree to comply with terms and conditions of the *Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Internal Security Assessors* (the "ISA Qualification Requirements document"); (B) the Council may include my name, contact information, the name of my employer, and my ISA approval, revocation, remediation, and/or qualification status in any applicable list or database of ISAs on the Council's website, provide any or all of the foregoing information to interested third parties, and publish or otherwise disclose any such list (in whole or in part) or information as the Council sees fit; (C) the Council may share my information with contracted training providers in connection with ISA training registration and examination activities; (D) I am currently employed on a full-time basis by the company identified in connection with my registration for the ISA qualification training examination (the "ISA Exam") in which I am about to participate ("Company"); (E) I have read and agree to continuously adhere to the current PCI SSC Code of Professional Responsibility (available on the PCI SSC website); (F) my qualification and/or approval by the Council as an ISA ("Qualification"), including but not limited to my qualification by the Council to perform the internal security assessments contemplated by the Program (collectively, "Assessments"), is subject to (i) required annual re-qualification and examination, and (ii) immediate and automatic suspension, conditions, and/or revocation if the Council determines, in its sole discretion, that I have failed to comply with, satisfy, or adhere to any applicable Program requirement, including but not limited to any interruption of my employment with Company; (G) my name, address, employer, and all other information that I have provided to the Council in connection with the Program and any related training are true and accurate in all respects; and (H) I have registered for the ISA Exam under my own name and no others. Without limiting the foregoing, I hereby expressly acknowledge, agree, and certify that I have not done and will not do any of the following, and that the Council may immediately terminate (and/or suspend, place conditions, or revoke) my Qualification if the Council determines, in its sole but reasonable discretion, that I have, at any time hereafter or within the preceding twenty-four (24) months:

- Failed to perform any Assessment in accordance with any applicable Program requirement;
- Violated any requirement regarding nondisclosure of confidential materials;
- Failed to maintain physical, electronic, and procedural safeguards to protect confidential or sensitive information as required;
- Failed to report unauthorized access to any system storing confidential or sensitive information;
- Engaged in any criminal or unprofessional or unethical business conduct;
- Failed to provide quality services, based on customer feedback or evaluation by the Council or its affiliates;

- Cheated on any exam in connection with Program training or qualification, including without limitation, by submitting work that is not my own, theft of or unauthorized access to any such exam, use of an alternate, stand-in, or proxy during any such exam, use of any prohibited or unauthorized materials, notes, or computer programs during or in connection with any such exam, or providing or communicating in any way any unauthorized information to another person during any such exam; or
- Failed to provide accurate and complete information to the Council in any application or other materials, or failed to promptly notify the Council of any event described above that occurs after the date hereof or occurred within the preceding twenty-four (24) months.

Appendix C: Sponsor Company Application Checklist

This checklist is provided as a tool to assist Sponsor Companies in organizing initial Sponsor Company and ISA application information. The application must be submitted through the Portal; and this checklist is for new Sponsor Company applications and is intended to prepare prospective Sponsor Companies for what to expect only. Information required for annual re-qualification is described in Section 2.2 of the ISA Qualification Requirements document.

Requirement	Information/Documentation Needed			
Sponsor Company Information	☐	Copy of current company formation document or equivalent approved by PCI SSC (the "Business License"), including year of incorporation, and location(s) of offices (Refer to the Document Library on the Website—*Business License Requirements*—for more information.)		
	☐	Year of incorporation		
	☐	Location(s) of office(s)		
Contacts – Primary and Secondary	☐	Name	☐	Telephone
	☐	Job Title	☐	Fax
	☐	Address	☐	E-mail address
ISA Attestation(s)	☐	One executed ISA Attestation for each initial ISA candidate (to be completed at the time of examination)		
Sponsor Attestation	☐	Sponsor Attestation agreed and accepted by and on behalf of Sponsor Company		