

# **Payment Card Industry (PCI) Software Security Framework**

---

## **Qualification Requirements for Assessors**

**1.0**

June 2019

## Document Changes

Date	Version	Description
June 2019	1.0	Initial release of the Software Security Framework Qualification Requirements for Assessors

# Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	Terminology .....	2
1.2	Qualification Process Overview.....	3
1.3	Document Structure Overview .....	4
1.4	Related Publications .....	5
1.5	Company Application Process .....	5
1.6	Additional Information Requests .....	6
<b>2</b>	<b>SSF Assessor Company Business Requirements .....</b>	<b>7</b>
2.1	Business Legitimacy.....	7
2.1.1	<i>Requirement</i> .....	7
2.1.2	<i>Provisions</i> .....	7
2.2	Independence.....	7
2.2.1	<i>Requirement</i> .....	7
2.2.2	<i>Provisions</i> .....	9
2.3	Insurance Coverage .....	9
2.3.1	<i>Requirement</i> .....	9
2.3.2	<i>Provisions</i> .....	10
2.4	SSF Assessor Company Fees .....	10
2.4.1	<i>Requirement</i> .....	10
2.5	SSF Assessor Company Agreement.....	10
2.5.1	<i>Requirement</i> .....	10
<b>3</b>	<b>SSF Assessor Company Capability Requirements .....</b>	<b>11</b>
3.1	SSF Assessor Company – Services and Experience .....	11
3.1.1	<i>Requirement</i> .....	11
3.1.2	<i>Provisions</i> .....	11
3.2	Assessor-Employee – Skills and Experience.....	12
3.2.1	<i>Secure SLC Assessor Requirements</i> .....	12
3.2.2	<i>Secure SLC Assessor Provisions</i> .....	15
3.2.3	<i>Secure Software Assessor Requirements</i> .....	15
3.2.4	<i>Secure Software Assessor Provisions</i> .....	17
3.3	Code of Professional Responsibility .....	17
3.4	Requirement .....	17
<b>4</b>	<b>SSF Assessor Company Administrative Requirements .....</b>	<b>18</b>
4.1	Contact Person .....	18
4.1.1	<i>Requirement</i> .....	18
4.1.2	<i>Provisions</i> .....	18
4.2	Background Checks .....	18
4.2.1	<i>Requirement</i> .....	18
4.2.2	<i>Provisions</i> .....	19
4.3	Internal Quality Assurance .....	19
4.3.1	<i>Requirement</i> .....	19
4.3.2	<i>Provisions</i> .....	21
4.4	Protection of Confidential and Personal Information.....	21
4.4.1	<i>Requirement</i> .....	21
4.5	Evidence Retention .....	23

4.5.1	Requirement.....	23
4.5.2	Provisions.....	24
4.6	Security Incident Response.....	24
4.6.1	Requirement.....	24
4.6.2	Provisions.....	25
4.7	Recognition of Secure SLC or Secure Software Validation Status.....	25
4.7.1	Requirements.....	25
4.7.2	Provisions.....	26
<b>5</b>	<b>SSF Assessor Company List and Annual Re-Qualification.....</b>	<b>27</b>
5.1	SSF Assessor Company List.....	27
5.2	Annual Re-Qualification.....	27
5.2.1	Requirements.....	27
5.2.2	Provisions.....	28
<b>6</b>	<b>Assessor Quality Management Program.....</b>	<b>29</b>
6.1	SSF Audit Process.....	29
6.2	SSF Quality Remediation Process.....	29
6.3	SSF Revocation Process.....	30
<b>Appendix A</b>	<b>SSF Assessor Company Agreement.....</b>	<b>33</b>
<b>Appendix B</b>	<b>Insurance Coverage.....</b>	<b>57</b>
<b>Appendix C</b>	<b>SSF Assessor Company Application.....</b>	<b>59</b>
<b>Appendix D</b>	<b>Secure SLC Assessor Application.....</b>	<b>67</b>
<b>Appendix E</b>	<b>Secure Software Assessor Application.....</b>	<b>70</b>
<b>Appendix F</b>	<b>Amending SSF Assessor Company Status.....</b>	<b>73</b>

# 1 Introduction

These PCI Software Security Framework Qualification Requirements for Assessors are intended for companies and their employees wishing to qualify to perform assessments under the PCI Software Security Framework (SSF) and describe the minimum capability and related documentation requirements that candidate SSF Assessor Companies and their Assessor-Employees must satisfy.

The SSF is a collection of software security standards and associated validation and listing programs developed, maintained and operated by PCI SSC, for the secure design, development and maintenance of payment software. The SSF comprises the following software security standards (each a “SSF Standard”), each of which is available through the Website:

*PCI Secure Software Lifecycle (Secure SLC) Standard*

*PCI Secure Software Standard*

Companies and their employees may choose to qualify to perform assessments using the PCI Secure SLC Standard, the PCI Secure Software Standard, or both.

- The Secure SLC Standard provides a baseline of requirements with corresponding assessment procedures and guidance to help payment software vendors design, develop, and maintain secure payment software throughout the software lifecycle. Secure Software Core Requirements apply to all types of payment software submitted for validation under the PCI Software Security Framework, regardless of the software’s functionality or underlying technology
- Module A – Account Data Protection applies to payment applications that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

**Note:** PCI SSC will publish additional modules for the Secure Software Standard (Module A and each such additional module, a “Module”), and will update the SSF Qualification Requirements to address such additional Modules or other matters, at any time and from time to time.

## 1.1 Terminology

Capitalized terms used but not otherwise defined in this document have the meanings set forth in this Section 1.1, or in the SSF Agreement, as applicable.

Term	Definition
Assessor-Employee	A Secure SLC Assessor and/or Secure Software Assessor.
Assessment Report	A report produced by an SSF Assessor Company and Assessor-Employee for the purposes of validating compliance with the applicable SSF Standard.
PCI Software Security Framework (SSF)	A collection of software security standards and associated validation and listing programs developed, maintained and operated by PCI SSC, for the secure design, development and maintenance of payment software.
PCI SSC	PCI Security Standards Council, LLC.
PCI SSC Program	The SSF and each other program offered by PCI SSC under which PCI SSC qualifies or authorizes entities and/or individuals for purposes of evaluating, assessing or validating compliance with any standard published by PCI SSC.
Remediation	See Section 6.1.
Revocation	See SSF Agreement.
Secure SLC Assessment	The onsite review of an entity to determine the entity's compliance with the Secure SLC Standard for SSF purposes.
Secure SLC Assessor	An individual who is employed by an SSF Assessor Company and satisfies and continues to satisfy all SSF Requirements applicable to individuals who are qualified by PCI SSC to conduct Secure SLC Assessments.
Secure SLC Standard	The then-current version of (or successor document to) the Payment Card Industry (PCI) Secure Software Life Cycle Requirements and Assessment Procedures as from time to time amended and made available on the Website.
Secure Software Assessment	Assessment of payment software to validate that software's compliance with the Secure Software Standard for SSF purposes.
Secure Software Assessor	An individual who is employed by an SSF Assessor Company and satisfies and continues to satisfy all SSF Requirements applicable to individuals who are qualified by PCI SSC to conduct Secure Software Assessments.
Secure Software Standard	The then-current version of (or successor document to) the Payment Card Industry (PCI) Secure Software Requirements and Assessment Procedures as from time to time amended and made available on the Website.
SSF Agreement	The then-current version of (or successor document to) the SSF Assessor Company Agreement, the current version of which is attached as Appendix A to the SSF Qualification Requirements.
SSF Assessment	A Secure SLC Assessment or Secure Software Assessment
SSF Assessor Company	An independent security organization qualified by PCI SSC to validate the compliance of an entity or its payment software against one or more applicable SSF Standards.
SSF Qualification Requirements	The then-current version of (or successor documents to) the Payment Card Industry (PCI) Software Security Framework Qualification Requirements for Assessors, as from time to time amended and made available on the Website.

Term	Definition
SSF Requirements	With respect to a given SSF Assessor Company or Assessor-Employee, the applicable requirements and obligations thereof pursuant to the SSF Qualification Requirements, the SSF Agreement, each other agreement, schedule, addendum, attestation or other instrument entered into between such SSF Assessor Company or Assessor-Employee and PCI SSC in connection with the SSF or participation therein, and any and all other policies, procedures, requirements, or obligations imposed, mandated, provided for or otherwise established by PCI SSC from time to time in connection with the SSF, including but not limited to, all policies, procedures, requirements, standards, and obligations under corresponding training programs, quality assurance programs, remediation programs, program guides and other related SSF materials, including without limitation, those relating to probation, fines, penalties, oversight, Remediation, suspension and/or Revocation.
Vendor	A company that engages an SSF Assessor Company to perform an SSF Assessment.
Website	The then-current PCI SSC website (and its accompanying web pages), which is currently available at <a href="http://www.pcisecuritystandards.org">www.pcisecuritystandards.org</a> .

## 1.2 Qualification Process Overview

To perform SSF Assessments, an organization must first qualify as an SSF Assessor Company by:

- Meeting or exceeding all applicable SSF Requirements.
- Executing the SSF Agreement with PCI SSC.
- Qualifying and maintaining at least one employee as an Assessor-Employee.
- Ensuring that its Assessor-Employees satisfy and continue to meet or exceed all applicable SSF Requirements, including those outlined within this document.

All SSF Assessor Companies are identified on the Website, including their qualification status and whether they are qualified to perform Secure SLC Assessments, Secure Software Assessments or both.

The SSF Qualification Requirements provided in this document serve as a qualification baseline and provide a transparent process for SSF Assessor Company and Assessor-Employee qualification and re-qualification. SSF Assessor Companies and Assessor-Employees must adhere to all applicable SSF Requirements and must make all required provisions described in this document.

The qualification process consists of two parts:

1. Qualification of the security company itself, and
2. Qualification of the assessor company's employee(s) who will be assisting, performing, and/or managing SSF Assessments.

To initiate the qualification process, the security company must submit to PCI SSC its:

- Unmodified, completed, and executed SSF Agreement, and
- Completed and executed SSF Assessor Company Application (Appendix C).

Additionally, an application must be completed for each company employee seeking qualification as an Assessor-Employee. Separate applications are required for SSF Assessor Companies (Appendix C), Secure SLC Assessors (Appendix D) and Secure Software Assessors (Appendix E). All applications must be submitted to PCI SSC.

**Note:** To become qualified by PCI SSC and maintain that qualification, an SSF Assessor Company must, at all times, have at least one employee qualified by PCI SSC as either a Secure Software Assessor or a Secure SLC Assessor.

### 1.3 Document Structure Overview

This document is structured as follows.

Section 1: Introduction offers a high-level overview of the application process.

Section 2: SSF Assessor Company Business Requirements covers minimum business requirements that must be demonstrated to PCI SSC by the security company. This section outlines information and items that must be provided to prove business stability, independence, and insurance coverage.

Section 3: SSF Assessor Company Capability Requirements reviews the information and documentation necessary to demonstrate the security company's service expertise.

Section 4: SSF Assessor Company Administrative Requirements describes standards for operating as a SSF Assessor Company, including background checks, adherence to PCI SSC procedures, quality assurance, and evidence retention.

Section 5: SSF Assessor Company List and Re-Qualification outlines the annual re-qualification process for the SSF Assessor Company.

Section 6: Assessor Quality Management Program describes PCI SSC's assessor quality management process, including remediation and revocation.

Appendices A to F:

- SSF Agreement (Appendix A)



- Insurance Requirements (Appendix B)
- SSF Assessor Company Application (Appendix C)
- Secure SLC Assessor Application (Appendix D)
- Secure Software Assessor Application (Appendix E)
- Amending SSF Assessor Company Status (Appendix F)

## 1.4 Related Publications

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

- PCI Secure Software Life Cycle (Secure SLC) Standard
- PCI Secure Software Standard
- PCI Secure Software Life Cycle (Secure SLC) Standard Program Guide
- PCI Secure Software Standard Program Guide
- PCI SSC Code of Professional Responsibility

## 1.5 Company Application Process

This document describes the information that must be provided to PCI SSC as part of the SSF Assessor Company application and qualification process, as well as ongoing re-qualification requirements. Each outlined requirement is followed by the information (“Provision”) that must be submitted to document how the security company meets or exceeds the stated requirements.

**Note:** Each candidate SSF Assessor Company Application must include all required qualification materials for the company’s employee(s) seeking to become Qualified as Secure SLC Assessors, Secure Software Assessors or both.

The “SSF Assessor Company Application” is attached as Appendix C to this document. All application materials and the signed SSF Agreement must be submitted in English. The SSF Agreement is binding in English even if it was translated and reviewed in another language. All other documentation provided by the SSF Assessor Company (or candidate) in a language other than English must be accompanied by a certified English translation (examples include business licenses and insurance certificates).

Applicants should complete and submit applications online to PCI SSC via PCI SSC’s secure web portal.

Applications that have not been approved or rejected after 180 days from submittal will be deleted.

**Note:** PCI SSC reserves the right to reject any application from any applicant that PCI SSC determines has committed, within three (3) years prior to the application date, any conduct that would have been considered a “Violation” (for purposes of Section 6.3 below or the SSF Agreement) if committed by an SSF Assessor Company or Assessor-Employee. The period of ineligibility will be a minimum of one (1) year, as determined by PCI SSC in a reasonable and non-discriminatory manner.

## 1.6 Additional Information Requests

In an effort to maintain the integrity of its programs, PCI SSC may request from time to time that SSF Assessor Companies and/or Assessor-Employees submit additional information or materials in order to demonstrate adherence to applicable requirements, as part of the applicable qualification or re-qualification process, or as part of the approval or quality assurance process, including but not limited to in connection with Remediation, Revocation, or appeals. All such information and materials must be submitted in accordance with the corresponding PCI SSC request, in English or with a certified English translation, within three (3) weeks of the corresponding PCI SSC request or as otherwise requested by PCI SSC.

## 2 SSF Assessor Company Business Requirements

This section describes the minimum business requirements for SSF Assessor Companies, and related information that must be provided to PCI SSC by each candidate SSF Assessor Company regarding its business legitimacy, independence, and required insurance coverage.

### 2.1 Business Legitimacy

#### 2.1.1 Requirement

Each candidate SSF Assessor Company must be recognized as a legal entity.

#### 2.1.2 Provisions

The following information must be provided to PCI SSC:

- Copy of current, valid SSF Assessor Company (or candidate SSF Assessor Company) formation document or equivalent approved by PCI SSC (the “Business License”), including year of incorporation, and location(s) of offices (Refer to the Documents Library on the Website – *Business License Requirements* for more information)
- Unless expressly prohibited by applicable law, written statements describing all past or present allegations or convictions of any fraudulent or criminal activity involving the SSF Assessor Company, SSF Assessor Company candidate or any principal thereof, and any Assessor-Employee thereof, and the status and resolution.
- Written statements describing any past or present appeals or revocations of any qualification issued by PCI SSC to the SSF Assessor Company (or any predecessor entity or, unless expressly prohibited by applicable law, any employee of any of the foregoing), and the current status and any resolution thereof.

### 2.2 Independence

#### 2.2.1 Requirement

The SSF Assessor Company must adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing SSF Assessments.

The SSF Assessor Company must have a code-of-conduct policy and provide the policy to PCI SSC upon request. The SSF Assessor Company's code-of-conduct policy must support—and never contradict—the PCI SSC Code of Professional Responsibility.

The SSF Assessor Company must adhere to all independence requirements as established by PCI SSC, including without limitation, the following:

- The SSF Assessor Company must not undertake to perform any SSF Assessment of any entity that it controls, is controlled by, is under common control with, or in which it holds any investment.
- The SSF Assessor Company must not (and will not) have offered or been offered, have provided or been provided, or have accepted any gift, gratuity, service, or other inducement to or from any employee of PCI SSC or any Vendor in connection with entering into the SSF Agreement or any agreement with a Vendor, or performing SSF Assessor Company-related services.
- The SSF Assessor Company must fully disclose in its Assessment Reports, if it assesses any Vendor that uses any security-related device, application, product, solution or software testing tool that is developed, manufactured, sold, resold, licensed, or otherwise made available to the applicable Vendor, directly or indirectly, by the SSF Assessor Company, or to which the SSF Assessor Company owns the rights, or that the SSF Assessor Company has configured or manages, including but not limited to the following:
  - Application or network firewalls
  - Intrusion detection/prevention systems
  - Database or other storage solutions
  - Encryption solutions
  - Security audit log solutions
  - File or data integrity monitoring solutions
  - Anti-malware solutions
  - Vulnerability detection services or solutions
  - Source code versioning and management solutions
- When recommending remediation actions that include one of its own solutions or products, the SSF Assessor Company must also recommend other market options that exist.

**Note:** Assessor-Employees are permitted to be employed by only one SSF Assessor Company at any given time.

- The SSF Assessor Company must ensure that its Assessor-Employees conducting or assisting with SSF Assessments are not subject to any conflict of interest, including by imposing and enforcing appropriate requirements regarding independence and separation of duties to limit sources of influence that might compromise independent judgment in performing SSF Assessments.
- The SSF Assessor Company will not use its status as an SSF Assessor Company to market services unnecessary to bring their clients into compliance with any SSF Standard.
- The SSF Assessor Company must not misrepresent any requirement of any SSF Standard, including but not limited to, in connection with its promotion or sales of services to its clients, or state or imply that any SSF Standard requires use of the SSF Assessor Company's products or services.
- The SSF Assessor Company must notify its Assessor-Employees of the independence requirements provided for in this document, as well as SSF Assessor Company's independence policy implementing such requirements, at least annually, and ensure compliance therewith.

## 2.2.2 Provisions

Written description of the SSF Assessor Company's (or candidate's) practices to maintain and assure Assessor-Employee and SSF Assessor Company independence with respect to all SSF Assessments, including but not limited to practices, organizational structure, separation of duties, and employee education in place to prevent conflicts of interest. The description must address each requirement listed in Section 2.2.1.

## 2.3 Insurance Coverage

### 2.3.1 Requirement

At all times while its SSF Agreement is in effect, the SSF Assessor Company shall maintain such insurance, coverage, exclusions and deductibles with such insurers as PCI SSC may reasonably request or require to adequately insure the SSF Assessor Company for its obligations and liabilities under the SSF Agreement, including without limitation the SSF Assessor Company's indemnification obligations.

The SSF Assessor Company must adhere to all requirements for insurance coverage required by PCI SSC, including without limitation the requirements in Appendix B, "Insurance Coverage," which includes details of required insurance coverage.

## 2.3.2 Provisions

The SSF Assessor Company (or candidate SSF Assessor Company) must provide a proof-of-coverage statement to PCI SSC to demonstrate that insurance coverage matches PCI SSC requirements and locally set insurance coverage requirements.

## 2.4 SSF Assessor Company Fees

### 2.4.1 Requirement

Each SSF Assessor Company applicant must pay an application processing fee, and a qualification fee. The application processing fee is credited toward the qualification fee. All fees are invoiced by PCI SSC, are nonrefundable, and must be paid to PCI SSC according to the instructions accompanying the invoice.

SSF Assessor Company fees Include:

- Qualification fees
- Annual re-qualification fees for subsequent years
- Annual training fee(s) for each Assessor-Employee (or candidate)
- Remediation fees (if applicable)

**Note:** All SSF Assessor Company fees are specified on the Website in the PCI SSC Programs Fee Schedule and are subject to change.

## 2.5 SSF Assessor Company Agreement

### 2.5.1 Requirement

The SSF Assessor Company's signed version of the then current SSF Agreement must (unless already in PCI SSC's possession) be provided to PCI SSC as part of the application process, and in connection with each annual re-qualification. In order to participate in the SSF, PCI SSC requires that all agreements between PCI SSC and the SSF Assessor Company (including the SSF Agreement) be signed by a duly authorized officer of the SSF Assessor Company (or candidate), and submitted to PCI SSC in unmodified form prior to submitting Assessor-Employee applications. Pursuant to the SSF Agreement, SSF Assessor Company agrees to comply with all applicable SSF Requirements.

### 3 SSF Assessor Company Capability Requirements

This section describes the minimum capability requirements for SSF Assessor Companies, as well as the related documentation that all SSF Assessor Companies must provide to PCI SSC in order to demonstrate requisite expertise, work history, and industry experience.

#### 3.1 SSF Assessor Company – Services and Experience

##### 3.1.1 Requirement

- The SSF Assessor Company must possess knowledge and experience in software security and assessment including code review similar or related to the SSF Assessments that they will be performing.
- The SSF Assessor Company must have a dedicated software security practice that includes staff with specific job functions that support the software security practice.
- The SSF Assessor Company must have demonstrated competence in cryptographic techniques, to include cryptographic algorithms, key management and rotation processes, and secure key storage.
- The SSF Assessor Company must have demonstrated competence in using application penetration-testing methodologies, to include use of forensic tools/methods, ability to exploit common software vulnerabilities, and ability to execute arbitrary code to test processes.

**Note:** The SSF Qualification Requirements for individuals are different for Secure Software Assessors and Secure SLC Assessors. The SSF Assessor Company must refer to the relevant appendix for details of the requirements for their Assessor-Employees seeking qualification as a Secure Software Assessor or Secure SLC Assessor.

##### 3.1.2 Provisions

The following information must be provided to PCI SSC:

- Description of the applicant SSF Assessor Company's software security knowledge and assessment experience including code review and a description of the methodology used to perform such reviews, preferably related to payment systems, equal to at least one year or three separate assessments.
- Evidence of a dedicated software security practice, such as:
  - The total number of employees on staff and the number of those performing software security assessments
- List of languages supported by the applicant SSF Assessor Company.

- Description of the applicant SSF Assessor Company's experience with cryptographic techniques, including cryptographic algorithms, key management and rotation processes, and secure key storage.
- Description of the applicant SSF Assessor Company's experience using application-penetration testing methodologies, to include use of forensic tools/methods, ability to exploit common software vulnerabilities, and ability to execute arbitrary code to test processes.
- Two client references from software security related engagements performed by the applicant SSF Assessor Company within the last 12 months.

## 3.2 Assessor-Employee – Skills and Experience

Each Assessor-Employee performing or managing SSF Assessments must be qualified by PCI SSC as a Secure SLC Assessor or a Secure Software Assessor. While in good standing or in Remediation, for SSF purposes, an Assessor-Employee is only authorized to conduct SSF Assessments against the specific SSF Standard(s) and Module(s) for which that Assessor-Employee has been qualified by PCI SSC, and no others. For example, an Assessor-Employee only qualified by PCI SSC as a Secure SLC Assessor is authorized to conduct SSF Assessments only against the Secure SLC Standard; and an Assessor-Employee only qualified by PCI SSC as a Secure Software Assessor is only authorized to conduct SSF Assessments against the Secure Software Standard and the specific Module for which that Assessor-Employee has been qualified. An Assessor-Employee may be qualified to perform SSF Assessments against more than one SSF Standard and Module.

All Assessor-Employees must:

- Adhere to the PCI SSC Code of Professional Responsibility.
- Be an employee of the SSF Assessor Company (meaning this work cannot be subcontracted to non-employees).

### 3.2.1 Secure SLC Assessor Requirements

Secure SLC Assessors are responsible for the following:

- Performing Secure SLC Assessments.
- Verifying the work product addresses all Secure SLC Assessment procedure steps and supports the validation status of the Vendor.
- Strictly following the Secure SLC Standard and PCI Secure SLC Standard Program Guide.



- Producing the final Assessment Report.

Each Secure SLC Assessor must satisfy the following requirements:

- Possess substantial information security knowledge and experience to conduct technically complex security assessments.
- Possess a minimum of one (1) year of experience in each of the following software development disciplines (experience may be acquired concurrently—for example, if the role involved experience in multiple disciplines at the same time):
  - Software/Systems Design
  - Programming/Software Development
  - Software/Systems Testing
- Possess a minimum of three (3) years of experience in each of the following information security disciplines (experience may be acquired concurrently—for example, if the role involved experience in multiple disciplines at the same time):
  - Security risk assessment
  - System/software security controls selection
  - Security architecture
  - Systems/software penetration testing
  - Threat & vulnerability detection and management
  - Incident detection and response
  - Cryptography and Key Management
- Possess at least **one** of the following accredited, industry-recognized professional certifications from **each of List A and List B**.

List A Information Security	List B Audit
<ul style="list-style-type: none"> <li>▪ (ISC)<sup>2</sup> Certified Information System Security Professional (CISSP)</li> <li>▪ (ISC)<sup>2</sup> Certified Information Security Manager (CISM)</li> <li>▪ Certified ISO 27001 Lead Implementer<sup>1</sup></li> <li>▪ (ISC)<sup>2</sup> Certified Software Security Life Cycle Professional (CSSLP)</li> <li>▪ Certified Application Security Engineer (CASE)</li> <li>▪ GIAC Secure Software Programmer-Java (GSSP-JAVA)</li> <li>▪ GIAC Secure Software Programmer-.NET (GSSP-.NET)</li> <li>▪ GIAC Certified Web Application Defender (GWEB)</li> <li>▪ Certified Ethical Hacker (CEH)</li> <li>▪ Offensive Security Certified Professional (OSCP)</li> <li>▪ CompTIA PenTest+</li> <li>▪ GIAC Penetration Tester (GPEN)</li> </ul>	<ul style="list-style-type: none"> <li>▪ ISACA Certified Information Systems Auditor (CISA)</li> <li>▪ GIAC Systems and Network Auditor (GSNA)</li> <li>▪ Certified ISO 27001, Lead Auditor, Internal Auditor<sup>1</sup></li> <li>▪ IRCA ISMS Auditor or higher (e.g., Auditor/Lead Auditor, Principal Auditor)</li> </ul> <p>Note: "Provisional" auditor designations do not meet the requirement</p> <ul style="list-style-type: none"> <li>▪ IIA Certified Internal Auditor (CIA)</li> </ul>

- Possess knowledge about the Secure SLC Standard and all applicable documents on the Website.
- Legitimately and successfully complete and pass all required annual Secure SLC Assessor training and exams provided as part of the SSF, of his or her own accord without any unauthorized assistance. Failure to pass any such exam, automatically disqualifies the individual as a Secure SLC Assessor and, accordingly, the employee must not perform or manage any Secure SLC Assessment until successfully passing the exam and reinstating his or her qualification.

---

<sup>1</sup> ISO27001 certifications will be accepted as meeting the requirement only when certifications are issued by an accredited certification body (for example, ANSI-ASQ National Accreditation Board (ANAB) and United Kingdom Accreditation Service (UKAS)). Certified ISO 27001 courses should be accredited to the ISO/IEC 17024 standard. It is the responsibility of the SSF Assessor Company/candidate to ensure that the certifying body is accredited, and to provide evidence of accreditation to PCI SSC. To find out if your country has an accreditation body, visit the International Accreditation Forum (IAF) website at [www.iaf.nu](http://www.iaf.nu) and use the IAF MLA signatories list to identify an accreditation body in your country or region. To find a certification body, visit the International Organization for Standardization certification information page; the section titled "Choosing a certification body" will explain how to find a certification body. Verification of company's certification should be addressed to the certification organization in question. You may also wish to contact the ISO member in your country or the country concerned, as they may have a national database of certified companies.

### 3.2.2 Secure SLC Assessor Provisions

This section is intended to draw out specific experience regarding candidate Secure SLC Assessors. Examples (including timeframes) of how each candidate's work experience meets the requirements must be provided for each candidate Secure SLC Assessor.

The following must be provided to PCI SSC for each individual to be considered for qualification as a Secure SLC Assessor:

- A record of working experience and responsibilities outlined in Section 3.2.1 above, by completing and submitting Appendix D,
- Résumé or Curriculum Vitae (CV), and;
- Certificates or other evidence of completion of industry-recognized professional certification.

### 3.2.3 Secure Software Assessor Requirements

Secure Software Assessors are responsible for the following:

- Performing Secure Software Assessments.
- Verifying the work product addresses all Secure Software Assessment procedure steps and supports the validation status of the payment software.
- Strictly following the Secure Software Standard and PCI Secure Software Assessor Program Guide.
- Producing the final Assessment Report

Each Secure Software Assessor performing or managing a Secure Software Assessment must satisfy the following requirements:

- Possess substantial information security knowledge and experience to conduct technically complex security assessments.
- Possess a minimum of three (3) years of experience in each of the following software development disciplines (experience may be acquired concurrently—for example, if the role involved experience in multiple disciplines at the same time):
  - Requirements Definition and Management
  - Software/Systems Design
  - Data Modelling and Design
  - Programming/Software Development
  - Software/Systems Testing

- Possess a minimum of three (3) years of experience in each of the following software security disciplines (experience may be acquired concurrently—for example, if the role involved experience in multiple disciplines at the same time):
  - Software security risk assessment
  - Software security controls selection
  - Secure software architecture
  - Threat & vulnerability detection and management
  - Software penetration testing
  - Incident detection and response
- Possess at least **one** of the following accredited, industry-recognized professional certifications from List A **or** List B
- Possess at least one of the following accredited, industry-recognized professional certifications from List C.

**Note:** Prior to July 1, 2021:

List C certification is not required for Secure Software Assessor candidates who (a) successfully complete and pass all requisite Secure Software Assessor training and exams and (b) are qualified by PCI SSC as PA-QSA Employees as of the time they submit their application for Secure Software Assessor qualification.

List A Information Security	List B Audit	List C Software Development
<ul style="list-style-type: none"> <li>▪ (ISC)<sup>2</sup> Certified Information System Security Professional (CISSP)</li> <li>▪ (ISC)<sup>2</sup> Certified Information Security Manager (CISM)</li> <li>▪ Certified ISO 27001 Lead Implementer<sup>1</sup></li> </ul>	<ul style="list-style-type: none"> <li>▪ ISACA Certified Information Systems Auditor (CISA)</li> <li>▪ GIAC Systems and Network Auditor (GSNA)</li> <li>▪ Certified ISO 27001, Lead Auditor, Internal Auditor<sup>1</sup></li> <li>▪ IRCA ISMS Auditor or higher (e.g., Auditor/Lead Auditor, Principal Auditor) Note: “Provisional” auditor designations do not meet the requirement</li> <li>▪ IIA Certified Internal Auditor (CIA)</li> </ul>	<ul style="list-style-type: none"> <li>▪ (ISC)<sup>2</sup> Certified Software Security Life Cycle Professional (CSSLP)</li> <li>▪ Certified Application Security Engineer (CASE)</li> <li>▪ GIAC Secure Software Programmer-Java (GSSP-JAVA)</li> <li>▪ GIAC Secure Software Programmer-.NET (GSSP-.NET)</li> <li>▪ GIAC Certified Web Application Defender (GWEB)</li> <li>▪ Certified Ethical Hacker CEH)</li> <li>▪ Offensive Security Certified Professional (OSCP)</li> <li>▪ CompTIA PenTest+</li> <li>▪ GIAC Penetration Tester (GPEN)</li> </ul>

- Possess knowledge about the Secure Software Standard and all applicable documents on the PCI SSC Website.
- Legitimately and successfully complete and pass all required annual Secure Software Assessor training and exams provided as part of the SSF, of his or her own accord without any unauthorized assistance. Failure to pass any such exam, automatically disqualifies the individual as a Secure Software Assessor and, accordingly, the employee must not perform or manage any Secure Software Assessment until successfully passing the exam and reinstating his or her qualification.

### **3.2.4 Secure Software Assessor Provisions**

This section is intended to draw out specific experience regarding candidate Secure Software Assessors. Examples (including timeframes) of how each candidate's work experience meets the requirements must be provided for each candidate Secure Software Assessor.

The following must be provided to PCI SSC for each individual to be considered for qualification as a Secure Software Assessor:

- A record of working experience and responsibilities outlined in Section 3.2.3 above, by completing and submitting Appendix E,
- Résumé or Curriculum Vitae (CV), and;
- Certificates or other evidence of completion of industry-recognized professional certification.

## **3.3 Code of Professional Responsibility**

### **3.4 Requirement**

PCI SSC has adopted a Code of Professional Responsibility (the "Code") to help ensure that SSF Assessor Companies and Assessor-Employees adhere to high standards of ethical and professional conduct. All SSF Assessor Companies and Assessor-Employees must advocate, adhere to, and support the Code (available on the Website).

## 4 SSF Assessor Company Administrative Requirements

This section describes the administrative requirements for SSF Assessor Companies.

### 4.1 Contact Person

#### 4.1.1 Requirement

The SSF Assessor Company must provide PCI SSC with a primary and secondary contact.

#### 4.1.2 Provisions

The following contact information must be provided to PCI SSC, for both primary and secondary contacts (see Appendix C):

- Name
- Job title
- Address
- Phone number
- Fax number
- E-mail address

### 4.2 Background Checks

#### 4.2.1 Requirement

Each SSF Assessor Company must perform background checks that satisfy the provisions described below (to the extent legally permitted within the applicable jurisdiction) with respect to each applicant Assessor-Employee.

Minor offenses—for example, misdemeanors or non-US equivalents—are allowed; but major offenses—for example, felonies or non-US equivalents within the prior 5-year period—automatically disqualify a candidate from qualifying as an Assessor-Employee. Upon request, each SSF Assessor Company must provide to PCI SSC the background check history for each Assessor-Employee (or candidate Assessor-Employee), to the extent legally permitted within the applicable jurisdiction.

**Note:** PCI SSC reserves the right to decline or reject any application or applicant Assessor-Employee.

## 4.2.2 Provisions

The SSF Assessor Company (or candidate SSF Assessor Company) must provide PCI SSC with responses to each of the following (see Appendix C):

- Attestation that its policies and hiring procedures include performing background checks: Examples of background checks include previous employment history, criminal record, credit history, and reference checks
- A written statement that it successfully completed such background checks for each candidate Assessor-Employee
- A summary description of current Assessor-Employee personnel background check policies and procedures, which must require and include the following:
  - Verification of aliases (when applicable)
  - Comprehensive country and (if applicable) state level review of records of any criminal activity such as felony (or non-US equivalent) convictions or outstanding warrants, within the past five years minimum
  - Annual background checks consistent with this section for each of its Assessor-Employees for any change in criminal records, arrests or convictions

## 4.3 Internal Quality Assurance

### 4.3.1 Requirement

The SSF Assessor Company must adhere to all quality assurance requirements described in this document or otherwise established by PCI SSC from time to time.

The SSF Assessor Company must have a quality assurance (QA) program, documented in its Quality Assurance manual.

The SSF Assessor Company must maintain and adhere to a documented quality assurance process and manual, which includes all of the following:

- Company name
- List of PCI SSC Programs in which the SSF Assessor Company participates
- A resource planning policy and process for SSF Assessments which includes: onboarding requirements for Assessor-Employees, résumés and current skill sets for Assessor-Employees, and a process for ongoing training, monitoring, and evaluation

- of Assessor-Employees to ensure their skill sets stay current and relevant for SSF Assessments
- Descriptions of all job functions and responsibilities within the SSF Assessor Company relating to its status and obligations as an SSF Assessor Company
  - Identification of QA manual process owner
  - Approval and sign-off processes for SSF Assessments and respective Assessment Reports
  - Requirements for independent quality review of SSF Assessor Company and Assessor-Employee work product
  - Requirements for handling and retention of workpapers and other Assessment Results and Related Materials (defined in the SSF Agreement; see also Section 4.5 for specific Workpaper Retention Policy requirements and specifications)
  - QA process flow
  - Distribution and availability of the QA manual
  - Evidence of annual review by the QA manual process owner
  - Coverage of all activities relevant to the SSF, including references to applicable SSF Qualification Requirements and to other applicable SSF documentation
  - Requirement for all Assessor-Employees to regularly monitor the Website for updates, guidance and new publications relating to the SSF.

For each SSF Assessment performed, the SSF Assessor Company must have qualified personnel conduct an independent quality assurance review of assessment procedures performed, supporting documentation workpapers retained in accordance with SSF Assessor Company's Workpaper Retention Policy, information documented in the Assessment Report related to the appropriate selection of system components, sampling procedures, compensating controls, remediation recommendations, proper use of payment definitions, consistent findings, and thorough documentation of results.

Upon commencement of each SSF Assessment, the SSF Assessor Company must inform the applicable Vendor of the Assessor Feedback Form (available on the Website) for the SSF Assessment to be performed.

PCI SSC, at its sole discretion, reserves the right to conduct audits of the SSF Assessor Company at any time and further reserves the right to conduct site visits at the expense of the SSF Assessor Company.

Upon request, the SSF Assessor Company (or applicant) must provide a complete copy of the quality assurance manual to PCI SSC.



## 4.3.2 Provisions

The applicant SSF Assessor Company must provide a completed Appendix C to PCI SSC.

## 4.4 Protection of Confidential and Personal Information

### 4.4.1 Requirement

The SSF Assessor Company must have and adhere to a documented process for classification of information and data in accordance with the information's confidentiality and privacy protection requirements. The classification process must include the classification of systems in accordance with the information and data handled by those systems.

The SSF Assessor Company must have and adhere to a documented process for protection of confidential and personal information. This must include adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and personal information against any unauthorized access or use during the acquisition, storage, processing, transmission, and disposal of such information.

The SSF Assessor Company must maintain the privacy and confidentiality of confidential and personal information created or obtained in the course of performing its duties and obligations as an SSF Assessor Company, unless (and to the extent) disclosure is required by legal authority.

The SSF Assessor Company (or applicant) must attest that their documented process for the classification of information and data includes the following:

- Definitions for confidential and personal information consistent with the definitions and usage of those terms within this document.
- Requirements that systems that store, process or transmit information of multiple classifications is classified according to the highest classification of information handled.

The SSF Assessor Company (or applicant) must attest that their documented process for protection of Confidential and Personal information includes the following:

- Physical, electronic, and procedural safeguards for protecting the acquisition and handling of confidential and personal information, including:
  - Labelling all confidential and Personal information (or the systems/media containing such information) with a unique identifier and classification.
  - Securely storing, transmitting and tracking all confidential and personal information (or the systems/media containing such information).

- Assigning confidential and personal information (or the systems/media containing such information) to authorized custodians who are responsible for ensuring its protection.
- Authenticating, authorizing, and logging all transfers of confidential and personal information (or the systems/media containing such information) between systems and/or custodians.
- Securely deleting, destroying, or returning (to the information owner) confidential or personal information upon completion of the duties and obligations of the SSF Assessor Company, unless retention and/or disclosure is required by legal authority, participation under this program, or under authorization of the information owner.
- Physical, electronic, and procedural safeguards for protecting the storage of and access to confidential and personal information, including:
  - Restricting access to confidential and personal information to only those individuals who possess a legitimate business reason to access such information.
  - Restricting access such that only the confidential and personal information necessary to carry out the relevant legitimate business function is accessible.
  - Storing confidential and personal information only on systems or media that are not accessible to the public (including by prohibiting access via the internet).
  - Encrypting electronic copies of confidential or personal information during storage.
  - Logging all attempts to access stored electronic confidential or personal information.
  - Generating alerts and notifying authorized custodians and other appropriate individuals upon any unauthorized attempts to access stored confidential or personal information.
- Physical, electronic, and procedural safeguards for protecting the transmission of confidential or personal information between authorized parties, systems or custodians, including:
  - Authenticating all transmissions of confidential and personal information.
  - Explicitly authorizing all transmissions of confidential and personal information.
  - Encrypting all electronic transmissions of confidential and personal information.
  - Logging all transmissions (electronic and physical) of confidential and personal information.
  - Generating alerts and notifying authorized custodians and other appropriate individuals upon any unauthorized attempts to access confidential or personal information during transmission.

- Requirements for establishing legal agreements with authorized third-parties with access to confidential or personal information that include provisions mandating adherence to these requirements.
- A blank copy of the SSF Assessor Company's confidentiality agreement(s) that each Assessor-Employee is required to sign.

## 4.5 Evidence Retention

### 4.5.1 Requirement

- Assessment Results and Related Materials (defined in the SSF Agreement), including but not limited to SSF Assessment workpapers and related materials, represent the evidence generated and/or gathered by an SSF Assessor Company and its Assessor-Employee(s) to support the contents of each Assessment Report. Retention of Assessment Results and Related Materials is required and the Assessment Results and Related Materials relating to a given SSF Assessment should represent all steps of the SSF Assessment from end-to-end. Such Assessment Results and Related Materials typically include screen captures, config files, interview notes, software test results, and a variety of other materials and information. The SSF Assessor Company must maintain and adhere to a documented retention policy regarding all Assessment Results and Related Materials (a "Workpaper Retention Policy"), which includes, at a minimum, the following: Formal assignment of an employee responsible for ensuring the continued accuracy of the Workpaper Retention Policy and that each Assessor-Employee (a) complies with the Workpaper Retention Policy and (b) signs an appropriate confidentiality agreement with the SSF Assessor Company (as contemplated by Section 4.4 above).
- A blank copy of the SSF Assessor Company's Workpaper Retention Policy agreement that each Assessor-Employee is required to sign, included as part of the policy, which includes agreement to conform at all times with the Workpaper Retention Policy and all applicable SSF Requirements.
- A requirement that all Assessment Results and Related Materials must be classified as confidential and handled accordingly, with detailed instructions describing how Assessor-Employees are to comply with this requirement. If the classification and handling of confidential and personal information is addressed in other confidential and sensitive data protection handling policies of the SSF Assessor Company, this should be clearly noted within the Workpaper Retention Policy.
- A requirement that Assessment Results and Related Materials must be retained for at least three (3) years and must include all digital and hard copy evidence created and/or

obtained by or on behalf of the SSF Assessor Company during or in connection with each SSF Assessment—including but not limited to: documentation reviewed (policies, processes, procedures, network and dataflow diagrams), case logs, meeting agendas and notes, evidence of onsite and offsite activities (including interview notes), screenshots, config files, results of any tests performed, and any other relevant information created and/or obtained.

- Requirements ensuring that the SSF Assessor Company has confirmed that all Assessment Results and Related Materials relating to a given SSF Assessment has in fact been retained in accordance with the procedures defined in the Workpaper Retention Policy, prior to releasing the final Assessment Report for that SSF Assessment.
- All Assessment Results and Related Materials must be made available to PCI SSC upon request for a minimum of three (3) years after completion of the applicable SSF Assessment.
- The SSF Assessor Company must provide a copy of the Workpaper Retention Policy and related procedures to PCI SSC upon request, including copies of any other policies and procedures referenced within any of the foregoing documents, such as general confidential and sensitive

## 4.5.2 Provisions

The applicant SSF Assessor Company must provide a completed version of Appendix C to PCI SSC.

## 4.6 Security Incident Response

This section describes obligations for SSF Assessor Companies where breach of cardholder data in their own or a Vendor's environment has or is suspected to have occurred.

### 4.6.1 Requirement

The SSF Assessor Company must have and adhere to a documented process for notifying the applicable Vendor where breach of cardholder data within that Vendor's environment (each an "Incident") has or is suspected to have occurred. Such process must require, and provide instruction for, notifying the Vendor in writing of the Incident and related findings, and informing the Vendor of its obligations to notify the Participating Payment Brands in accordance with each Participating Payment Brands' notification requirements.

The Vendor notification must be documented and retained in accordance with the SSF Assessor Company's evidence retention policy, along with a summary of the Incident and what actions were taken in connection with the Incident and corresponding discovery and/or notification. SSF Assessor Companies and Assessor-Employees are required to be familiar with the obligations for reporting Incidents to each of the Participating Payment Brands.

After becoming aware of an Incident, the SSF Assessor Company and its Assessor-Employees shall not take any action that is reasonably likely to diminish the integrity of, or otherwise interfere with or negatively affect the ability of a PCI Forensic Investigator (PFI) to perform any PFI Investigation (see the PCI Forensic Investigator (PFI) Program Guide on the Website for additional details).

Failure to provide such written notification to the Vendor or otherwise comply with any of the above (or any other) SSF Requirements constitutes a "Violation" (see Section 6.3 below) and may result in Remediation, Revocation of PCI SSC qualifications, and/or termination of the SSF Agreement.

## 4.6.2 Provisions

The applicant SSF Assessor Company must attest (see Appendix C) that it has an internal incident response plan, including but not limited to:

- Instructions and procedures for notifying Vendors of Incidents discovered during or in connection with the performance of an SSF Assessment or other SSF-related services and documenting those Incidents and related information in accordance with Section 4.6.1.
- Retention requirements for all Incident-related documentation, notices, and reports, with the same protections as those noted for work-paper retention in the SSF Assessor Company's evidence-retention policy and procedures.

## 4.7 Recognition of Secure SLC or Secure Software Validation Status

### 4.7.1 Requirement

The SSF Assessor Company must not provide any formal recognition of validation status in connection with validation against either the Secure Software Standard or the Secure SLC Standard until:

- PCI SSC has issued a corresponding notification of acceptance to both the SSF Assessor Company and the Vendor; and

- PCI SSC has added a corresponding listing on the applicable list on the Website.

## 4.7.2 Provisions

The SSF Assessor Company must provide the following:

- A statement that the SSF Assessor Company will not recognize validation status in connection with either the Secure Software Standard or the Secure SLC Standard until PCI SSC has (a) notified the SSF Assessor Company and the applicable Vendor via a notification of acceptance and (b) added a corresponding listing on the applicable list on the Website.

## 5 SSF Assessor Company List and Annual Re-Qualification

This section describes what happens after initial qualification, and activities related to annual re-qualification.

### 5.1 SSF Assessor Company List

Once a company has met all applicable SSF Qualification Requirements, and has at least one employee who has met all applicable SSF Qualification Requirements to be qualified as an Assessor-Employee, PCI SSC will add the SSF Assessor Company to the list of SSF Assessor Companies on the Website (“SSF Assessor Company List”).

**Note:** *The SSF Assessor Company List on the Website indicates the type of SSF Assessment the company is qualified to perform.*

Once an individual has met all applicable SSF Qualification Requirements to be qualified as an Assessor-Employee, PCI SSC will add the Assessor-Employee to the applicable search tool on the Website.

Only those SSF Assessor Companies and Assessor-Employees included on the SSF Assessor Company List or in such search tool (as applicable) as Secure SLC Assessors are recognized by PCI SSC to perform or support Secure SLC Assessments.

Only those SSF Assessor Companies and Assessor-Employees included on the SSF Assessor Company List or in such search tool (as applicable) as Secure Software Assessors are recognized by PCI SSC to perform or support Secure Software Assessments.

If, at any time, an SSF Assessor Company and/or Assessor-Employee does not meet the applicable SSF Requirements (including without limitation, payment or documentation requirements), PCI SSC reserves the right to remove the SSF Assessor Company and/or Assessor-Employee immediately from the respective list(s) or tool(s) on the Website, regardless of Remediation or Revocation. PCI SSC will notify the SSF Assessor Company of each such removal in accordance with the SSF Agreement, typically via registered or overnight mail and/or e-mail. Refer to Sections 6.2 and 6.3 below for additional information relating to Remediation and Revocation.

### 5.2 Annual Re-Qualification

#### 5.2.1 Requirements

All SSF Assessor Companies must be re-qualified by PCI SSC on an annual basis. The annual re-qualification date is based upon the SSF Assessor Company’s original

qualification date. Re-qualification requires payment of annual Assessor-Employee training and re-qualification fees, and continued compliance with applicable SSF Requirements, including but not limited to, the requirement to employ at least one Assessor-Employee at all times.

All Assessor-Employees must be re-qualified by PCI SSC on an annual basis. The annual re-qualification date is based upon the Assessor-Employee's *previous qualification or re-qualification date*. Re-qualification requires proof of training successfully completed, payment of annual training and re-qualification fees, and continued compliance with all applicable SSF Requirements.

Negative feedback from SSF Assessor Company clients, PCI SSC, Participating Payment Brands, or others may impact SSF Assessor Company and/or Assessor-Employee eligibility for re-qualification.

## 5.2.2 Provisions

The following must be provided to PCI SSC during the annual re-qualification process:

### SSF Assessor Companies

- Payment of annual re-qualification fee in accordance with the Website – *PCI SSC Programs Fee Schedule*.

### Assessor-Employees

- Maintaining professional certification(s) as required per Section 3.2 “Assessor-Employee – Skills and Experience”. PCI SSC reserves the right to request proof of current professional certifications at any time.
- Payment of annual re-qualification fees in accordance with the Website – *PCI SSC Programs Fee Schedule*.

**Note:** PCI SSC may from time to time request that SSF Assessor Companies and/or Assessor-Employees submit additional information or materials in order to demonstrate adherence to applicable requirements or as part of the applicable qualification or re-qualification process.



## 6 Assessor Quality Management Program

The PCI SSC's Assessor Quality Management (AQM) team monitors and reviews PCI SSC-qualified assessor work in order to provide reasonable assurance that such assessors maintain a baseline standard of quality.

### 6.1 SSF Audit Process

PCI SSC reserves the right to audit any SSF Assessor Company at any time, and further reserves the right to conduct site visits, at the expense of the SSF Assessor Company.

### 6.2 SSF Quality Remediation Process

SSF Assessor Companies that do not meet all applicable quality assurance standards set by PCI SSC may be offered the option to participate in PCI SSC's SSF Assessor Company Quality Remediation program ("Remediation"). Without limiting the generality of the foregoing, PCI SSC may offer Remediation in connection with any quality assurance audit, any Violation (defined in the SSF Agreement and further described below) or any other SSF-related quality concerns, including but not limited to unsatisfactory feedback from SSF Assessor Company customers or Participating Payment Brands. When an SSF Assessor Company qualifies for Remediation, the SSF Assessor Company will be notified in accordance with the SSF Agreement, typically via registered or overnight mail and/or e-mail. Once the SSF Assessor Company signs the agreement to participate in Remediation ("Remediation Agreement") and pays the fee(s) required in the notification, the applicable listing on the SSF Assessor Company List will be annotated with "In Remediation" and the listing will display the SSF Assessor Company's details in red text. Refer to the Website – PCI SSC Programs Fee Schedule for details of all applicable fees.

At the time of notification that the SSF Assessor Company qualifies for Remediation, AQM will provide the SSF Assessor Company with information on the requirements and procedures of the Remediation process and what it entails. If, during Remediation, AQM gains sufficient assurance of quality improvement and the requirements of the Remediation Agreement have been fulfilled, Remediation ends, and the SSF Assessor Company's listing on the Website returns to "In Good Standing" in black text. SSF Assessor Companies that fail to satisfy Remediation requirements may be revoked, and SSF Assessor Companies electing not to participate in Remediation when eligible will be revoked.

**Note:** The Remediation Statement on the Website affirms the Council’s position on Remediation, and any external queries about an SSF Assessor Company’s status will be directed to the SSF Assessor Company in question.

SSF Assessor Companies in Remediation may continue to perform SSF Assessments for which they are qualified by PCI SSC unless otherwise instructed by PCI SSC.

### 6.3 SSF Revocation Process

Each event below is an example of a “Violation” (defined in the SSF Agreement), and accordingly, regardless of prior warning or Remediation, may result in Revocation of SSF Assessor Company and/or Assessor-Employee qualification(s). This list is not exhaustive. Among other things, any qualification under the SSF may be revoked if PCI SSC determines that either the SSF Assessor Company or any of its Assessor-Employees has breached any provision of the SSF Agreement or otherwise failed to satisfy any applicable SSF Requirement (each also a Violation), including but not limited to.

- Failure to meet applicable SSF quality standards or comply with applicable SSF Requirements
- Failure to pay applicable SSF fees
- Failure to meet applicable SSF training requirements (annual or otherwise)
- Failure to meet applicable SSF continuing education requirements
- Failure to provide quality services, based on customer feedback or evaluation by PCI SSC or its affiliates
- Failure to maintain applicable SSF insurance requirements
- Failure to comply with or validate compliance in accordance with applicable SSF Requirements, the applicable SSF Standard, the PCI Secure SLC Standard Program Guide or PCI Secure Software Standard Program Guide (as applicable), or the terms of the SSF Agreement or supplements or addenda thereto
- Failure to maintain physical, electronic, or procedural safeguards to protect confidential or sensitive information
- Failure to report unauthorized access to any system storing confidential or sensitive information
- Engaging in unprofessional or unethical business conduct, including without limitation, plagiarism or other improper use of third-party work product in Assessment Reports

- Failure to comply with any provision or obligation regarding non-disclosure or use of confidential information or materials
- Cheating on any exam in connection with PCI SSC Program training; submitting exam work in connection with any PCI SSC Program training that is not the work of the individual candidate taking the exam; theft of or unauthorized access to any PCI SSC Program exam content; use of an alternate, stand-in or proxy during any PCI SSC Program exam; use of any prohibited or unauthorized materials, notes or computer programs during any such exam; or providing or communicating in any way any unauthorized information to another person, device or other resource during any PCI SSC Program exam
- Providing false or intentionally incomplete or misleading information to the Council in any application or other materials
- Failure to be in Good Standing (as defined in the SSF Agreement) as an SSF Assessor Company, including but not limited to failure to successfully complete applicable quality assurance audits and/or comply with all applicable requirements, policies, and procedures of PCI SSC's quality assurance, Remediation, and oversight programs and initiatives as established or imposed from time to time by PCI SSC in its sole discretion
- Failure to promptly notify PCI SSC of any event described above that occurred within three (3) years prior to the SSF Assessor Company's or Assessor-Employee's initial SSF Assessor qualification date

Each Violation constitutes a breach of the SSF Agreement, and a failure to comply with applicable SSF Requirements, and may result in Revocation of SSF Assessor Company and/or Assessor-Employee qualification(s) and/or termination of the SSF Agreement.

If the decision is made to revoke any SSF qualification, notification will be provided in accordance with the SSF Agreement and will include information regarding the appeal process.

Appeals must be submitted to the SSF Manager, within 30 days from the date of the notice of Revocation, by postal mail to the following address (e-mail submissions will not be accepted):

PCI SSC  
401 Edgewater Place, Suite 600  
Wakefield, MA 01880, USA  
Phone number: 1-781-876-8855

In connection with Revocation, the following will occur:

- The SSF Assessor Company and/or Assessor-Employee (as applicable) name will be removed from the relevant SSF Assessor Company List and/or search tool (as applicable).
- PCI SSC may notify third parties.
- The revoked company and/or individual (as applicable) can reapply for qualification after 180 days; provided however, that (i) if revoked in connection with Remediation, an election not to participate in Remediation when offered, or due to failure to satisfy applicable quality assurance standards set by PCI SSC, such company and/or individual shall be ineligible to re-apply as an SSF Assessor for a period of two (2) years; and (ii) acceptance of qualification applications after Revocation is determined at the Council's discretion in a reasonable and nondiscriminatory manner, in light of the relevant facts and circumstances, including but not limited to the nature and severity of the violation, occurrence of repeat violations, and the applicant's demonstrated ability to comply with Remediation requirements (if applicable).

## Appendix A SSF Assessor Company Agreement

### A.1 Introduction

This document (the "Agreement") is an agreement between PCI Security Standards Council, LLC ("PCI SSC") and the undersigned Applicant ("SSF Assessor") regarding SSF Assessor's qualification and designation to perform the Services (as defined in this document). PCI SSC and SSF Assessor are each sometimes referred in this document as a "party" and collectively as the "parties." Effective upon the date of PCI SSC's approval of this Agreement (the "Effective Date"), as evidenced by the PCI SSC signature below, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, SSF Assessor and PCI SSC agree to the terms and conditions set forth in this Agreement.

## A.2 General Information

Applicant					
Company Name:					
Business Address:				City:	
State/Province:		Country:		ZIP/Postal Code:	
Regions					
Language(s) to be displayed on Listing:					

Primary Contact			
Name:		Job Title:	
Direct Telephone Number:		E-mail:	
Location:		Fax:	

Secondary Contact			
Name:		Job Title:	
Direct Telephone Number:		E-mail:	
Location:		Fax:	

Applicant SSF Assessor Company Officer			
Applicant Officer Name:		Job Title:	
<i>Applicant's Officer Signature</i> ↑		<i>Date</i> ↑	

PCI SSC			
Name:			
Job Title:			
<i>PCI SSC Signature</i> ↑		<i>Date</i> ↑	

## A.3 Terms and Conditions

### A.3.1 SSF Assessor Services

Subject to the terms and conditions of this Agreement, while SSF Assessor is in Good Standing (defined in Section A.5.1(a) below) as a SSF Assessor Company or in compliance with Remediation, PCI SSC hereby approves SSF Assessor to perform, as part of the SSF and in accordance with this Agreement and all applicable SSF Requirements, those SSF Assessments for which SSF Assessor has received and maintains the corresponding Qualification from PCI SSC. For purposes of this Agreement: (i) the Vendor for which SSF Assessor is performing a given SSF Assessment is referred to herein as a “SSF Assessor Company client”; (ii) the SSF Assessments, collectively with all related services provided by SSF Assessor to PCI SSC, SSF Assessor Company clients or others in connection with this Agreement and the SSF, are referred to herein as the “Services”; (iii) “SSF Qualification Requirements” means the most current version of (or successor documents to) the *Payment Card Industry (PCI) Software Security Framework Qualification Requirements for Assessors*, as may be amended from time to time in PCI SSC’s discretion and made available on the Website, including without limitation, any and all additional supplements or addenda thereto which are applicable to SSF Assessor as a result of its participation in the SSF and related SSF initiatives operated by PCI SSC (each of which initiatives is hereby deemed to be included within the meaning of the term “SSF” for purposes of this Agreement); (iv) “Member” means an entity that is then formally admitted as (or an affiliate of) a member of PCI SSC in accordance with its governing documents (status as a PCI SSC “Participating Organization” does not establish that an entity is a “Member”); (v) “Participating Payment Brand” means a payment card brand that is then a Member and owner of PCI SSC (or an affiliate of such a payment card brand); (vi) “Qualification” means a qualification granted by PCI SSC as part of the SSF, authorizing the recipient SSF Assessor Company to perform security assessments of subject payment applications or Vendors (as applicable), for purposes of validating compliance against the specific SSF Standard and/or Module for which such Qualification was granted; and (vii) unless otherwise indicated, all other capitalized terms used in this Agreement without definition shall have the meanings ascribed to them in the SSF Qualification Requirements. The SSF Qualification Requirements are hereby incorporated into this Agreement, and SSF Assessor acknowledges and agrees that it has reviewed the current version of the SSF Qualification Requirements available on the Website.

SSF Assessor acknowledges that data security practices exist within a rapidly changing environment and agrees to monitor the Website at least weekly for changes to the SSF

Standards and the SSF Qualification Requirements. SSF Assessor will incorporate all such changes into all applicable SSF Assessments initiated on or after the effective date of such changes. SSF Assessor acknowledges and agrees that any Assessment Report or other required report regarding a SSF Assessment that is not conducted in accordance with the applicable SSF Standard as in effect at the initiation date of such SSF Assessment may be rejected.

### **A.3.2 Performance of Services**

SSF Assessor warrants, represents and agrees that it will only perform SSF Assessments for which it has been and is then qualified by PCI SSC, and that it will perform each such SSF Assessment in strict compliance with the applicable SSF Standard(s) as in effect as of the commencement date of such SSF Assessment. SSF Assessor acknowledges and agrees that SSF Assessor is only authorized to conduct SSF Assessments against the specific SSF Standard(s) and Module(s) for which SSF Assessor has received and continues to maintain the corresponding Qualification, and no others. Without limiting the foregoing, SSF Assessor will include in each Assessment Report, an applicable “Attestation of Compliance” (in the form available through the Website) signed by a duly authorized officer of the SSF Assessor, in which the SSF Assessor certifies without qualification that (a) in performing such SSF Assessment, the Assessor-Employee followed the requirements and procedures of the applicable SSF Standard(s) without deviation and (b) application of such requirements and procedures did not indicate any conditions of non-compliance with the applicable SSF Standard(s) other than those expressly noted in the applicable Assessment Report.

### **A.3.3 SSF Assessor Service Staffing**

SSF Assessor shall ensure that an Assessor-Employee that is fully qualified in accordance with all applicable *SSF Requirements* supervises all aspects of each engagement to perform Services, including without limitation, reviewing the work product that supports SSF Assessor's SSF Assessment procedures, and ensuring adherence to the SSF Qualification Requirements. All employees performing the following tasks for or on behalf of SSF Assessor in connection with the SSF must be qualified as Assessor-Employees: scoping decisions, selection of samples where sampling is employed (in accordance with the applicable SSF Standard(s)), and final report production, evaluation and/or review. SSF Assessor hereby designates the individual identified as the “Primary Contact” in Section A.2 above as SSF Assessor's primary point of contact and “Primary Contact” for purposes of the SSF and this Agreement. SSF Assessor may change its Primary Contact at any time upon



written notice to PCI SSC, and hereby represents that each Primary Contact shall have authority to execute any and all decisions on SSF Assessor's behalf concerning SSF matters. SSF Assessor acknowledges that whenever it designates a contact or representative to PCI SSC, PCI SSC will notify the individual of the designation and corresponding data privacy rights.

### **A.3.4 SSF Requirements**

SSF Assessor agrees to comply with all SSF Requirements, including without limitation, SSF Assessor's responsibilities and obligations pursuant to this Agreement, all SSF quality assurance and Remediation requirements, and all requirements applicable to SSF Assessor pursuant to the SSF Qualification Requirements. Without limiting the foregoing, SSF Assessor agrees to comply with all requirements of, make all provisions provided for in, and ensure that its Assessor-Employees comply with all applicable SSF Qualification Requirements, agrees to comply with all such requirements regarding background checks, and warrants that it has obtained all required consents to such background checks from each employee designated by SSF Assessor to PCI SSC to perform Services hereunder. SSF Assessor warrants that, to the best of SSF Assessor's ability to determine, all information provided to PCI SSC in connection with this Agreement and SSF Assessor's participation in the SSF is and shall be accurate and complete as of the date such information is provided. In the event of any change as a result of which any such information is no longer accurate or complete (including but not limited to any change in SSF Assessor's circumstances or compliance with applicable SSF Requirements), SSF Assessor shall promptly (and in any event within thirty (30) days after such change) notify PCI SSC of such change and provide such information as may be necessary to ensure that the information PCI SSC has received is then accurate and complete. SSF Assessor acknowledges that PCI SSC from time to time may require SSF Assessor to provide a representative and/or Assessor-Employees to attend any mandatory training programs in connection with the SSF, which may require the payment of attendance and other fees by SSF Assessor.

### **A.4 Fees**

SSF Assessor agrees to pay all applicable fees imposed by PCI SSC in connection with SSF Assessor's and its employees' participation in the SSF (collectively, "Fees"), in each case as and in the manner provided for in the SSF Qualification Requirements, the schedule of PCI SSC program fees on the Website (the "*PCI SSC Programs Fee Schedule*") and/or the other applicable SSF documentation. Such Fees may include, without limitation, company fees, training fees, fees in connection with quality assurance and/or Remediation,

penalties and other costs and fees. SSF Assessor agrees to pay all such Fees as and when required by PCI SSC and that all Fees are nonrefundable (regardless of whether SSF Assessor's application is approved, SSF Assessor has been removed from the SSF Assessor List (defined below), this Agreement has been terminated, or otherwise).

SSF Assessor acknowledges that PCI SSC may review and modify its Fees at any time and from time to time. Whenever a change in Fees occurs, PCI SSC shall notify SSF Assessor in accordance with the terms of Section A.10.1. Such change(s) will be effective immediately after the date of such notification. However, should SSF Assessor not agree with such change(s), SSF Assessor shall have the right to terminate this Agreement upon written notice to PCI SSC in accordance with the provisions of Section A.10.1 at any time within 30 days after such notification from PCI SSC. Except to the extent otherwise expressly provided in the SSF Qualification Requirements or other applicable SSF documentation, all fees payable to PCI SSC in connection with the SSF must be paid in US dollars (USD), by check, by credit card or by wire transfer to a PCI SSC bank account specified for such purpose by PCI SSC. SSF Assessor acknowledges and agrees that such Fees do not include any taxes, such as value added taxes (VAT), sales, excise, gross receipts and withholding taxes, universal service fund fee, or any similar tax or other government-imposed fees or surcharges which may be applicable thereto. SSF Assessor shall pay all such taxes and fees as invoiced or otherwise required in accordance with local law, and agrees to pay or reimburse PCI SSC for all such taxes or fees, excluding tax on PCI SSC's income. In respect of withholding tax, SSF Assessor will pay such additional amounts as may be necessary, such that PCI SSC receives the amount it would have received had no withholding been imposed.

## **A.5 Advertising and Promotion; Intellectual Property**

### **A.5.1 SSF Assessor List and SSF Assessor Use of PCI Materials and Marks**

- a. So long as SSF Assessor is qualified by PCI SSC as a SSF Assessor Company, PCI SSC may, at its sole discretion, display the identification of SSF Assessor, together with related information regarding SSF Assessor's status as a SSF Assessor Company (including without limitation, good standing, Remediation and/or Revocation (defined in Section A.9.5(a)) status), in such publicly available lists of SSF Assessor Companies as PCI SSC may maintain and/or distribute from time to time, whether on the Website or otherwise (collectively referred to herein as the "SSF Assessor List"). SSF Assessor shall provide all requested information

- necessary to ensure to PCI SSC's satisfaction that the identification and information relating to SSF Assessor on the SSF Assessor List is accurate. Without limiting the rights of PCI SSC set forth in the first sentence of this Section or elsewhere, PCI SSC expressly reserves the right to remove SSF Assessor from the SSF Assessor List at any time during which SSF Assessor is not in Good Standing as a SSF Assessor Company. SSF Assessor shall be deemed to be in "Good Standing" with respect to the SSF as long as this Agreement is in full force and effect, SSF Assessor has been approved as a SSF Assessor Company and such approval has not been revoked, and SSF Assessor is not in breach of any of the terms or conditions of this Agreement (including without limitation, any term or provision regarding compliance with the SSF Requirements or payment).
- b. In advertising or promoting its Services, so long as SSF Assessor is in Good Standing as a SSF Assessor Company, SSF Assessor may make reference to the fact that SSF Assessor is listed in the SSF Assessor List, provided that it may do so only during such times as SSF Assessor actually appears in the SSF Assessor List.
  - c. Except as expressly authorized herein, SSF Assessor shall not use any PCI SSC trademark, service mark, certification mark, logo or other indicator of origin or source (each a "Mark") without the prior written consent of PCI SSC in each instance. Without limitation of the foregoing, absent the prior written consent of PCI SSC in each instance and except as otherwise expressly authorized herein, SSF Assessor shall have no authority to make, and consequently shall not make, any statement that would constitute any implied or express endorsement, recommendation or warranty by PCI SSC regarding SSF Assessor, any of its services or products, or the functionality, quality or performance of any aspect of any of the foregoing. SSF Assessor shall not: (i) make any false, misleading, incomplete or disparaging statements or remarks regarding, or misrepresent the requirements of, PCI SSC or any SSF Standard, including without limitation, any requirement regarding the implementation of any SSF Standard or the application thereof to any third party, or (ii) state or imply that any SSF Standard requires usage of SSF Assessor or any of its products or services. Subject to the foregoing, and except with respect to (A) factual references that SSF Assessor includes from time to time in its contracts with SSF Assessor Company clients that are required or appropriate in order for SSF Assessor to accurately describe the nature of the Services SSF Assessor will provide pursuant to such contracts, and (B) references permitted pursuant to Section A.5.1(b) above, SSF Assessor shall not, without the separate prior written agreement or consent of PCI SSC in each instance: (1) copy, create derivative works of, publish, disseminate or otherwise use or make available any SSF Standard, PCI Materials (defined in Section A.7.3). PCI SSC mark or any copy of, or statement or material (in

any form) that incorporates any of the foregoing or any portion thereof or (2) incorporate any of the foregoing, the name of PCI SSC or the term “PCI SSC” into any product or service (in any form). Prior review and/or approval of such statements, materials or products by PCI SSC does not relieve SSF Assessor of any responsibility for the accuracy and completeness of such statements, materials or products or for SSF Assessor’s compliance with this Agreement or any applicable law. Except as otherwise expressly agreed by PCI SSC in writing, any dissemination or use of promotional or other materials or publicity in violation of Section A.5 shall be deemed a material breach of this Agreement and upon any such violation, PCI SSC may remove SSF Assessor’s name from the SSF Assessor List and/or terminate this Agreement in its sole discretion.

### **A.5.2 Uses of SSF Assessor Name and Designated Marks**

SSF Assessor grants PCI SSC and each Participating Payment Brand the right to use SSF Assessor’s name and trademarks, as designated in writing by SSF Assessor, to list SSF Assessor on the SSF Assessor List and to include reference to SSF Assessor in publications to Vendors and the public regarding the SSF. Neither PCI SSC nor any Participating Payment Brand shall be required to include any such reference in any materials or publicity regarding the SSF. SSF Assessor warrants and represents that it has authority to grant to PCI SSC and its Participating Payment Brands the right to use its name and designated marks as contemplated by this Agreement.

### **A.5.3 No Other Rights Granted**

Except as expressly stated in this Section A.5, no rights to use any party’s or Member’s marks or other Intellectual Property Rights (as defined below) are granted herein, and each party respectively reserves all of its rights therein. Without limitation of the foregoing, except as expressly provided in this Agreement, no rights are granted to SSF Assessor with respect to any Intellectual Property Rights in any SSF Standard or any other PCI Materials.

### **A.5.4 Intellectual Property Rights**

All Intellectual Property Rights, title and interest in and to the SSF, each SSF Standard and all other PCI Materials, all materials SSF Assessor receives from PCI SSC, and each portion, future version, revision, extension, and improvement of any of the foregoing, are and at all times shall remain solely and exclusively the property of PCI SSC or its licensors, as applicable. Subject to the foregoing and to the restrictions set forth in Section A.6, so long as SSF Assessor is in Good Standing as a SSF Assessor Company or in compliance

with Remediation, SSF Assessor may, on a non-exclusive, non-transferable, worldwide, revocable basis, use the PCI Materials (and any portion thereof), provided that such use is solely for SSF Assessor's internal review purposes or as otherwise expressly permitted in this Agreement or pursuant and subject to the terms of a separate written consent or agreement between PCI SSC and SSF Assessor in each instance. For purposes of this Agreement, "Intellectual Property Rights" shall mean all present and future patents, trademarks, service marks, design rights, database rights (whether registrable or unregistrable, and whether registered or not), applications for any of the foregoing, copyright, know-how, trade secrets, and all other industrial or intellectual property rights or obligations whether registrable or unregistrable and whether registered or not in any country.

- a. All right, title and interest in and to the Intellectual Property Rights in all materials and information generated by or on behalf of PCI SSC with respect to SSF Assessor are and at all times shall remain the property of PCI SSC. Subject to the provisions of Section A.6, SSF Assessor may use and disclose such materials and information solely for the purposes expressly permitted by this Agreement. SSF Assessor shall not revise, abridge, modify or alter any such materials or information.
- b. SSF Assessor shall not during or at any time after the completion, expiry or termination of this Agreement in any way question or dispute PCI SSC's or its licensors' (as applicable) Intellectual Property Rights in the SSF or any of the PCI Materials.
- c. Except as otherwise expressly agreed by the parties, as between PCI SSC and SSF Assessor, all Intellectual Property Rights, title and interest in and to the materials and information created by SSF Assessor and submitted by SSF Assessor to PCI SSC in connection with its performance under this Agreement are and at all times shall remain vested in SSF Assessor, or its licensors.

## **A.6 Confidentiality**

### **A.6.1 Definition of Confidential Information**

As used in this Agreement, "Confidential Information" means (i) all terms of this Agreement; (ii) any and all information designated in this Agreement as Confidential Information; (iii) any and all originals or copies of, any information that either party has identified in writing as confidential at the time of disclosure; and (iv) any and all Personal Information, proprietary information, merchant information, technical information or data, assessment reports, trade secrets or know-how, information concerning either party's past, current, or planned products, services, fees, finances, member institutions, acquirers, issuers, concepts,

methodologies, research, experiments, inventions, processes, formulas, designs, drawings, business activities, markets, plans, customers, equipment, card plastics or plates, software, source code, hardware configurations or other information disclosed by either party or any Member, or their respective directors, officers, employees, agents, representatives, independent contractors or attorneys, in each case, in connection with any SSF or activity in which SSF Assessor is a participant and in whatever form embodied (e.g., oral, written, electronic, on tape or disk, or by drawings or inspection of parts or equipment or otherwise), including without limitation, any and all other information that reasonably should be understood to be confidential. "Personal Information" means any and all Participating Payment Brand payment card account numbers, Participating Payment Brand transaction information, IP addresses or other PCI SSC, Member, or third-party information relating to a natural person, where the natural person could be identified from such information. Without limiting the foregoing, Personal Information further includes any information related to any Participating Payment Brand accountholder that is associated with or organized or retrievable by an identifier unique to that accountholder, including accountholder names, addresses, or account numbers.

## A.6.2 General Restrictions

- a. Each party (the "Receiving Party") agrees that all Confidential Information received from the other party (the "Disclosing Party") shall: (i) be treated as confidential; (ii) be disclosed only to those Members, officers, employees, legal advisers, accountants, representatives and agents of the Receiving Party who have a need to know and be used solely as required in connection with (A) the performance of this Agreement and/or (B) the operation of such party's or its Members' respective payment card data security compliance programs (if applicable) and (iii) not be disclosed to any third party except as expressly permitted in this Agreement or in writing by the Disclosing Party, and only if such third party is bound by confidentiality obligations applicable to such Confidential Information that are in form and substance similar to the provisions of this Section A.6.
- b. Except with regard to Personal Information, such confidentiality obligation shall not apply to information which: (i) is in the public domain or is publicly available or becomes publicly available otherwise than through a breach of this Agreement; (ii) has been lawfully obtained by the Receiving Party from a third party; (iii) is known to the Receiving Party prior to disclosure by the Disclosing Party without confidentiality restriction; or (iv) is independently developed by a member of the Receiving Party's staff to whom no Confidential Information was disclosed or communicated. If the Receiving Party is required to disclose Confidential Information of the Disclosing



Party in order to comply with any applicable law, regulation, court order or other legal, regulatory or administrative requirement, the Receiving Party shall promptly notify the Disclosing Party of the requirement for such disclosure and co-operate through all reasonable and legal means, at the Disclosing Party's expense, in any attempts by the Disclosing Party to prevent or otherwise restrict disclosure of such information.

### **A.6.3 SSF Assessor Client Data**

To the extent any data or other information obtained by SSF Assessor relating to any SSF Assessor Company client in the course of providing Services thereto may be subject to any confidentiality restrictions between SSF Assessor and such SSF Assessor Company client, SSF Assessor shall provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such SSF Assessor Company client in writing) that (i) SSF Assessor may disclose each Assessment Report, attestation of compliance and other related or similar reports or information generated or gathered by SSF Assessor in connection with its performance of the Services to PCI SSC and/or Participating Payment Brands, as requested by the SSF Assessor Company client, (ii) to the extent any Participating Payment Brand obtains such reports or information in accordance with the preceding clause A.6.3(i), such Participating Payment Brand may disclose (a) such reports or information on an as needed basis to other Participating Payment Brands and to such Participating Payment Brands' respective financial institutions and issuers and to relevant governmental, regulatory, and law enforcement inspectors, regulators and agencies and (b) that such Participating Payment Brand has received an Assessment Report and other related information with respect to such SSF Assessor Company client (identified by name) and whether the Assessment Report or other information was satisfactory, and (iii) SSF Assessor may disclose such information as necessary to comply with its obligations and requirements pursuant to Section A.10.2(b) below. Accordingly, notwithstanding anything to the contrary in Section A.6.2(a) above, to the extent requested by a SSF Assessor Company client, PCI SSC may disclose Confidential Information relating to such SSF Assessor Company client and obtained by PCI SSC in connection with this Agreement to Participating Payment Brands in accordance with this Section A.6.3, and such Participating Payment Brands may in turn disclose such information to their respective member financial institutions and other Participating Payment Brands. SSF Assessor hereby consents to such disclosure by PCI SSC and its Participating Payment Brands. As between any Member, on the one hand, and SSF Assessor or any SSF Assessor Company client, on the other hand, the confidentiality of Assessment Reports and any other information provided to Members

by SSF Assessor or any SSF Assessor Company client is outside the scope of this Agreement and may be subject to such confidentiality arrangements as may be established from time to time between such Member, on the one hand, and SSF Assessor or such SSF Assessor Company client (as applicable), on the other hand.

#### **A.6.4 Personal Information**

In the event that SSF Assessor receives Personal Information from PCI SSC or any Member or SSF Assessor Company client in the course of providing Services or otherwise in connection with this Agreement, in addition to the obligations set forth elsewhere in this Agreement, SSF Assessor will at all times during the Term (as defined in Section A.9.1) maintain such data protection handling practices as may be required by PCI SSC from time to time, including without limitation, as a minimum, physical, electronic and procedural safeguards designed: (i) to maintain the security and confidentiality of such Personal Information (including, without limitation, encrypting such Personal Information in accordance with applicable Participating Payment Brand guidelines, if any); (ii) to protect against any anticipated threats or hazards to the security or integrity of such information; and (iii) to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the natural persons to whom such Personal Information relates. SSF Assessor will make available to PCI SSC and the Participating Payment Brands, and will require in its agreements with SSF Assessor Company clients that SSF Assessor Company clients will make so available, such appropriate reviews and reports to monitor SSF Assessor's compliance with the foregoing commitments as PCI SSC or any Participating Payment Brand may reasonably request from time to time.

SSF Assessor acknowledges and agrees that information relating to an identified or identifiable natural person ("Personal Data") submitted to PCI SSC by or on behalf of SSF Assessor in connection with SSF or any other PCI SSC program is governed by the Privacy Policy available on the Website. If such Personal Data relates to a person resident or located in the European Union or European Economic Area, that person may have certain rights under the General Data Protection Regulation ("GDPR") and may contact PCI SSC through its Data Protection Program at [dataprivacy@pcisecuritystandards.org](mailto:dataprivacy@pcisecuritystandards.org) if they have concerns regarding their Personal Data, or wish to exercise any of their rights under the GDPR.



## **A.6.5 Return**

Within fourteen (14) days after notice of termination of this Agreement or demand by PCI SSC, SSF Assessor promptly shall return to PCI SSC all property and Confidential Information of PCI SSC and of all third parties to the extent provided or made available by PCI SSC; provided, however, that SSF Assessor may retain copies of Confidential Information of PCI SSC to the extent the same were, prior to such notice of termination or demand, either automatically generated archival copies or incorporated into SSF Assessor's workpapers as a result of providing services to a SSF Assessor Company client; and SSF Assessor shall continue to maintain the confidentiality of all such retained Confidential Information in accordance with this Agreement. If agreed by PCI SSC, SSF Assessor may instead destroy all such materials and information and provide a certificate of destruction to PCI SSC, with sufficient detail regarding the items destroyed, destruction date, and assurance that all copies of such information and materials also were destroyed.

## **A.6.6 Remedies**

In the event of a breach of Section A.6.2 by the Receiving Party, the Receiving Party acknowledges that the Disclosing Party will likely suffer irreparable damage that cannot be fully remedied by monetary damages. Therefore, in addition to any remedy that the Disclosing Party may possess pursuant to applicable law, the Disclosing Party retains the right to seek and obtain injunctive relief against any such breach in any court of competent jurisdiction. In the event any such breach results in a claim by any third party, the Receiving Party shall indemnify, defend and hold harmless the Disclosing Party from any claims, damages, interest, attorney's fees, penalties, costs and expenses arising out of such third-party claim(s).

## **A.7 Indemnification and Limitation of Liability**

### **A.7.1 Indemnification**

SSF Assessor shall defend, indemnify, and hold harmless PCI SSC and its Members, and their respective subsidiaries, and all affiliates, subsidiaries, directors, officers, employees, agents, representatives, independent contractors, attorneys, successors, and assigns of any of the foregoing (collectively, including without limitation, PCI SSC and its Members, "Indemnified Parties") from and against any and all claims, losses, liabilities, damages, suits, actions, government proceedings, taxes, penalties or interest, associated auditing and legal expenses and other costs (including without limitation, reasonable attorney's fees and

related costs) that arise or result from any claim by any third party with respect to SSF Assessor's (i) breach of its agreements, representations or warranties contained in this Agreement; (ii) participation in the SSF or use of any PCI Materials or SSF-related information (a) in violation of this Agreement or (b) in violation of any applicable law, rule, or regulation; (iii) non-performance of Services for any SSF Assessor Company client that has engaged SSF Assessor to perform Services, including without limitation claims asserted by SSF Assessor Company clients or Members; (iv) negligence or willful misconduct in connection with the SSF, this Agreement, or SSF Assessor's performance of Services, except to the extent arising out of negligence or willful misconduct of an Indemnified Party; or (v) breach, violation, infringement, or misappropriation of any third-party Intellectual Property Right. All indemnities provided for under this Agreement shall be paid by SSF Assessor as incurred by the Indemnified Party. This indemnification shall be binding upon SSF Assessor and its executors, heirs, successors, and assigns. Nothing in this Agreement shall be construed to impose any indemnification obligation on SSF Assessor to the extent the corresponding claim or liability arises solely from a defect in the PCI Materials provided by an Indemnified Party and such PCI Materials are used by SSF Assessor without modification and in accordance with all then applicable publicly available updates, guidance, and best practices provided by PCI SSC.

## **A.7.2 Indemnification Procedure**

SSF Assessor's indemnity obligations are contingent on the Indemnified Party's providing notice of the claim or liability to SSF Assessor, provided that the failure to provide any such notice shall not relieve SSF Assessor of such indemnity obligations except and to the extent such failure has materially and adversely affected SSF Assessor's ability to defend against such claim or liability. Upon receipt of such notice, SSF Assessor will be entitled to control, and will assume full responsibility for, the defense of such matter. PCI SSC will cooperate in all reasonable respects with SSF Assessor, at SSF Assessor's expense, in the investigation, trial and defense of such claim or liability and any appeal arising there from; provided, however, that PCI SSC and/or its Members may, at their own cost and expense, participate in such investigation, trial and defense, and any appeal arising therefrom or assume the defense of any Indemnified Party. In any event, PCI SSC and/or its Members will each have the right to approve counsel engaged by SSF Assessor to represent any Indemnified Party affiliated therewith, which approval shall not be unreasonably withheld. SSF Assessor will not enter into any settlement of a claim that imposes any obligation or liability on PCI SSC or any other Indemnified Party without the express prior written consent of PCI SSC or such Indemnified Party, as applicable.

### **A.7.3 No Warranties; Limitation of Liability**

- a. PCI SSC PROVIDES THE SSF STANDARDS, THE SSF, THE SSF QUALIFICATION REQUIREMENTS, THE WEBSITE AND ALL RELATED AND OTHER MATERIALS PROVIDED OR OTHERWISE MADE ACCESSIBLE BY PCI SSC IN CONNECTION WITH THE SSF (THE FOREGOING, COLLECTIVELY, THE "PCI MATERIALS") ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND. SSF Assessor ASSUMES THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE ARISING OUT OF ITS USE OF ANY OF THE PCI MATERIALS.
- b. PCI SSC MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, THE SSF, THE PCI MATERIALS OR ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR THE SSF. PCI SSC SPECIFICALLY DISCLAIMS, AND SSF ASSESSOR EXPRESSLY WAIVES, ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THIS AGREEMENT, THE SSF, THE PCI MATERIALS, ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR THE SSF, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITATION OF THE FOREGOING, PCI SSC SPECIFICALLY DISCLAIMS, AND SSF ASSESSOR EXPRESSLY WAIVES, ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THE PCI MATERIALS AND ANY INTELLECTUAL PROPERTY RIGHTS SUBSISTING THEREIN OR IN ANY PART THEREOF, INCLUDING BUT NOT LIMITED TO ANY AND ALL EXPRESS OR IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, OR SUITABILITY FOR ANY PURPOSE RELATING TO ANY OF THE FOREGOING. THE FOREGOING DISCLAIMER IS MADE BY PCI SSC FOR ITSELF AND, WITH RESPECT TO EACH SUCH DISCLAIMER, ON BEHALF OF ITS LICENSORS AND MEMBERS.
- c. In particular, without limiting the foregoing, SSF Assessor acknowledges and agrees that the accuracy, completeness, sequence or timeliness of the PCI Materials or any portion thereof cannot be guaranteed. In addition, PCI SSC makes no representation or warranty whatsoever, expressed or implied, and assumes no liability, and shall not be liable in any respect to SSF Assessor regarding (i) any delay or loss of use of any of the PCI Materials, or (ii) system performance and effects on or damages to software or hardware in connection with any use of the PCI Materials.
- d. EXCEPT FOR DAMAGES CAUSED BY THE GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF A PARTY, AND EXCEPT FOR THE OBLIGATIONS OF SSF

Assessor UNDER SECTIONS A.5 OR A.6, IN NO EVENT SHALL EITHER PARTY OR ANY MEMBER BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT OR SPECIAL DAMAGES, HOWEVER CAUSED, WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY DOES NOT APPLY TO INDEMNIFICATION OWED TO AN INDEMNIFIED PARTY PURSUANT TO THIS SECTION A.7.

- e. PCI SSC shall be liable vis-à-vis SSF Assessor only for any direct damage incurred by SSF Assessor as a result of PCI SSC's gross negligence (contractual or extra-contractual) under this Agreement provided PCI SSC's aggregate liability for such direct damage under and for the duration of this Agreement will never exceed the fees paid by SSF Assessor to PCI SSC under Section A.4.
- f. Except as otherwise expressly provided in this Agreement, neither PCI SSC nor any Participating Payment Brand shall be liable vis-à-vis SSF Assessor for any other damage incurred by SSF Assessor under this Agreement or in connection with the SSF, including but not limited to, loss of business, revenue, goodwill, anticipated savings, or other commercial or economic loss of any kind arising in any way out of the use of the SSF (regardless of whether such damages are reasonably foreseeable or PCI SSC has been advised of the possibility of such damages), or for any loss that results from force majeure.

#### **A.7.4 Insurance**

At all times while this Agreement is in effect, SSF Assessor shall maintain insurance in such amounts, with such insurers, coverages, exclusions and deductibles which, at a minimum, meet the applicable insurance requirements for U.S. or European Union SSF Assessor Companies (as applicable) participating in the SSF, including without limitation, the insurance requirements for SSF Assessor Companies set forth in Appendix B of the SSF Qualification Requirements. SSF Assessor acknowledges and agrees that if it is a non-U.S. and non-European Union SSF Assessor Company, unless otherwise expressly agreed by PCI SSC in writing, at all times while this Agreement is in effect, SSF Assessor shall maintain insurance in such amounts, with such insurers, coverages, exclusions and deductibles that PCI SSC determines, in its sole discretion, is substantially equivalent to the insurance required by PCI SSC for U.S. and European Union SSF Assessor Companies participating in the SSF. SSF Assessor hereby represents and warrants that it meets all applicable insurance requirements as provided for in this Section and that such insurance shall not be cancelled or modified without giving PCI SSC at least twenty (20) days' prior

written notice. PCI SSC may modify its insurance requirements from time to time based on parameters affecting risk and financial capability that are general to SSF Assessor Companies or specific to SSF Assessor, provided that PCI SSC is under no obligation to review and does not undertake to advise SSF Assessor on the adequacy of SSF Assessor's insurance coverage.

## **A.8 Independence; Representations and Warranties**

SSF Assessor agrees to comply with all applicable SSF Qualification Requirements, including without limitation, all requirements and provisions regarding independence, and hereby warrants and represents that SSF Assessor is now, and shall at all times during the Term, remain in compliance with all such SSF Qualification Requirements. SSF Assessor represents and warrants that by entering into this Agreement it will not breach any obligation to any third party. SSF Assessor represents and warrants that it will comply with all applicable laws, ordinances, rules, and regulations in any way pertaining to this Agreement or its performance of the Services or its obligations under this Agreement.

## **A.9 Term and Termination**

### **A.9.1 Term**

This Agreement shall commence as of the Effective Date and, unless earlier terminated in accordance with this Section A.9, continue for an initial term of one (1) year (the "Initial Term") and thereafter, for additional subsequent terms of one year (each a "Renewal Term" and together with the Initial Term, the "Term"), subject to SSF Assessor's successful completion of all applicable re-qualification requirements for each Renewal Term.

### **A.9.2 Termination by SSF Assessor**

SSF Assessor may terminate this Agreement at any time upon thirty (30) days' written notice to PCI SSC. Notwithstanding Section A.10.1 below, any notice or other written communication (including by electronic mail) from SSF Assessor pursuant to which or to the effect that SSF Assessor requests, notifies, elects, opts, chooses, decides, or otherwise indicates its desire to cease participation in the SSF, be removed from the SSF Assessor List or terminate this Agreement shall be deemed to constitute notice of termination of this Agreement, and the corresponding Qualification(s), by SSF Assessor pursuant to this Section, and thereafter, notwithstanding the thirty (30) day notice period provided for in the preceding sentence and without any further action by SSF Assessor, PCI SSC may

immediately remove SSF Assessor from the SSF Assessor List(s) and may terminate this Agreement effective upon written notice to SSF Assessor.

### **A.9.3 Termination by PCI SSC**

PCI SSC may terminate this Agreement effective as of the end of the then-current Term by providing SSF Assessor with written notice of its intent to terminate or not to renew this Agreement at least sixty (60) days prior to the end of the then-current Term. Additionally, PCI SSC may terminate this Agreement: (i) with written notice upon SSF Assessor's voluntary or involuntary bankruptcy, receivership, reorganization dissolution or liquidation under state or federal law that is not otherwise dismissed within thirty (30) days; (ii) with written notice upon SSF Assessor's breach of any representation or warranty under this Agreement; (iii) with fifteen (15) days' prior written notice following SSF Assessor's breach of any other term or provision of this Agreement (including without limitation, SSF Assessor's failure to comply with any of the SSF Requirements), provided such breach remains uncured when such 15-day period has elapsed; (iv) in accordance with Section A.9.5 below; (v) if PCI SSC ceases to operate the SSF, whether with or without replacing it with any other program; or (vi) if PCI SSC determines in its sole discretion that remaining a party hereto or performing any of its obligations hereunder has caused, will cause, or is likely to cause PCI SSC to violate any applicable statute, law, regulation, or other legal or regulatory requirement.

### **A.9.4 Effect of Termination**

Upon any termination or expiration of this Agreement: (i) SSF Assessor will be removed from the SSF Assessor List; (ii) SSF Assessor shall immediately cease all advertising and promotion of its Qualification and status as a SSF Assessor Company and its listing(s) on the SSF Assessor List, and ensure that it and its employees do not state or imply that any employee of SSF Assessor is an "Assessor-Employee," a "SSF Assessor" or otherwise qualified by PCI SSC under the SSF; (iii) SSF Assessor shall immediately cease soliciting for and performing all Services (including but not limited to processing of Assessment Reports), provided that SSF Assessor shall complete any and all Services contracted with SSF Assessor Company clients prior to such expiration or the notice of termination if and to the extent instructed by PCI SSC in writing; (iv) to the extent SSF Assessor is instructed to complete any Services pursuant to preceding clause (iii), SSF Assessor will deliver all corresponding outstanding Assessment Reports and other corresponding reports within the time contracted with the SSF Assessor Company client, (v) SSF Assessor shall remain responsible for all of the obligations, representations, and warranties hereunder with respect



to all Assessment Reports and other corresponding reports submitted by SSF Assessor to PCI SSC or any other person or entity; (vi) SSF Assessor shall return or destroy all PCI SSC and third-party property and Confidential Information in accordance with the terms of Section A.6; (vii) if requested by PCI SSC, SSF Assessor shall obtain (at SSF Assessor's sole cost and expense) the services of a replacement SSF Assessor Company acceptable to PCI SSC for purposes of completing those Services for which SSF Assessor was engaged in its capacity as a SSF Assessor Company prior to such expiration or the notice of termination but which SSF Assessor has not been instructed to complete pursuant to Section (iii) above; (viii) SSF Assessor shall, within fifteen (15) days of such expiration or the notice of termination, in a manner acceptable to PCI SSC, notify those of its SSF Assessor Company clients with which SSF Assessor is then engaged to perform any SSF Assessment or other Services of such expiration or termination; (ix) if requested by PCI SSC, SSF Assessor shall within fifteen (15) days of such request, identify to PCI SSC in writing all SSF Assessor Company clients with which SSF Assessor was engaged to perform Services immediately prior to such expiration or notice of termination and the status of such Services for each; and (x) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify any of its Members and any acquirers, SSF Assessor Company clients or others of such expiration or termination and the reason(s) therefor. The provisions of Sections A.5.4, A.6, A.7, A.9.4 and A.10 of this Agreement shall survive the expiration or termination of this Agreement for any or no reason.

## A.9.5 Revocation

- a. Without limiting the rights of PCI SSC as set forth elsewhere in this Agreement, in the event that PCI SSC determines in its sole but reasonable discretion that SSF Assessor meets any condition for Revocation of its Qualification as a SSF Assessor Company as established by PCI SSC from time to time (satisfaction of any such condition, a "Violation"), including without limitation, any of the conditions identified as or described as examples of Violations herein or in the SSF Qualification Requirements, PCI SSC may, effective immediately upon notice of such Violation to SSF Assessor, revoke such Qualification from SSF Assessor ("Revocation"), and such revoked Qualification shall be subject to reinstatement pending a successful appeal in accordance with Section A.9.5(b) below and PCI SSC policies and procedures.
- b. In the event of any Revocation: (i) SSF Assessor will be removed from the SSF Assessor List(s) and/or its listing(s) thereupon may be annotated as PCI SSC deems appropriate; (ii) upon Revocation of Qualification as a SSF Assessor Company, SSF Assessor must comply with Section A.9.4 above in the manner otherwise required if

- this Agreement had been terminated as of the effective date of such Revocation; (iii) SSF Assessor will have a period of thirty (30) days from the date SSF Assessor is given notice of such Violation to submit its written request for appeal to the SSF Program Manager; (iv) SSF Assessor shall, within fifteen (15) days of such Revocation, in a manner acceptable to PCI SSC, provide notice of such Revocation to those of its SSF Assessor Company clients with which SSF Assessor is then engaged to perform any SSF Assessment or other Services for which such revoked Qualification is required and, if applicable, of any conditions, restrictions or requirements of such Revocation that may impact its ability to perform such SSF Assessment or other Services for such SSF Assessor Company clients going forward; and (v) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify any of its Members and any acquirers, SSF Assessor Company clients, or others of such Revocation and the reason(s) therefor. In the event SSF Assessor fails to submit a request for appeal within the allotted 30-day period or such request is denied, this Agreement shall automatically terminate and SSF Assessor's right to such appeal shall be forfeited effective immediately as of the end of such period or such denial, as applicable.
- c. All Revocation appeal proceedings will be conducted in accordance with such procedures as PCI SSC may establish from time to time for the SSF, PCI SSC will review all relevant evidence submitted by SSF Assessor and each complainant (if any) in connection with therewith, and PCI SSC shall determine whether termination of SSF Assessor's Qualification is warranted or, in the alternative, no action, or specified remedial actions shall be required. All determinations of PCI SSC regarding Revocation and any related termination or appeals shall be final and binding upon SSF Assessor. If PCI SSC determines that termination is warranted, then effective immediately and automatically upon such determination, such Qualification and this Agreement shall terminate. If PCI SSC determines that such termination is not warranted, the Revocation shall be lifted, such Qualification shall be reinstated, and the listing of SSF Assessor that was removed from the SSF Assessor List as a result of such Revocation shall be reinstated. If PCI SSC determines that remedial action is required, PCI SSC shall notify SSF Assessor and may establish a date by which such remedial action must be completed; provided, however, that unless otherwise agreed by PCI SSC in writing the Revocation shall not be lifted, and SSF Assessor shall not be reinstated on the SSF Assessor List, unless and until such time as SSF Assessor has completed such remedial action; and provided, further, that if SSF Assessor fails to complete any required remedial actions by the date (if any) established by PCI SSC for completion thereof, PCI SSC may terminate such Qualification and this Agreement, effective immediately as of or any time after such date.



## **A.10 General Terms**

### **A.10.1 Notices**

All notices required under this Agreement shall be in writing and shall be deemed given when delivered (a) personally, (b) by overnight delivery upon written verification of receipt, (c) by facsimile or electronic mail transmission upon electronic transmission confirmation or delivery receipt, or (d) by certified or registered mail, return receipt requested, five (5) days after the date of mailing. Notices from PCI SSC to SSF Assessor shall be sent to the attention of the Primary Contact named, and at the location specified, on the signature page of this Agreement. Notices from SSF Assessor to PCI SSC shall be sent to the PCI SSC signatory identified on the signature page of this Agreement, at 401 Edgewater Place, Suite 600, Wakefield, Massachusetts 01880. A party may change its addressee and address for notices by giving notice to the other party pursuant to this Section A.10.1. Notwithstanding (and without limitation of) the foregoing: (i) any notice from PCI SSC to SSF Assessor hereunder may be given and shall be deemed to have been effectively delivered in writing when posted to the secure portal designated or reserved by PCI SSC for the SSF; and (ii) any notice from PCI SSC to SSF Assessor of any change in Fees may be given and shall be deemed to have been effectively delivered in writing when posted to the PCI SSC Program Fee Schedule on the Website.

### **A.10.2 Audit and Financial Statements**

- a. SSF Assessor shall allow PCI SSC or its designated agents access during normal business hours throughout the Term and for six (6) months thereafter to perform audits of SSF Assessor's facilities, operations and records of Services to determine whether SSF Assessor has complied with this Agreement. SSF Assessor also shall provide PCI SSC or its designated agents during normal business hours with books, records and supporting documentation adequate to evaluate SSF Assessor's performance hereunder. Upon request, SSF Assessor shall provide PCI SSC with a copy of its most recent audited financial statements or those of its parent company which include financial results of SSF Assessor, a letter from SSF Assessor's certified public accountant, or other documentation acceptable to PCI SSC setting out SSF Assessor's current financial status and warranted by SSF Assessor to be complete and accurate. PCI SSC acknowledges that any such statements that are non-public are Confidential Information, and shall restrict access to them in accordance with the terms of this Agreement.

- b. Notwithstanding anything to the contrary in Section A.6 of this Agreement, in order to assist in ensuring the reliability and accuracy of SSF Assessor's SSF Assessments, SSF Assessor hereby agrees to comply with all quality assurance procedures and requirements established or imposed by PCI SSC from time to time in connection with the SSF (including but not limited to conditions and requirements imposed in connection with Remediation, Revocation, or any other Qualification status) and that, within 15 days of any written request by PCI SSC, SSF Assessor hereby agrees to provide to PCI SSC such Assessment Results and Related Materials (defined below) as PCI SSC may reasonably request with respect to any SSF Assessor Company client for which SSF Assessor has performed a SSF Assessment. Each agreement between SSF Assessor and each of its SSF Assessor Company clients (each a "Client Agreement") shall include such provisions as may be necessary or appropriate, or otherwise required by PCI SSC, to ensure that SSF Assessor has all rights, licenses and other permissions necessary for SSF Assessor to comply with its obligations and requirements pursuant to this Agreement, with no conditions, qualifications or other terms (whether in such Client Agreement or otherwise) that might tend to nullify, impair or render unenforceable SSF Assessor's right to disclose such Assessment Results and Related Materials as required by this Section. Any failure of SSF Assessor to comply with this Section A.10.2 shall be deemed to be a breach of SSF Assessor's representations and warranties under this Agreement for purposes of Section A.9.3, and upon any such failure, PCI SSC may terminate SSF Assessor's Qualification as a SSF Assessor Company, remove SSF Assessor's name from the SSF Assessor List and/or terminate this Agreement in its sole discretion, upon notice to SSF Assessor. For purposes of the foregoing, "Assessment Results and Related Materials" means: (1) all Assessment Reports and related or similar information, reports, materials and assessment results generated and/or obtained in connection with SSF Assessor's performance of SSF Assessments, including without limitation, all workpapers, notes and other materials and information generated or obtained in connection therewith in any form, and (2) complete and accurate copies of the provisions of each Client Agreement that relate to or otherwise impact SSF Assessor's ability to comply with its disclosure obligations pursuant to this Agreement; provided that, in each case: (A) any materials otherwise required to be provided to PCI SSC pursuant to this Section may (or shall, as the case may be) be redacted to the extent necessary to comply with applicable law and/or permitted pursuant to PCI SSC policies and procedures, including but not limited to redaction of information regarding pricing, delivery process, and/or confidential and proprietary information of the SSF Assessor Company client (and/or its customers) if such redaction is in accordance with PCI SSC policy, does not eliminate or obscure any language (or the intent or meaning

thereof) that may tend to nullify, impair, or render unenforceable SSF Assessor's right to disclose Assessment Results and Related Materials to PCI SSC as required by this Section, and is as limited as reasonably possible; and (B) upon request, SSF Assessor shall provide to PCI SSC a written certification that such redaction complies with preceding clause (A) executed by an officer of SSF Assessor.

### **A.10.3 Governing Law; Severability**

Any dispute in any way arising out of or in connection with the interpretation or performance of this Agreement, which 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. Each of the parties 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. Should any individual provision of this Agreement be or become void, invalid or unenforceable, the validity of the remainder of this Agreement shall not be affected thereby and shall remain in full force and effect, in so far as the primary purpose of this Agreement is not frustrated.

### **A.10.4 Entire Agreement; Modification; Waivers**

The parties agree that this Agreement, including the SSF Qualification Requirements and any other documents, addenda, supplements, amendments, appendices, exhibits, schedules or other materials incorporated herein by reference (each of which is hereby incorporated into and made a part of this Agreement by this reference), is the exclusive statement of the agreement between the parties with respect to the subject matter hereof, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the parties with respect to such subject matter. This Agreement 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 SSF Assessor, provided, however, that if SSF Assessor does not agree with such unilateral modification, alteration or amendment, SSF Assessor shall have the right, exercisable at any time within the aforementioned thirty (30) day period, to terminate this Agreement 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 unless the Agreement is earlier terminated by SSF Assessor pursuant to the preceding sentence. The waiver or

failure of either party to exercise in any respect any right provided for in this Agreement shall not be deemed a waiver of any further right under this Agreement.

### **A.10.5 Assignment**

SSF Assessor may not assign this Agreement, or assign, delegate or subcontract any of its rights and/or obligations under this Agreement.

### **A.10.6 Independent Contractors**

The parties to this Agreement are independent contractors and neither party shall hold itself out to be, nor shall anything in this Agreement be construed to constitute either party as the agent, representative, employee, partner, or joint venture of the other. Neither party may bind or obligate the other without the other party's prior written consent.

### **A.10.7 Remedies**

All remedies in this Agreement are cumulative, in addition to and not in lieu of any other remedies available to either party at law or in equity, subject only to the express limitations on liabilities and remedies set forth herein.

### **A.10.8 Counterparts**

This Agreement may be signed in two or more counterparts, any or all of which may be executed by exchange of facsimile and/or electronic transmission, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

### **A.10.9 Conflict**

In the event of any express conflict or inconsistency between the terms and provisions of this Agreement and terms and provisions of the SSF Qualification Requirements, this Agreement shall control. Any and all disputes or disagreements regarding any such conflict or inconsistency shall be resolved by PCI SSC in its sole but reasonable discretion, and all determinations of PCI SSC in this regard shall be final and binding.

### **A.10.10 No Third-Party Beneficiaries**

Except as expressly provided herein, the provisions of this Agreement are for the benefit of the parties hereto only, no third-party beneficiaries are intended and no third party may seek to enforce or benefit from the provisions hereof.

## Appendix B Insurance Coverage

Prior to the commencement of the Services under the SSF Agreement between PCI SSC and the applicable SSF Assessor Company (the “Agreement”), the SSF Assessor Company (“Security Assessor”) shall procure the following insurance coverage, at its own expense, with respect to the performance of such Services. Such insurance shall be issued by financially responsible and properly licensed insurance carriers in the jurisdictions where the Services are performed and rated at least A VIII by *Best’s Rating Guide* (or otherwise acceptable to PCI SSC) and with minimum limits as set forth below. Such insurance shall be maintained in full force and effect for the duration of the Agreement and any renewals thereof:

- WORKERS’ COMPENSATION: Statutory Workers Compensation as required by applicable law and
- EMPLOYER’S LIABILITY with a limit of \$1,000,000
- COMMERCIAL GENERAL LIABILITY INSURANCE including PRODUCTS, COMPLETED OPERATIONS, ADVERTISING INJURY, PERSONAL INJURY and CONTRACTUAL LIABILITY INSURANCE with the following minimum limits for Bodily Injury and Property Damage on an Occurrence basis: \$1,000,000 per occurrence and \$2,000,000 annual aggregate. PCI SSC to be added as “Additional Insured.” The policy Coverage Territory must be global.
- COMMERCIAL AUTOMOBILE INSURANCE including owned, leased, hired, or non-owned autos subject to minimum limits of \$1,000,000 per accident
- CRIME/FIDELITY BOND including first-party employee dishonesty, robbery, fraud, theft, forgery, alteration, mysterious disappearance and destruction. Coverage must also include third-party employee dishonesty, i.e., coverage for claims made by the Security Assessor’s client against the Security Assessor for theft committed by the Security Assessor employees. The minimum limit shall be \$1,000,000 each loss and annual aggregate. The policy Coverage Territory must be global.
- TECHNOLOGY ERRORS & OMISSIONS, CYBER-RISK and PRIVACY LIABILITY INSURANCE covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering computer or information technology Services, or from data damage/destruction/corruption, including without limitation, failure to protect privacy, unauthorized access, unauthorized use, virus transmission, denial of service and loss of income from network security failures in connection with the Services provided under this agreement with a minimum limit of two million dollars (\$2,000,000) each claim and annual aggregate. The policy Coverage Territory must be global.

If any of the above insurance is written on a claims-made basis, then Security Assessor shall maintain such insurance for five (5) years after the termination of the Agreement. The limits shown in the appendix may be written in other currencies, but should be the equivalent of the limits in US dollars shown here.

Without limiting Security Assessor's indemnification duties as outlined in the indemnification section of the Agreement, PCI SSC shall be named as an additional insured under the Commercial General Liability for any claims and losses arising out of, allegedly arising out of or in any way connected to the Security Assessor's performance of the Services under the Agreement. The insurers shall agree that the Security Assessor's insurance is primary and any insurance maintained by PCI SSC shall be excess and non-contributing to the Security Assessor's insurance.

Prior to commencing of Services under the Agreement and annually thereafter, Security Assessor shall furnish a certificate, satisfactory to PCI SSC from each insurance company evidencing that the above insurance is in force in compliance with the terms of this insurance appendix, stating policy numbers, dates of expiration and limits of liability, and further providing that Security Assessor will endeavor to provide at least thirty (30) days' prior written notice in the event the insurance is canceled. In addition to the certificate of insurance, Security Assessor shall provide copies of the actual insurance policies if requested by PCI SSC at any time. Security Assessor shall send to PCI SSC Certificate(s) of Insurance (or other proof of insurance statements acceptable to PCI SSC) confirming the coverage required by this appendix, as part of the initial application process, and upon request by PCI SSC from time to time thereafter. Fulfillment of obligations to procure insurance shall not otherwise relieve Security Assessor of any liability hereunder or modify Security Assessor's obligations to indemnify PCI SSC.

*In the event that Security Assessor subcontracts or assigns any portion of the Services in the Agreement, the Security Assessor shall require any such subcontractor to purchase and maintain insurance coverage and waiver of subrogation as required herein.*

**WAIVER OF SUBROGATION:** Security Assessor agrees to waive subrogation against PCI SSC for any injuries to its employees arising out of or in any way related to Security Assessor's performance of the Service under the Agreement. Further, Security Assessor agrees that it shall ensure that the Workers' Compensation/Employer's Liability insurers agree to waive subrogation rights, in favor of PCI SSC, for any claims arising out of or in any way connected to Security Assessor's performance of the Services under the Agreement.

## Appendix C SSF Assessor Company Application

Please provide the information requested in Section 1 below, check each applicable box and complete the fields in Sections 2–4 below, and sign where indicated at the end of this SSF Assessor Company Application.

- The Company certifies they are currently a PCI QSA Company in good standing. (exempt from items are indicated by footnote “1” as part of initial SSF Assessor Company Application process)

### Applicant Company (the “Company”) Information – Section 1

Company Name:				
<b>Primary Contact Name:</b>		Job Title:		
Telephone:		E-mail:		
Business Address:		City:		
State/Province:		Country:	ZIP/Postal Code:	
<b>QA Contact Name:</b>		Job Title:		
Telephone:		E-mail:		
Business Address:		City:		
State/Province:		Country:	ZIP/Postal Code:	
<b>Secondary Contact Name:</b>		Job Title:		
Telephone:		E-mail:		
Business Address:		City:		
State/Province:		Country:	ZIP/Postal Code:	
URL:				

- The Company acknowledges and agrees that in order to participate as an SSF Assessor Company in the SSF Framework it must satisfy all of the requirements specified in the SSF Qualification Requirements for Assessors and supporting documents

### SSF Assessor Company Business Requirements – Section 2

- The Company acknowledges the minimum business requirements and related information that must be provided to PCI SSC regarding the Company’s business legitimacy, independence, and required insurance coverage pursuant to Section 2 of the SSF Qualification Requirements for Assessors and agrees to comply with such requirements.

#### Business Legitimacy – 2.1.2 Provisions

- The Company certifies that it is a legal entity<sup>1</sup>.
- The Company certifies that it is providing to PCI SSC herewith a copy of its current formation document or equivalent (the “Business License”). (Refer to the Documents Library on the Website – *Business License Requirements* for more information.)<sup>1</sup>



## SSF Assessor Company Business Requirements – Section 2

Year of incorporation/formation of Company:

Location(s) of Company offices:

Describe any past or present allegations or convictions of any fraudulent or criminal activity involving the company (and/or company principals), and the status and resolution:

Describe any past or present appeals or revocations of any qualification issued by PCI SSC to the Company (or any predecessor entity or, unless prohibited by applicable law, any Assessor-Employee of any of the foregoing), and the current status and any resolution thereof<sup>1</sup>:

*(Continued)*

### Independence – 2.2.2 Provisions

- The Company hereby acknowledges and agrees that it must adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing SSF Assessments.
- The Company hereby certifies that it has a code-of-conduct policy and agrees to provide that policy to PCI SSC upon request.
- The Company hereby agrees to adhere to all independence requirements as established by PCI SSC, including without limitation, all items listed in Section 2.2.1 of the SSF Qualification Requirements for Assessors.
- Below or attached hereto are (a) a description of the Company's practices for maintaining and assuring assessor independence, including but not limited to, the Company's practices, organizational structures, separation of duties, rules, and employee education in place to prevent conflicts of interest, and (b) copies of all written Company policies relating to any of the foregoing.<sup>1</sup>



## SSF Assessor Company Business Requirements – Section 2

- The Company hereby:
  - Agrees to maintain and adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing SSF Assessments.
  - Agrees to maintain and adhere to a code-of-conduct policy and provide the policy to PCI SSC upon request.
  - Agrees to adhere to all independence requirements as established by PCI SSC, including without limitation, all items listed in Section 2.2.1 of the SSF Qualification Requirements for Assessors.
  - Agrees not to undertake to perform any SSF Assessment of any entity that it controls, is controlled by, is under common control with, or in which it holds any investment.
  - Agrees that it has not and will not have offered or provided (and has not and will not have been offered or received) to (or from) any employee of PCI SSC or any customer, any gift, gratuity, service, or other inducement (other than compensation in an arm’s-length transaction), in order to enter into the SSF Agreement or any agreement with a customer, or to provide SSF-related services.
  - Agrees to fully disclose in the Assessment Report if the Company assesses any customer that uses any security-related device, application, product or solution that have been developed, manufactured, sold, resold, licensed or otherwise made available to the applicable customer by the Company, or to which the Company owns the rights, or that the Company has configured or manages, including, but not limited to the items described in Section 2.2.1 of the SSF Qualification Requirements for Assessors.
  - Agrees that when any of its Assessor-Employees recommends remediation actions that include any solution or product of the Company, the Assessor-Employee will also recommend other market options that exist.
  - Agrees that the Company has and will maintain separation of duties controls in place to ensure that its Assessor-Employees conducting SSF Assessments are independent and not subject to any conflict of interest.
  - Agrees that its Assessor-Employees will be employed by only one SSF Assessor Company at any given time.
  - Agrees not to use its status as a “listed SSF Assessor Company” to market services unnecessary to bring clients into compliance with the SSF Standards.
  - Agrees not to misrepresent any requirement of the SSF Standards in connection with its promotion or sales of services to clients, and not to state or imply that the SSF Standards requires usage of any of the Company’s products or services.

### Insurance Coverage – 2.3.2 Provisions

- The Company agrees that at all times while its SSF Assessor Company Agreement is in effect, Company will maintain sufficient insurance, insurers, coverage, exclusions, and deductibles that PCI SSC reasonably requests to adequately insure the Company for its obligations and liabilities under the SSF Assessor Company Agreement, including without limitation the Company’s indemnification obligations.
- The Company hereby acknowledges and agrees to adhere to all requirements for insurance coverage required by PCI SSC, including without limitation the requirements in Appendix B, “Insurance Coverage,” which includes details of required insurance coverage.
- The Company hereby certifies to PCI SSC that, along with this application, the Company is providing to PCI SSC a proof-of-coverage statement demonstrating that its insurance coverage matches locally set insurance coverage requirements.<sup>1</sup>
- A copy of the Company’s bound insurance coverage is attached to this application<sup>1</sup>

## SSF Assessor Company Business Requirements – Section 2

### Fees – 2.4.1 Requirements

- The Company acknowledges that it will be charged an application processing fee, an SSF Assessor Company fee and annual fees for each Assessor-Employee's PCI SSC training.
- The Company agrees to pay all such fees upon invoice from PCI SSC (or as part of the training registration process, if applicable), and that any such fees invoiced by PCI SSC will be made payable to PCI SSC according to instructions provided on the corresponding invoice.

### SSF Assessor Company Agreement – 2.5.1 Requirements

- The Company acknowledges and agrees that along with its completed application package it is providing to PCI SSC an SSF Assessor Company Agreement between PCI SSC and the Company, in unmodified form, signed by a duly authorized officer of the Company.

### PCI SSC Code of Professional Responsibility – 2.6.1 Requirements

- The Company acknowledges and agrees that it has read and understands the PCI SSC Code of Professional Responsibility, and hereby agrees to advocate, continuously adhere to, and support the terms and provisions thereof.

## SSF Assessor Company Capability Requirements – Section 3

### SSF Assessor Company Skills and Experience – 3.1.2 Provisions

**Note:** *These sections are intended to draw out specific experience about the company. The company must provide examples (including the timeframe) of how its work experience meets the program requirements.'*

- The Company represents and warrants that it currently possesses (and at all times while it is a SSF Assessor Company will continue to possess) technical security assessment experience similar or related to SSF Assessments, and that it has (and must have) a dedicated software security practice that includes staff with specific job functions that support the software security practice.

#### **Knowledge of cryptographic techniques including cryptographic algorithms, key management and rotation processes, and secure key storage:**

*Describe the company's knowledge and expertise of cryptographic techniques and the Company's role ((e.g., implementation, developer, management, etc.). For example, the types of cryptography, such as hashing, symmetric, asymmetric; the algorithms, such as AES, TDES, RSA, Diffie-Hellman, elliptic curve, key management implementations or assessments including descriptions of how keys are stored, access privileges, expected incident response when/if keys were compromised; and lifecycle management (rotation, destruction, revocation).*

Total time: Years                  Months

#### **Knowledge of application penetration-testing methodologies, to include use of forensic tools/methods, ability to exploit common software vulnerabilities, and ability to execute arbitrary code to test processes.**

*Describe the Company's expertise in application-penetration testing including use of forensic tools/methods, ability to exploit common software vulnerabilities and ability to execute arbitrary code to test processes.*

Total time: Years                  Months

### Company acknowledgements

### SSF Assessor Company Capability Requirements – Section 3

- The Company acknowledges and agrees that all of the above skill sets will be present and fully utilized on every SSF Assessment.
- The Company acknowledges and agrees that in order to perform or manage any SSF Assessment it must be qualified by PCI SSC as, and in Good Standing or in compliance with remediation as an SSF Assessor Company.
- The Company acknowledges and agrees that it must fulfill all SSF Qualification Requirements for Assessor, all SSF Assessor Company Requirements, and comply with all terms and provisions of the SSF Assessor Company Agreement, any other agreements executed with PCI SSC, and all other applicable policies and requirements of the SSF, as mandated or imposed by PCI SSC from time to time, including but not limited to all requirements in connection with PCI SSC's quality assurance initiatives, remediation, and revocation.

<sup>1</sup> QSA Companies in good standing will have already provided these materials and will not be required to resubmit them as part of the initial SSF Assessor Company application process if there have been no changes to such materials since those materials were last submitted to PCI SSC.

Additional Deliverables for SSF Assessor Companies			
Two client references from relevant security engagements within the last 12 months <sup>1</sup> :			
Client Company Name:		From (date):	To (date):
Contact Name:		Job Title:	
Telephone or e-mail:			
State/Province:		Country:	
Client Company Name:		From (date):	To (date):
Contact Name:		Job Title:	
Telephone or e-mail:			
State/Province:		Country:	
Describe any additional evidence of a dedicated software security practice within the Company <sup>1</sup> :			
<hr/>			
Describe other core business offerings:			
<hr/>			
Languages supported by the applicant SSF Assessor Company:			
<hr/>			

## SSF Assessor Company Administrative Requirements – Section 4

- The Company hereby acknowledges and agrees to the administrative requirements for SSF Assessor Companies set forth in the Qualification Requirements for SSF Assessors, including company contacts, background checks, quality assurance, and protection of confidential and sensitive information.

### Background Checks – 4.2.2 Provisions

- The Company agrees that its policies and hiring procedures must include performing background checks and satisfying the provisions in Section 4.2.2 (to the extent legally permitted within the applicable jurisdiction) when hiring each applicant Assessor-Employee.

Below is a summary description of the Company's personnel background check policies<sup>1</sup>:

The Company's personnel background check policies and procedures include the following (*to the extent legally permitted within the applicable jurisdiction*)<sup>1</sup>:

- Verification of aliases (when applicable)
- Reviewing records of any criminal activity, such as felony (or non-US equivalent) convictions or outstanding warrants
- Annually review records of any criminal activity, such as felony (or non-US equivalent) convictions or outstanding warrants
- Minor offenses (for example, misdemeanors or non-US equivalents) are allowed, but major offenses (for example, felonies or non-US equivalents) automatically disqualify an employee from serving as an Assessor-Employee
- The Company understands and agrees that, upon request, it must provide to PCI SSC the background check history for each of its Assessor-Employees, to the extent legally permitted within the applicable jurisdiction.

### Internal Quality Assurance – 4.3.2 Provisions

- The Company acknowledges and agrees that it must adhere to all quality assurance requirements described in the SSF Qualification Requirements for Assessors and supporting documentation, must have a quality assurance program, documented in its Quality Assurance manual, and must maintain and adhere to a documented quality assurance process and manual that includes all items described in Section 4.3.1 of the SSF Qualification Requirements for Assessors.
- The Company acknowledges and agrees that its internal quality assurance reviews must be performed by qualified personnel and must cover assessment procedures performed, supporting documentation, information documented in the Assessment Report related to the appropriate selection of system components, sampling procedures, compensating controls, remediation recommendations, proper use of payment definitions, consistent findings, and thorough documentation of results.

## SSF Assessor Company Administrative Requirements – Section 4

The Company acknowledges and agrees that as a SSF Assessor Company, it must at its sole cost and expense:

- At all times maintain and adhere to the internal quality assurance requirements as described in Section 4.3.1 of the SSF Qualification Requirements for Assessors.
- Provide to PCI SSC, upon request and from time to time, a complete copy of the Company's quality assurance manual, in accordance with the SSF Qualification Requirements for Assessors and supporting documentation.
- Permit PCI SSC, upon request from time to time, to conduct audits of the Company and/or to conduct site visits.
- Inform each Company SSF Assessment client of the *SSF Assessor Feedback Form* (available on the Website), upon commencement of the SSF Assessment for that client.

### Protection of Confidential and Sensitive Information – 4.4.2 Provisions

- The Company currently has and agrees to adhere to a documented process for protection of confidential and sensitive information, which includes adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information.
- The Company must maintain the privacy and confidentiality of information obtained in the course of performing its duties under the SSF Assessor Company Agreement, unless (and to the extent) disclosure is expressly permitted thereunder.
- The Company's confidential and sensitive data protection handling policies and practices include all physical, electronic, and procedural safeguards described in Section 4.4 of the SSF Qualification Requirements for Assessors.
- The Company agrees to provide PCI SSC a blank copy of the confidentiality agreement that it requires each Assessor-Employee to sign (include a blank copy of such confidentiality agreement with this application)<sup>1</sup>.

### Evidence (Workpaper) Retention – 4.5.2 Provisions

- The Company has an evidence-retention policy and procedures per Section 4.5.1 of the SSF Qualification Requirements for Assessors and agrees to retain all records created and/or obtained during each SSF Assessment for a minimum of three (3) years.
- The Company has and agrees to adhere to a documented process for securely maintaining digital and/or hard copies of all case logs, Assessment Results, workpapers, notes, and other information created and/or obtained by the Company during each SSF Assessment.
- The Company agrees to make the foregoing materials and information available to PCI SSC upon request for a minimum of three (3) years.
- The Company agrees to provide a copy of the foregoing evidence-retention policy and procedures to PCI SSC upon request.

### Security Incident Response – 4.6.2 Provisions

- The Company has a security incident-response plan and procedures per Section 4.6 of the SSF Qualification Requirements for Assessors and agrees to retain all records created and/or obtained in connection with the discovery and response regarding the applicable Incident for a minimum of three (3) years.

**SSF Assessor Company Administrative Requirements – Section 4**

- The Company's security incident-response plan includes instructions and procedures for reporting and documenting evidence of each Incident.

**Signature**

**By signing below, the undersigned hereby:**

- (a) Represents and certifies to PCI SSC that (s)he is an officer of the Company and is duly authorized to legally bind the Company to the terms of this SSF Assessor Company Application; and
- (b) Both individually and by and on behalf of the Company: (i) represents and certifies that the information provided in this SSF Assessor Company Application is true, correct, and complete; and (ii) acknowledges, accepts, agrees to, and makes the attestations and certifications set forth in (as the case may be) each of the statements checked (or otherwise marked) in this SSF Assessor Company Application above.

<b>Legal Name of Applicant SSF Assessor Company</b>			
Officer:		Title:	
By:			
<i>Duly authorized officer signature</i> ↑		<i>Date</i> ↑	

## Appendix D Secure SLC Assessor Application

For each individual applying for qualification as a Secure SLC Assessor (each a “Candidate”), the SSF Assessor Company or applicant SSF Assessor Company employing such individual (the “Company”) must submit to PCI SSC a copy of this Secure SLC Assessor Application, completed and executed by such Candidate.

Company Information				
Company Name:				
Candidate Information				
Name:		Job Title:		
Telephone:		E-mail:		
Business Address:		City:		
State/Province:		Country:	ZIP/Postal Code:	
URL:				
<input type="checkbox"/> The applicant is an existing QSA Employee, employed by a QSA Company (If yes, this applicant may be eligible for computer based training)				

### Candidate Skills, Experience and Education

**Examples of work or description of the Candidate's experience with *Software/Systems Design*:**

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

**Examples of work or description of the Candidate's experience with *Programming/Software Development*:**

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

**Examples of work or description of the Candidate's experience with *Software/Systems Testing*:**

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

**Examples of work or description of the Candidate's experience with *Security risk assessment*:**

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

**Candidate Skills, Experience and Education**

**Examples of work or description of the Candidate's experience with *Systems/software security controls*:**

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

**Examples of work or description of the Candidate's experience with *Security architecture*:**

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

**Examples of work or description of the Candidate's experience with *System/software penetration testing***

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

**Examples of work or description of the Candidate's experience with *Threat & vulnerability detection and management***

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

**Examples of work or description of the Candidate's experience with *Incident detection and response*:**

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

**Examples of work or description of the Candidate's experience with *Cryptography and Key Management*:**

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

**Candidate Professional Certifications (check all that apply):**

<input type="checkbox"/> CASE	Certification number:	Expiry date:
<input type="checkbox"/> CEH	Certification number:	Expiry date:
<input type="checkbox"/> CompTIA PenTest+	Certification number:	Expiry date:
<input type="checkbox"/> (ISC) <sup>2</sup> CISSP	Certification number:	Expiry date:
<input type="checkbox"/> (ISC) <sup>2</sup> CSSLP	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"/> IRCA Auditor	Certification number:	Expiry date:
<input type="checkbox"/> IIA CIA	Certification number:	Expiry date:



### Candidate Skills, Experience and Education

<input type="checkbox"/>	ISO 27001, Lead Auditor/Implementer, Internal Auditor	Certification number: Accredited certification body:	Date achieved:
<input type="checkbox"/>	OSCP	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/GSNA	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/GSSP-JAVA	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/.NET	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/GWEB	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/.GPEN	Certification number:	Expiry date:

**NOTE:** "In process" certifications, where the certification number has not yet been issued, do not meet the requirement.

### 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 SSFQualification Requirements for Assessors and will comply with the terms thereof; and
- (c) I have read and understand the PCI SSC Code of Professional Responsibility, and will advocate, continuously adhere to and support the terms and provisions thereof.

Candidate:		Title:	
<i>Candidate signature</i> ↑		<i>Date</i> ↑	

## Appendix E Secure Software Assessor Application

For each individual applying for qualification as a Secure Software Assessor (each a “Candidate”), the SSF Assessor Company or applicant SSF Assessor Company employing such individual (the “Company”) must submit to PCI SSC a copy of this Secure Software Assessor Application, completed and executed by such Candidate.

Company Information				
Company Name:				
Candidate Information				
Name:		Job Title:		
Telephone:		E-mail:		
Business Address:		City:		
State/Province:		Country:		ZIP/Postal Code:
URL:				

### Candidate Skills, Experience and Education

**Examples of work or description of the Candidate's experience with *Requirements Definition and Management*:**

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

**Examples of work or description of the Candidate's experience with *Software/Systems Design*:**

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

**Examples of work or description of the Candidate's experience with *Data Modelling and Design*:**

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

**Examples of work or description of the Candidate's experience with *Programming/Software Development*:**

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

**Examples of work or description of the Candidate's experience with *Software/Systems Testing*:**

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

### Candidate Skills, Experience and Education

**Examples of work or description of the Candidate's experience with *Software security risk assessment*:**

From (date): \_\_\_\_\_ To (date): \_\_\_\_\_ Total time: Years \_\_\_\_\_ Months \_\_\_\_\_

**Examples of work or description of the Candidate's experience with *Software security controls selection*:**

From (date): \_\_\_\_\_ To (date): \_\_\_\_\_ Total time: Years \_\_\_\_\_ Months \_\_\_\_\_

**Examples of work or description of the Candidate's experience with *Secure software architecture*:**

From (date): \_\_\_\_\_ To (date): \_\_\_\_\_ Total time: Years \_\_\_\_\_ Months \_\_\_\_\_

**Examples of work or description of the Candidate's experience with *Threat & vulnerability detection and management*:**

From (date): \_\_\_\_\_ To (date): \_\_\_\_\_ Total time: Years \_\_\_\_\_ Months \_\_\_\_\_

**Examples of work or description of the Candidate's experience with *Software penetration testing***

From (date): \_\_\_\_\_ To (date): \_\_\_\_\_ Total time: Years \_\_\_\_\_ Months \_\_\_\_\_

**Examples of work or description of the Candidate's experience with *Incident detection and response*:**

From (date): \_\_\_\_\_ To (date): \_\_\_\_\_ Total time: Years \_\_\_\_\_ Months \_\_\_\_\_

### Candidate Professional Certifications (check all that apply):

<input type="checkbox"/>	CASE	Certification number:	Expiry date:
<input type="checkbox"/>	CEH	Certification number:	Expiry date:
<input type="checkbox"/>	CompTIA PenTest+	Certification number:	Expiry date:
<input type="checkbox"/>	(ISC) <sup>2</sup> CISSP	Certification number:	Expiry date:
<input type="checkbox"/>	(ISC) <sup>2</sup> CSSLP	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"/>	IRCA Auditor	Certification number:	Expiry date:
<input type="checkbox"/>	IIA CIA	Certification number:	Expiry date:

### Candidate Skills, Experience and Education

<input type="checkbox"/>	ISO 27001, Lead Auditor/Implementer, Internal Auditor	Certification number: Accredited certification body:	Date achieved:
<input type="checkbox"/>	OSCP	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/GSNA	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/GSSP-JAVA	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/.NET	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/GWEB	Certification number:	Expiry date:
<input type="checkbox"/>	SANS GIAC/.GPEN	Certification number:	Expiry date:

**NOTE:** "In process" certifications, where the certification number has not yet been issued, do not meet the requirement.

### Signature

By signing below, I hereby acknowledge and agree that:

- (d) The information provided above is true, accurate and complete;
- (e) I have read and understand the SSFQualification Requirements for Assessors and will comply with the terms thereof; and
- (f) I have read and understand the PCI SSC Code of Professional Responsibility, and will advocate, continuously adhere to and support the terms and provisions thereof.

Candidate:		Title:	
<i>Candidate signature</i> ↑		<i>Date</i> ↑	

## **Appendix F Amending SSF Assessor Company Status**

SSF Assessor Companies may choose to qualify to perform Secure SLC Assessments, Secure Software Assessments or both. For each SSF Assessor Company the Website will indicate the types of SSF Assessment the company is qualified to perform.

An SSF Assessor Company in Good Standing qualified to perform Secure Software Assessments may additionally qualify to perform Secure SLC Assessments by having one or more of its Assessor-Employees qualify as a Secure SLC Assessor in accordance with Section 3.2 Assessor-Employees Skills and Experience.

An SSF Assessor Company in Good Standing qualified to perform Secure SLC Assessments may additionally qualify to perform Secure Software Assessments by having one or more of its Assessor-Employees qualify as a Secure SLC Assessor in accordance with Section 3.2 Assessor-Employees Skills and Experience.