Schellman
APEC PRP Accountability Agent Recertification Application

Table of Contents

Introduction

1. Schellman Compliance, LLC ("Schellman") is headquartered in the United States, Tampa, Florida. Schellman Compliance, LLC was formed as a Delaware limited liability company on approximately August 24, 2021. Schellman Compliance, LLC which is partly and indirectly owned by current or former Schellman & Company, LLC principals, directors, and executives, operates in an alternative practice structure with Schellman & Company, LLC. Schellman is also a PCI QSA, ISO certification body, FedRAMP 3rd Party Assessment Organization (3PAO) and current APEC Accountability Agent. Schellman provides compliance and certification services to a variety of companies, including PCI-DSS and PA-DSS assessments, FedRAMP assessments, HITRUST assessments, AICPA examinations (SOC 1, SOC 2, SOC 3), Penetration Testing services, ISO 27001, 27701, 9001, 20000, and 22301certifications, GDPR, CCPA and MS DPR examinations, and several other types of compliance assessments.

Conflicts of Interest

2. Schellman decisions, as an Accountability Agent, are based on objective evidence of conformity, or non-conformity, obtained by Schellman; decisions are not influenced by other interests or by other parties. Management is committed to impartiality in every manner of the certification services.

3. Schellman is aware that threats to impartiality may include, but not be limited to, any of the following.

   3.1. Self-interest threats: threats that arise from a person or body acting in their own interest. A concern related to certification, as a threat to impartiality, is financial self-interest.

   3.2. Self-review threats: threats that arise from a person or body reviewing the work done by themselves. Auditing the program requirements of an Applicant organization or Participant organization to whom Schellman provided consultancy would be a self-review threat.

   3.3. Familiarity (or trust) threats: threats that arise from a person or body being too familiar with or trusting of another person instead of seeking audit evidence.

   3.4. Intimidation threats: threats that arise from a person or body having a perception of being coerced openly or secretively, such as a threat to be replaced or reported to a supervisor.

4. Schellman performs an annual Independence Review which helps to identify, analyze and document the possibilities for conflict of interests arising from provision of certification, including any conflicts arising from its relationships. Having relationships does not necessarily present Schellman with a conflict of interest; however, if any relationship creates a threat to impartiality, Schellman shall

document and be able to demonstrate how it eliminates or minimizes such threats as a result of the annual Independence Review.

5. As part of the Independence Review, each employee is required to disclose personal relationships with the management or owners of any Applicant organization or Participant organization on an annual basis. Additionally, Schellman shall evaluate its finances and sources of income and demonstrate that on an ongoing basis, commercial, financial or other pressures do not compromise its impartiality. The results of the review are reviewed by human resources and management and potential conflicts are analyzed at that time. Threats identified as a result of the Independence Review that could impact the impartiality of the services provided by Schellman will be handled on a per-incident basis and where appropriate, Schellman will withdraw from the engagement.

6. Note that a relationship that threatens the impartiality of Schellman can be based on ownership, governance, management, personnel, shared resources, finances, contracts, marketing and payment of a sales commission or other inducement for the referral of new clients, etc.

Outsourcing

7. Schellman does not outsource any activities related to the certification services that it provides. All related certification services activities are performed by Schellman employees.

8. The decision for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing certification is not outsourced and is the sole responsibility of Schellman. Schellman is responsible for, and retains authority for, its decisions relating to certification services.

Key Elements of Independence for Certification Clients

9. Schellman will not offer or provide consulting or technical services related to the development or implementation of Participant organization's or Applicant organization's data privacy practices and procedures.

10. Schellman will not offer or provide internal audits to its certified clients.

11. Personnel handling sales for Schellman that may collect a sales commission will not be part of the certification audit team for an Applicant organization or Participant organization.

12. Schellman will not offer consulting or technical services related to the development of its privacy policy or statement or to its security safeguards.

13. Schellman will require personnel to reveal any situation known to them that may present them or Schellman with a conflict of interest. Schellman will use this information as input to identifying threats to impartiality raised by the activities of such personnel or by the organizations that employ them, and shall not use such personnel, internal or external, unless they can demonstrate that there is no conflict of interest. If a conflict of interest arises that can be cured by the existence of a safeguard, the existence of the affiliation between an Applicant organization or Participant organization and audit personnel will be disclosed to the Joint Oversight Panel. The communication will include the safeguards explanation and how these safeguards do not compromise the ability to render a fair decision to the Applicant organization or Participant organization. Such affiliations include, but are not limited to, the following:
    13.1. Officers of the Applicant organization or Participant organization serving on the Accountability Agent's board of directors in a voting capacity, and vice versa;
    13.2. Significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant organization or Participant organization, outside of the fee charged for certification and participation in the APEC PRP System; or
    13.3. All other affiliations which might allow the Applicant organization or Participant organization to exert undue influence on the Accountability Agent regarding the Applicant organization's certification and participation in the PRP System.

See Appendix A: Conflicts of Interest

Program Requirements

14. Schellman utilized the assessment criteria outlined in the template documentation developed by APEC to map the PRP Certification Program Requirements. Please see the attached Appendix B for the APEC assessment criteria and Schellman's PRP Program Requirements outlined in a separate document submitted with the application.

See Appendix B: PRP Framework Requirements

Certification Process

Client Assessment

15. During the initial assessment of a new client or a reassessment of an existing client, Schellman will perform a formal review to help ensure that engaging the client does not create a conflict of interest. The following requirements are considered during the assessment phase:

15.1. Certification shall not be considered or provided when a relationship poses an unacceptable threat to impartiality, such as a wholly owned subsidiary of Schellman requesting certification from its parent, and

15.2. Certification shall not be considered or provided for another Accountability Agent.

Scope and Planning

16. Based on information received from the organization, Schellman will determine the timing of the audit, assign the audit team members, and communicate to the organization the certification process, subsequent audits required to maintain certification, the dispute process, and any standard business terms applicable.

17. Upon agreement of the audit scope and timing between the client and Schellman, a job arrangement letter (JAL) or master services agreement (MSA) with a statement of work (SOW) will be documented to address the contractual agreements between the client and Schellman pertaining to the certification services. Upon execution of the JAL or MSA/SOW, Schellman will provide the client with preliminary planning documents, which include, but are not limited to, the following:

17.1. Project Calendar outlining the testing areas to be performed by audit team members during the dates of fieldwork and dates and deadlines subsequent to the on-site assessment;

17.2. Information Request List (IRL) that documents each piece of evidence that the audit will need to determine compliance with the framework; and

17.3. The PRP System Intake Questionnaire.

See Appendix C: PRP System Intake Questionnaire

Fieldwork Process

The fieldwork process includes the following activities:

18. Information gathering and analysis

18.1. Schellman will review the completed Intake Questionnaire provided by the client. Schellman will draft an IRL outlining the documentation to be provided by the client based on the responses from the completed Intake Questionnaire.

18.2. Schellman will review the documents provided by the client in response to the IRL provided to the client following the assessment criteria outlined within the Framework Requirements. Schellman will perform one or more testing procedures that includes inquiry, observation and inspection of documentation. The below table defines these testing procedures:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related requirement. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, policies, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing may involve tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling Guidelines

19. Schellman has established a standard sampling methodology. Non-statistical samples are used and each client environment is evaluated to determine the impact of multi-site locations on the population and suggested sample sizes.

20. For any clients with multi-site locations, the audit team must determine the sample sizes required by location. Explanations must be documented in the client project files for any deviations from the standard sampling guidelines.

See Appendix E: Sampling Guidelines

Identification of Non-Compliant Requirements

21. The audit team is responsible for communicating inconsistencies and requirements that are not compliant to appropriate client personnel in a timely manner. Information related to the non-compliant requirements must be included within internal memorandums and supporting audit documentation.

22. Upon notification of non-compliant requirements, the client must analyze, document, and take corrective actions to remedy the identified issues within the timeframe provided by Schellman. Details regarding the corrective actions must be submitted to Schellman for review. The audit team will review the corrective actions and perform subsequent or additional testing as applicable. The minimum program requirements must be compliant prior to granting certification.

Report Deliverables

23. Schellman will issue a written audit report upon completion of the fieldwork to the Applicant organization noting the organization's level of compliance with the program requirements. Where non-fulfillment or non-compliance of any of the program

requirements is found, the report must include a list of changes the Applicant organization needs to complete for purposes of obtaining certification for participation in the PRP System as well as the required timeframe for completion. The report will also outline the corrective actions, if those were communicated to Schellman by the Applicant organization.

24. If all requirements are compliant, the audit report will confirm compliance with the program requirements.

Certification Seal Policy

25. The Schellman certification seal is a service mark of Schellman. The Schellman certification seal may not be used in connection with any product or service that was not within the scope of the PRP certification review, or in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Schellman. The certification seal should be used only upon the granting or extending of a PRP certification.

26. Schellman provides public access to information about its certification process on the Schellman website (https://www.schellman.com/apec/prp-process#requirements). Information about the certification status that includes the granting, extending, maintaining, enforcing, renewing, suspending, reducing the scope of, or withdrawing of certification of any organization will be publicly provided through the website.

27. Schellman maintains a directory of valid certifications (https://www.schellman.com/apec-certificate-directory) that at a minimum show the name of the certified organization, a website for the certified organization and a link to the organization's privacy policy, contact information, the scope of the certification, the organization's original certification date, and the date that the current certification expires.

Ongoing Monitoring and Compliance Review Process

28. Participants are monitored throughout the certification period to ensure compliance with the program. The monitoring process may include periodic reviews of the Participant's privacy policy for updates or modifications. It may also include a review of any matters disclosed on the Participant's website, other than the privacy policy. Where changes or modifications occur that are not compliant with the program requirements, or result in significant changes, the recertification process will be immediately implemented as described below, which may include short-notice or unannounced audits.

29. Where there are reasonable grounds to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate

review process will be triggered whereby verification of compliance will be carried out. In these situations, the Compliant process, as outlined below, will be followed

30. The complaint process provides another method of on-going monitoring and compliance review during the certification period. Where non-compliance with any of the program requirements is found, Schellman will notify the Participant as outlined in the Complaint process outlined below. As the Complaint process outlines, Schellman will verify that the required changes have been properly completed by the Participant within the stated timeframe. At such time, the certification will be suspended until Schellman can verify that the Participant is in compliance with the requirements.

Recertification and Annual Attestation

31. In order for Participants to maintain their certification, recertification must take place at least every year following the date of initial certification.

32. There are occasions when Schellman must conduct audits of certified clients at short notice or unannounced to investigate complaints, or in response to changes, or as follow-up on suspended clients.

33. When Schellman determines that an unannounced or short-notice audit is required, Schellman describes and makes known in advance to the certified client the conditions under which these short-notice visits are to be conducted.

34. Prior to recertification, Schellman will determine adjustments to audit time and resources based on modifications to the client scope. Client personnel are required to disclose significant changes within their organization to Schellman.

35. The recertification process will include:

    35.1. An updated and completed PRP Intake Questionnaire provided by the client. Schellman will review the completed form looking for any changes since the initial certification.

    35.2. If there has been a material change, reasonably determined by the Accountability Agent, Schellman will perform a review process that will be similar to the initial certification fieldwork process as outlined above.

    35.3. An audit report will be provided to the Participant outlining the Accountability Agent's findings regarding the Participant's level of compliance with the program requirements. The report will include any areas of non-compliance and corrections the Participant needs to make to correct areas and the timeframe within which the corrections must be completed for purposes of obtaining recertification.

    35.4. If non-compliance areas were found during the recertification process, Schellman will review documentation provided by the Participant to verify that

correction has been completed and is compliant, prior to obtaining recertification.

35.5. Upon verification that the requirements are in compliance, a final report will be provided to the Participant as notice of compliance with the program requirements and that the Participant has been recertified.

Complaint Process

36. Schellman utilizes its current dispute process to receive, investigate and resolve complaints about Participants. The complaint process is handled by Schellman and is not outsourced. Additionally, the complaint process is available via the Schellman website and is outlined below.

Receiving Complaints and Consent

37. Any complaint is required to be formally submitted using the form at https://www.schellman.com/apec/stats, whether the complaint is filed by the individual or the personal information controller. The complaint should include the reason for complaint, the date of the complaint, and any evidence supporting the complaint. The form will include a consent to share any personal information with the relevant enforcement authority in connection with a request for assistance. Submission, investigation, and decision on complaints do not result in any discriminatory actions against the complainant.

38. Each complaint is logged and recorded including the date the complaint was received and by whom it was received.

39. Each complaint will be investigated to determine whether it concerns the Participant's obligations under the program and if the complaint falls within the scope of the certification and requirements. The nature and duration of the investigation will vary depending on the complaint that was submitted, and the complainant will receive an update, at a minimum, once per month on the status of their complaint.

40. Where the complaint is from an individual and concerns the processing of his/her personal information and the Participant's obligations under the program, the complaint will be forwarded to the Participant within five business days. Schellman will require confirmation from the Participant that the complaint was forwarded to the personal information controller, if the controller can be identified and whose contact information is available.

Complaint Notification

41. Once the complaint is received, the individual that submitted the complaint will be notified to confirm the complaint and the determination made based on the review outlined above. A confirmation of receipt of the complaint is required to be provided to the individual submitting the complaint within five business days. The

confirmation will include verification that the complaint was forwarded to the Participant, if the complaint was filed by an individual.

Complaint Resolution

42. If noncompliance was found with any of the program requirements, Schellman will contact the Participant outlining the details of the noncompliance that require remediation and the required timeframe for completion. At such time, the certificate will be suspended.

43. The Participant is required to provide evidence of remediation within the required timeframe for the certification to be reinstated. If the Participant fails to provide sufficient evidence, during the required timeframe, or is not responsive, the certification will remain suspended. The timeframe shall not exceed a period of six (6) months or upon the due date of the annual recertification.

44. If Schellman receives sufficient evidence of the remediation within the required timeframe, the suspension will be removed and the certificate will be reinstated.

45. Schellman will provide written notice of complaint resolution and closure to the complainant and the Participant.

Publicly Available Statistics

46. Schellman will include statistics on the types of complaints received by Schellman and the outcomes of such complaints on the company website, that is publicly available. This information will be provided to the FTC and the Joint Oversight Panel during recertification or as required to be reported.

See Appendix D: Complaint Statistics Template

Mechanism for Enforcing Program Requirements

47. Schellman has the authority to enforce its program requirements against clients, or Participants, through the JAL or MSA/SOW. Schellman has the authority to suspend, withdraw, or reduce the scope of a certification under just cause and as a result of reasonable evidence.

48. Certification shall be suspended in cases when, for example:

    48.1. The client was found to be in noncompliance within the scope of the program's requirements throughout the certification period, including identification during the initial certification; recertification; ongoing monitoring; or the complaint process, and the findings have not been resolved within the required timeframes, which shall not exceed a period of six (6) months or upon the due date of the annual recertification;

48.2. The certified client does not allow recertification audits to be conducted at the required frequencies;

48.3. Where there are reasonable grounds to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements; or

48.4. The certified client has voluntarily requested a suspension.

49. As previously noted, if noncompliance was found with any of the program requirements, Schellman will contact the Participant outlining the details of the noncompliance that require remediation and the required timeframe for completion.

50. The certificate is suspended until the Participant has provided sufficient evidence of the remediation within the required timeframe, which shall not exceed a period of six (6) months or upon the due date of the annual recertification. Upon receipt of sufficient evidence of remediation within the required timeframe, Schellman will perform a review of the evidence to determine if the certificate should be reinstated. The results are communicated to the client via an audit report. Failure to resolve the issues that have resulted in the suspension in the time established by Schellman will result in withdrawal or reduction of the scope of certification, if applicable.

    A reduction in the scope of the certification may be applicable and would exclude the parts not meeting the requirements, when the client has persistently or seriously failed to meet the program requirements for those parts of the scope of certification.

51. Under suspension, the client's certification is temporarily invalid. Included within the JAL or MSA/SOW are the enforceable arrangements regarding the suspension of the certification to help ensure, that in case of suspension, the client refrains from further promotion of its certification and use of the Schellman certification seal. Schellman will make publicly accessible the suspended status of the certification.

52. Schellman is required to refer the violation to the Federal Trade Commission, where a reasonable belief is pursuant to its established review process that a client's failure to comply with the APEC PRP System has not been remedied within a reasonable time, so long as such failure to comply can be reasonably believed to be a violation of applicable law. Schellman will respond to requests from enforcement entities in APEC Economies that reasonably relate to that Economy and to the PRP related activities of Schellman.

53. If the determination is to withdrawal the certification, Schellman, as included in the JAL or MSA/SOW, has enforceable arrangements with the Participant concerning conditions of withdrawal, ensuring upon notice of withdrawal of certification that the client discontinues its use of all advertising matter that contains any reference to a certified status.

54. Upon request by any party, Schellman will correctly state the status of certification of the participant, or client, as being suspended, withdrawn, or reduced.

PRP Framework: Appendices

Appendix A: Conflicts of Interest Policy

CONFLICTS OF INTEREST

All employees have a duty to further the Company's aims and goals, and to work on behalf of its best interest. Employees should not place themselves in a position where the employee's actions or personal interests may be in conflict with those of the Company.

Examples include, but are not limited to, the following:

- Self-interest threats: threats that arise from a person or body acting in their own interest. A concern related to certification, as a threat to impartiality, is financial self-interest.
- Self-review threats: threats that arise from a person or body reviewing the work done by themselves. Auditing the program requirements of an Applicant organization or Participant organization to whom Schellman provided consultancy would be a self-review threat.
- Familiarity (or trust) threats: threats that arise from a person or body being too familiar with or trusting of another person instead of seeking audit evidence.
- Intimidation threats: threats that arise from a person or body having a perception of being coerced openly or secretively, such as a threat to be replaced or reported to a supervisor.
- Officers of the Applicant organization or Participant organization serving on the Accountability Agent's board of directors in a voting capacity, and vice versa.
- Significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant organization or Participant organization, outside of the fee charged for certification and participation in the APEC CBPR or PRP System.
- All other affiliations which might allow the Applicant organization or Participant organization to exert undue influence on the Accountability Agent regarding the Applicant organization's certification and participation in the CBPR or PRP System.

Employees should report to their manager any situation or position (including outside employment by the employee or any member of the employee's immediate household) which may create a conflict of interest with the Company. Additionally, employees are required to complete an annual independence review and disclose any potential conflict of interest. Human resources and management review the results from the annual independence review. Having relationships does not necessarily present the Company with a conflict of interest; however, if any relationship creates a threat to impartiality, the Company is required to document and be able to demonstrate how it eliminates or minimizes such threats. Threats identified as a result of the Independence Review that could impact the impartiality of the services provided by Schellman will be handled on a per-incident basis and where appropriate, Schellman will withdraw from the engagement. If a conflict of interest arises that can be cured by the existence of a safeguard, the existence of the affiliation between an Applicant organization or Participant organization and audit personnel will be disclosed to the Joint Oversight Panel. The communication will include the safeguards explanation and how these safeguards do not compromise the ability to render a fair decision to the Applicant organization or Participant organization.

Schellman is solely responsible for the decisions for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing certification. Schellman does not outsource any activities related to the certification services that it provides. Schellman also does not offer or provide consulting or technical services to any client includes those services related to the development or implementation of Participant organization's or Applicant organization's data privacy practices and procedures. Schellman does not perform internal audits for any client. Personnel handling sales for Schellman that may collect a sales commission will not be part of the certification audit team for an Applicant organization or Participant organization.

Appendix B: PRP Framework Requirements

SECURITY SAFEGUARDS

Please note the additional column to the far right for mapping of Schellman's Certification Requirements to these APEC PRP Framework Requirements. The yellow highlight serves to provide easy reference to the mapped areas.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	*Security Safeguards* 1. Implement an information security policy that covers personal information processed on behalf of a controller.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (e.g. password protections) • Encryption • Boundary protection (e.g. firewalls, intrusion detection) • Audit logging • Monitoring (e.g. external and internal audits, vulnerability scans) • Other (specify) The Applicant must periodically review and reassess these measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle	*Security Safeguards* 2. Implement physical, technical and administrative safeguards that may include the following and periodically review and reassess the implemented measures to evaluate their relevance and effectiveness: • Authentication and access control (e.g. password protections) • Encryption • Boundary protection (e.g. firewalls, intrusion detection) • Audit logging • Monitoring (e.g. external and internal audits, vulnerability scans)

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
3. Describe how your organization makes employees aware of the importance of maintaining the security of personal information.	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	*Security Safeguards* 3. Implement regular training and oversight of employees to ensure they are aware of the importance of, and obligations for, respecting and maintaining the security of personal information. Procedures may include the following: • Documented training program for employees • Regular staff meetings or other documented communications • Security policy signed by employees
4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such measures is required for compliance with this principle.	*Security Safeguards* 4. Implement measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information. The measures implemented should be tested on a periodic basis and measures should be adjusted to reflect the results of the tests.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	*Security Safeguards* 4. Implement measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information. The measures implemented should be tested on a periodic basis and measures should be adjusted to reflect the results of the tests.
6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?	The Accountability Agent must verify that the Applicant has in place appropriate processes to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information.	*Security Safeguards* 5. Implement a notification process to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information.
7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	*Security Safeguards* 6. Implement procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
8. Does your organization use third-party certifications or other risk assessments? Please describe.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	*Security Safeguards* 7. Perform periodic third-party certifications or other risk assessments and adjust the security safeguards to reflect the results of these certifications or risk assessments.

ACCOUNTABILITY MEASURES

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
9. Does your organization limit its processing of personal information to the purposes specified by the controller?	The Accountability Agent must verify that the Applicant has policies in place to limit its processing to the purposes specified by the controller.	*Accountability Measures* 1. Implement policies to ensure that processing of personal information is limited to the purposes specified by the controller.
10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?	The Accountability Agent must verify that the Applicant has measures in place to delete, update, and correct information upon request from the controller where necessary and appropriate.	*Accountability Measures* 2. Implement procedures to delete, update, and correct information upon request from the controller where necessary and appropriate.
11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.	The Accountability Agent must verify that the Applicant indicates the measures it takes to ensure compliance with the controller's instructions.	*Accountability Measures* 3. Implement measures to ensure compliance with the controller's instructions related to the activities of personal information processing.
12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the PRP?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with the PRP. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with the PRP.	*Accountability Measures* 4. Appoint an individual(s) to be responsible for the overall compliance with the requirements of the PRP.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to handle, or forward to the controller as appropriate, privacy-related complaints or requests. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	*Accountability Measures* 5. Implement procedures to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller.
14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place for notifying the controller, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	*Accountability Measures* 6. Implement procedures to notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information. 9.. Regularly train employees on the organization's privacy policies and procedures and related client instructions.
15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors?	The Accountability Agent must verify that the Applicant has in place a procedure to notify controllers that the Applicant is engaging subprocessors.	*Accountability Measures* 7. Notify the controller of your engagement of subprocessors.
16. Does your organization have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP? Please describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of each type of mechanism described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such mechanisms is required for compliance with this principle.	*Accountability Measures* 8. Implement mechanisms with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
17. Do the mechanisms referred to above generally require that subprocessors: a) Follow instructions provided by your organization relating to the manner in which personal information must be handled? b) Impose restrictions on further subprocessing c) Have their PRP recognized by an APEC Accountability Agent in their jurisdiction? d) Provide your organization with self assessments or other evidence of compliance with your instructions and/or agreements/contracts? If **YES**, describe. e) Allow your organization to carry out regular spot checking or other monitoring activities? If **YES**, describe. f) Other (describe)	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	*Accountability Measures* 8. Implement mechanisms with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP. Mechanisms should require subprocessors to perform the following: • Follow-instructions provided by your organization relating to the manner in which personal information must be handled • Impose restrictions on further subprocessing • Have their PRP recognized by an APEC Accountability Agent in their jurisdiction • Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts • Allow your organization to carry out regular spot checking or other monitoring activities

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place for training employees relating to personal information management and the controller's instructions. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this requirement.	*Accountability Measures* 9. Regularly train employees on the organization's privacy policies and procedures and related client instructions.

Appendix C: PRP System Intake Questionnaire

1) Name of the Organization that is seeking certification:
   _____

2) List of subsidiaries and/or affiliates to be covered by this recognition, their location, and the relationship of each to you:
   _____

Name of subsidiary and/or affiliate	Location of subsidiary and/or affiliate	Relationship of affiliate and/or subsidiary to you

3) Organization's Contact Point for PRP
   Name: _____
   Title: _____
   Email: _____
   Phone: _____

4) For what offering(s) or type(s) of processing service(s) are you applying for recognition?
   _____

SECURITY SAFEGUARDS (QUESTIONS 1-8)

The questions in this section are directed towards ensuring that when individuals entrust their information to an organization, their information will be protected with reasonable security safeguards to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification or disclosure of information or other misuses.

1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?

   _____ Y _____ N

2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.

3. Describe how your organization makes employees aware of the importance of maintaining the security of personal information.

4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?

   _____ Y _____ N

5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.

   _____ Y _____ N

6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?

_____ Y _____ N

7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?

_____ Y _____ N

8. Does your organization use third-party certifications or other risk assessments? Please describe.

_____ Y _____ N

ACCOUNTABILITY (QUESTIONS 9-18)

The questions in this section are directed towards ensuring that you are accountable for complying with measures that give effect to the Principles stated above. Additionally, when transferring information, you should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.

9. Does your organization limit its processing of personal information to the purposes specified by the controller?

_____ Y _____ N

10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?

_____ Y _____ N

11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.

_____ Y _____ N

12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the PRP?

_____ Y _____ N

13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?

_____ Y _____ N

14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information?

_____ Y _____ N

15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors?

_____ Y _____ N

16. Does your organization have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP? Please describe.

_____ Y _____ N

17. Do the mechanisms referred to above generally require that subprocessors:

- Follow-instructions provided by your organization relating to the manner in which personal information must be handled?_____
- Impose restrictions on further subprocessing? _____
- Have their PRP recognized by an APEC Accountability Agent in their jurisdiction? _____
- Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If **YES**, describe. _____
- Allow your organization to carry out regular spot checking or other monitoring activities? If **YES**, describe. _____
- Other (describe) _____

18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.

_____ Y _____ N

Appendix D: Complaint Statistics Template

Complaint Numbers

The total number of complaints will be reported. Where no complaints are received, the complaint statistics template will indicate “none” to ensure it is clear that no complaints were received that year. The number of complaints will be listed by year so that its clear regarding the number of new complaints received as well as older complaints carried over from the previous reporting period.

To assist readers to understand the reported figures and to aid in comparability there will be a note that the number reflects and actual and confirmed complaint rather than an inquiry.

Complaint Processing and Outcomes

A description of the process will be outlined.

A listing of the number of the outcomes of each complaint by the following types will be included:

- Complaints received that were outside of the scope of the program requirements or were not covered by the PRP program
- Complaints that were forwarded to the Participant
- Complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority
- Complaints received that were incomplete or the complainant was unresponsive to additional information requirements

Complaints Type

This section will include informative breakdowns of the complaints by type to provide a statistical picture of who is complaining and why.

The complaint types will be listed in the following categories:

- Complaint subject matter broken down by APEC information privacy principle (security safeguards and accountability);
- Information about complainants, when known, including the economy from which complaints have been made and industry;
- Information about the type of respondents to complaints, including industry classification (e.g. financial service activities, insurance) and size of company (e.g., small, mid-market, or large).

While some complaints will raise several different issues, the report will provide the basis upon which Schellman is reporting, for example, the principal aspect of the complaint.

Complaints Process Quality Measures

This section will outline how well the complaints resolution system is working. The timeliness of the processing will be reported, including the number or complaints that took longer than the target date to resolve.

General

Schellman will provide a comment on the various figures reported at the end of the reporting period as compared to previous periods to set the statistics in context.

Appendix E: Sampling Guidelines Policy

In some cases, an auditor may need to inspect a sample of documents. Sampling should first validate consistency amongst like systems (build, version, patch levels), employee processes and procedures (through interviews), locations, and requisite documentation. Schellman selects the sample size based on the validated consistency (e.g., number of relevant systems, process events). Where variances or non-compliance occurred, Schellman required additional samples. Sampling guidelines are defined in the table shown below.

Sampling Guidelines

No Exceptions (No areas of Non-Compliance)	Testing Exception(s)/Non-Compliance
Test at least 25% of the population up to a total sample size 25	Increase sample to 40% of the population up to a total sample size of 40

NOTE: Sample testing should be described within the project files.