I. Introduction ........................................................................................................................................2
   A. Purpose ........................................................................................................................................................................................................2
   B. Participants.................................................................................................................................................................................................2
   C. Scope of Work ..........................................................................................................................................................................................2
   D. Limitations...................................................................................................................................................................................................3

II. The Standards ...................................................................................................................................3
   A. Objective ......................................................................................................................................................................................................3
   B. Process ..........................................................................................................................................................................................................3
   C. Quality Assurance ...................................................................................................................................................................................5

III. Glossary .............................................................................................................................................5

IV. Administration .................................................................................................................................6
   A. SCA Standards Contact Information .............................................................................................................................................6
   B. Issue Date: April 30, 2018.....................................................................................................................................................................6
   C. Compliance Date: May 31, 2019 .............................................................................................................................................................6
   D. Revision History: Version 1.0 – Released April 30, 2018........................................................................................................6

V. References .........................................................................................................................................6
   A. Shared Assessments - Standard Information Gathering questionnaire and Standardized Control
      Assessment procedures – Outsourcing Relationships Overview ............................................................................................6
I. INTRODUCTION

A. Purpose

These standards are intended for use by any third party risk assessor that utilizes the 2018 Shared Assessments Standardized Control Assessment (SCA) procedures - formerly the Agreed Upon (AUP) procedures. The SCA is an objective set of testing procedures to be used and followed when performing third party control validation assessments. These procedures align with the Shared Assessments Standardized Information Gathering (SIG) questionnaire.

1. These standards are provided in addition to Shared Assessments materials developed, released, licensed and distributed to support the examination of controls related to risk domains, control areas, procedures and execution of third party assessments.

2. Members of the Shared Assessments Program can use the SCA procedures.

3. Outsourcers or Assessee who purchase a Standardized Control Assessment license can use the SCA procedures.

4. Assessment Firms can utilize a licensed version of the SCA procedures, which relate to the planning, execution, reporting and distribution of an SCA Engagement.

5. Certified Public Accountants can use the SCA procedures when performing an Agreed Upon Procedures, or other attestation engagement.

B. Participants

Typically participants planning and performing an SCA include an: Outsourcer, Assessee and Assessor, (and if needed a Shared Assessments Program Facilitator).

1. Outsourcer(s) - The company which contractually engages an Assessee (Third Party) to utilize their products and/or perform specific services, which are provided to assist the Outsourcer in meeting their strategic objectives and business requirements. The Outsourcer must ensure that controls covering specific products and/or services received from the Assessee are adequate and sufficient to meet the Outsourcer’s risk appetite and control requirements. Note: If multiple Outsourcers use the same products/services from a common Assessee and agree to pay for or partially pay for a Collaborative SCA Engagement (Page 5), the Assessee would be able to leverage the resultant SCA Report, if they:

   a. Agree on the independent Assessment Firm (Assessor) to be used;

   b. Confirm the economic model that will be used to pay for the independent Assessment Firm;

   c. Establish the timing associated with delivery of the resultant report to meet any of their internal policy, control and compliance requirements;

   d. Agree to the products/services, risk domains, controls and testing procedures to be included as part of the assessment;

   e. Agree to the Assessee location(s) to be included in the assessment; and

   f. Agree to the period of time being used for the assessment.

2. Assessee - The company (vendor/third party) which provides products/services to an Outsourcer(s) and must demonstrate to the Outsourcer(s) that controls are in place and operational to identify and mitigate potential risks associated with those products/services, inclusive of any work the Assessee may have assigned to Subcontractors.

3. Assessor – Subject matter expert(s) will perform the SCA procedures. Typically, these experts are resident in external Assessment Firms or, in cases when an SCA is being performed on internal processes, expertise is found within internal control functions. Note: If the Assessor is an Assessment Firm, the Outsourcer or the Assessee will typically contractually engage the Assessment Firm to perform the SCA assessment.

C. Scope of Work

Typically identifies the areas within the Assessee’s environment that will be included within scope of the assessment.

1. The Outsourcer and the Assessee will define and agree upon the scope of work the SCA procedures will cover, to include:

   a. Products/services provided to an Outsourcer,

---

1 See References – SA SIG and SCA Outsourcing Relationships and Terms Definitions (Page 6).
b. Risk domains and control areas of the SCA to be performed which are pertinent for the products/services provided and agreed with the Outsourcer;

c. Understand the supporting documentation requirements needed to validate the controls for the procedures performed.

• Agree with the Assessee on any sharing conditions/obligations, which should be specified in the contractual agreement between the Assessee and the Assessment Firm, and

d. Period of time the assessment covers;

e. Expected duration of the assessment; and


2. The Assessor/Assessment Team to perform the SCA scope of work, will:

a. Ensure required certifications are present, which are:

• The Lead Assessor for an SCA Engagement must hold a Shared Assessments Certified Third Party Risk Assessor (CTPRA) Certification and a Certified Third Party Risk Professional (CTPRP) Certification.

• The Assessors who perform an onsite control validation assessment are encouraged to obtain the CTPRA Associate certification.

• The Assessors performing a SA SIG and or a SA SCA must hold the corresponding SIG or SCA Add-On certification for CTPRP and CTPRA Certification holders. Note: If SCA procedures are used to perform an internal control assessment and the SCA results will not be shared with external parties, then the Assessor certification requirements do not apply.

b. Ensure there is a clear understanding of the risk domains, control areas to be assessed and the procedures to be used to validate controls.

c. Understand the supporting documentation requirements needed to validate the controls for the procedures performed.

• Agree with the Assessee on any sharing conditions/obligations, which should be specified in the contractual agreement between the Assessee and the Assessment Firm.

• Agree with Assessee on any restrictions, limitations or requirements for sharing the SCA Report.

D. Limitations

The following items either limit the use of the SCA or the distribution of the resultant report:

1. The Assessee and/or the Outsourcer must:

a. Hold a license to use the SCA; and

b. Agree on the procedures to be performed.

2. The Assessment Firm (Assessor) must be a member of the Shared Assessments Program and hold a license to the SCA.

3. All parties must:

a. Acknowledge that the SCA Report does not provide an opinion (attestation) and is designed solely to depict the results of testing procedures performed;

b. Agree to conditions on how the resultant report can be shared; and

c. If shared with multiple Outsourcers, the report distribution and sharing conditions are clearly understood and agreed prior to work commencing.

II. THE STANDARDS

A. Objective

These standards are provided to further ensure consistency related to the execution and reporting of an SCA Engagement. The use of the procedures, determined to be in scope and contained in the SCA, by an Assessor/Assessment Team to perform and validate the presence of expected controls to mitigate the risk associated with the products and services provided by an Assessee to an Outsourcer (clients). The SCA procedures are reviewed annually and updated as needed by the Shared Assessments Program.

B. Process

1. Identification and Responsibilities of Participants:

a. The Assessee – Confirms resource and funding availability, when considering using an SCA in order to provide Outsourcers with sufficient detail regarding the Assessee controls. Using standardized testing procedures improves the efficiency of the assessment for all parties and
reduces the number of control assessments performed. Other efficiencies can be achieved by identifying additional Outsourcers that utilize similar services within the scope of the SCA and controls being assessed and sharing the SCA Report.

b. The Outsourcer – Obtains senior management agreement to the approach to be used. Agrees that the procedures to be performed will satisfy their control requirements, and confirms no pre-existing contractual requirements exist that specify a specific assessment methodology to be used.

c. The Assessor – Can be an internal individual or team comprised of qualified subject matter expert(s) from the Assessee, an Assessment Firm or from the Outsourcer who perform the SCA procedures.

2. Planning and Approach would include all of the following items, a-h:

a. Confirm version of SCA to be utilized:
   • Procedures included in the SCA are the standard procedures to be used for the controls determined to be in scope, when conducting an SCA Engagement; and
   • Confirm single or Collaborative SCA Engagement.

b. If multiple organizations from the same industry are considering a Collaborative SCA Engagement, those firms may need to confirm that the SCA procedures meet their specific industry regulations and individual organizational requirements. If any additional procedures are defined by those firms, they will be provided to the Shared Assessments Program for inclusion consideration. Identify and confirm resources, budget, timing, etc., as necessary to support performing the assessment.

c. Verify with participants that no restrictions exist on assessment approach to be used.

d. Select, confirm and engage external assessment firm, if used, and agree that the Assessee and the Assessment Firm selected have no limitations on the shareability of the report.

e. Ensure procedures to be performed are identified, reviewed, understood and agreed by the participants.

f. Ensure there is a clear understanding of documentation required to support the results of the control procedure(s) tested.

g. Agree to document the results of the assessment using the SCA Report Template.

h. Agree to hold regular status meeting to report progress.

3. SCA Engagement Scoping:

a. Assessee/Assessor confirm scope and consider, for example, such items as:
   • Understanding of the environment and documentation available to verify controls;
   • Any systems associated with the provision of services to an Outsourcer;
   • Any software development associated with the provision of services to an Outsourcer;
   • Any information security, privacy or business resiliency requirements associated with the provision of services to an Outsourcer.

b. Determine and document the order in which the procedures within scope will be executed.

4. Performing the SCA Engagement:

a. Risk Domains - The SCA provides objective and consistent procedures to evaluate key cybersecurity and risk management controls in the following risk domains:

<table>
<thead>
<tr>
<th>Risk Domains</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Risk Assessment and Treatment</td>
<td>J. Incident Event and Communications Management</td>
</tr>
<tr>
<td>B. Security Policy</td>
<td>K. Business Resiliency</td>
</tr>
<tr>
<td>C. Organizational Security</td>
<td>L. Compliance</td>
</tr>
<tr>
<td>D. Asset and Information Management</td>
<td>M. End User Device Security</td>
</tr>
<tr>
<td>E. Human Resources Security</td>
<td>N. Network Security</td>
</tr>
<tr>
<td>F. Physical and Environmental Security</td>
<td>P. Privacy</td>
</tr>
<tr>
<td>G. Operations Management</td>
<td>T. Threat Management</td>
</tr>
<tr>
<td>H. Access Control</td>
<td>U. Server Security</td>
</tr>
<tr>
<td>I. Application Security</td>
<td>V. Cloud Hosting</td>
</tr>
</tbody>
</table>
b. Control Areas - Each SCA Control Area contains:
   • Objective(s): Statements describing the business interest behind assessing the controls within the risk domain;
   • Risk Statement(s): Statements describing the risk exposure if the control is not present;
   • Control(s): Statements about the Assessee’s controls that should be in place;
   • Procedure(s): Action statements an assessor will perform to verify each control statement; and
   • Industry Reference(s): As appropriate are included in the SCA procedures.

c. Procedures - Specific procedures that will be executed to:
   • Capture and validate the presence and operational nature of the controls.

5. Report Issuance and Sharing Results:
   a. The SCA Report does not express an opinion and covers only those procedures performed under the scope of the assessment.
   b. Utilize the SCA Report Template to document the results of the SCA Engagement.
   c. The Assessee/Outsourcer will share the SCA Report, in accordance:
      • With any conditions/obligations specified in the contractual agreement between the Assessee and the Assessment Firm; and
      • With their internal procedures for sharing confidential material.
   d. The Assessee can provide a Management Response report to communicate why any procedures performed resulted in identified controls that were not present. Note: Management Response must be a separate document from and not included in the SCA Report.
   e. The Assessee should consider an administrative function which shows which Outsourcers have received the SCA report to:
      • Confirm the SCA report conforms to the Outsourcer’s control requirements; and
      • Ensure the Assessee works with the Outsourcer to establish a remediation plan to address any identified specific control weaknesses.

C. Quality Assurance
   1. The Outsourcer or Assessee will ensure that the Assessment Firm they engaged, has:
      a. An executed contractual agreement;
      b. The necessary industry qualification and Shared Assessments certifications;
      c. Performed the engagement in accordance with their own internal quality assurance practices; and
      d. Verified the Assessment Firm is a current member of the Shared Assessments Program.
   2. When the SCA is being used to perform an internal control evaluation of the Assessee and the results and or report will not be shared with any Outsourcer, these Quality Assurance requirements may not be applicable.

III. Glossary

Affiliate – An entity under the Outsourcer’s effective control.

Assessee – An entity (organization) being assessed and either performs work on behalf of an Outsourcer or is being considered for such a role. The Assessee is always independent of the Outsourcer, except that in those instances where the Outsourcer is evaluating its own controls and work processes. The Outsourcer also assumes the role of the Assessee in Shared Assessments evaluations and associated materials.

Assessor – A team comprised of qualified subject matter experts from the Outsourcer, Assessee or an independent Assessment Firm, who will perform the SCA procedures. If the Assessor is an Assessment Firm, the Assessee or the Outsourcer will typically contractually engage the Assessment Firm to perform the SCA procedures.

Collaborative SCA Engagement – In the absence of an existing control assessment that meets Outsourcer requirements, a Shared Assessments Collaborative SCA Engagement may be performed by an Assessor on behalf of multiple Outsourcers when the Outsourcers leverage common services from a Service Provider (Assessee) and agree the SCA Report meets the Outsourcers’ specific control requirements. Such a standardized risk assessment approach improves control validation.
assessments, thereby achieving economies and scalability for Outsourcers as well as their Assessees by:

- Producing a robust, repeatable, consistent methodology that can be leveraged by any Assessor (independent Assessment Firm or in-house assessor);
- Utilizing a standardized set of control procedures for determining an Assessees’ risk posture in a way that accommodates individual Outsourcers’ risk tolerances; and
- Reducing time and expense of conducting multiple Assessee control validation assessments.

**Outsourcer** – An entity delegating a function to the independent Assessee or is considering doing so. The Outsourcer is the entity receiving the Assessee’s assessment results. In those instances, where the Outsourcer assesses itself, the Outsourcer also assumes the role of the Assessee in Shared Assessments evaluations and associated materials.

**Shared Assessments Program Facilitator** – An individual from The Santa Fe Group – who can act as a resource to address questions and coordinate activities, as appropriate, when performing a Collaborative SCA Engagement.

**Subcontractor** – An entity independent of and directly performing tasks for the Assessee being evaluated. The subcontractor (fourth party) is ultimately doing work on behalf of the Outsourcer.

**IV. Administration**

1. SCA Standards Contact Information
   P: (505) 466-6434
   F: (505) 466-3111
   E: info@santa-fe-group.com

2. Issue Date: April 30, 2018

3. Compliance Date: May 31, 2019

4. Revision History: Version 1.0 – Released April 30, 2018

**V. References**

1. SA SIG and SCA Outsourcing Relationships and Terms Definitions.

---

**SA SIG AND SCA OUTSOURCING RELATIONSHIPS AND TERMS DEFINITIONS**

The terms used to describe different entities in both the Shared Assessments SIG and SCA are always defined from the perspective of the entity being assessed.

---

**THE OUTSOURCER**

The Outsourcer is the entity delegating a function to the independent Assessee, or is considering doing so. The Outsourcer is the entity receiving the Assessee’s evaluation. In those instances where the Outsourcer assesses itself, the Outsourcer also assumes the role of the Assessee in SA evaluations and associated materials.

**THE AFFILIATE**

The Affiliate is any entity under the Outsourcer’s direct control. Affiliates are Assessees when being evaluated by a parent organization.

**THE ASSESSEE**

The Assessee is the entity being evaluated and either performs work on behalf of the Outsourcer or is being considered for such a role. The Assessee is always separate from the Outsourcer, except in those instances where the Outsourcer is evaluating its own work processes. When evaluating its own work processes the Outsourcer also assumes the role of the Assessee in SA evaluations and associated materials.

**THE SUBCONTRACTOR**

The Subcontractor is an entity independent of and directly performing tasks for the Assessee being evaluated. The Subcontractor is ultimately doing work on behalf of the Outsourcer.

---

There are three use cases typically associated with Shared Assessments processes: (1) when an entity conducts due diligence on a vendor prior to engagement; (2) when an entity assesses a vendor in the course of business; and (3) when an entity uses SA tools to assess its own internal processes.

Notes: Arrows in diagram depict work flow direction. Defined terms are capitalized.
The Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, the trusted source in third party risk assurance, is a member-driven, industry-standard body with tools and best practices, that injects speed, consistency, efficiency and cost savings into the control assessment process. Shared Assessments Program members work together to build and disseminate best practices, building resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments.

P: (505) 466-6434
F: (505) 466-3111
E: info@santa-fe-group.com
© 2018 The Santa Fe Group, Shared Assessments Program. All Rights Reserved.

SHARED ASSESSMENTS – STEERING COMMITTEE
SCA STANDARDS SUBCOMMITTEE

Thank you for the Shared Assessments members who contributed to this work.

- **Angela Dogan**, Director of Vendor Risk and Compliance Services, LYNX Technology Partners, Inc.
- **Gaurav Dhawan**, Senior Manager, EY
- **Shane Hasert**, AVP Business Compliance, Radian Group
- **Brad Keller**, Senior Director, Third Party Risk Strategy, Prevalent Inc.
- **Paul Kooney**, Managing Director, Protiviti Inc.
- **Shawn Malone**, CEO, Security Diligence LLC
- **Don Williams**, Principal Consultant, Churchill and Harriman

SFG STAFF

- Charlie Miller; Bob Jones; Gary Roboff; Mike Jordan; Robin Slade; Marya Roddis