SHARED ASSESSMENTS

THIRD PARTY RISK MANAGEMENT TOOLKIT

Voluntary Guidelines for Performing a Shared Assessments Standardized Control Assessment (SCA)

Version 6.1 September 29, 2021

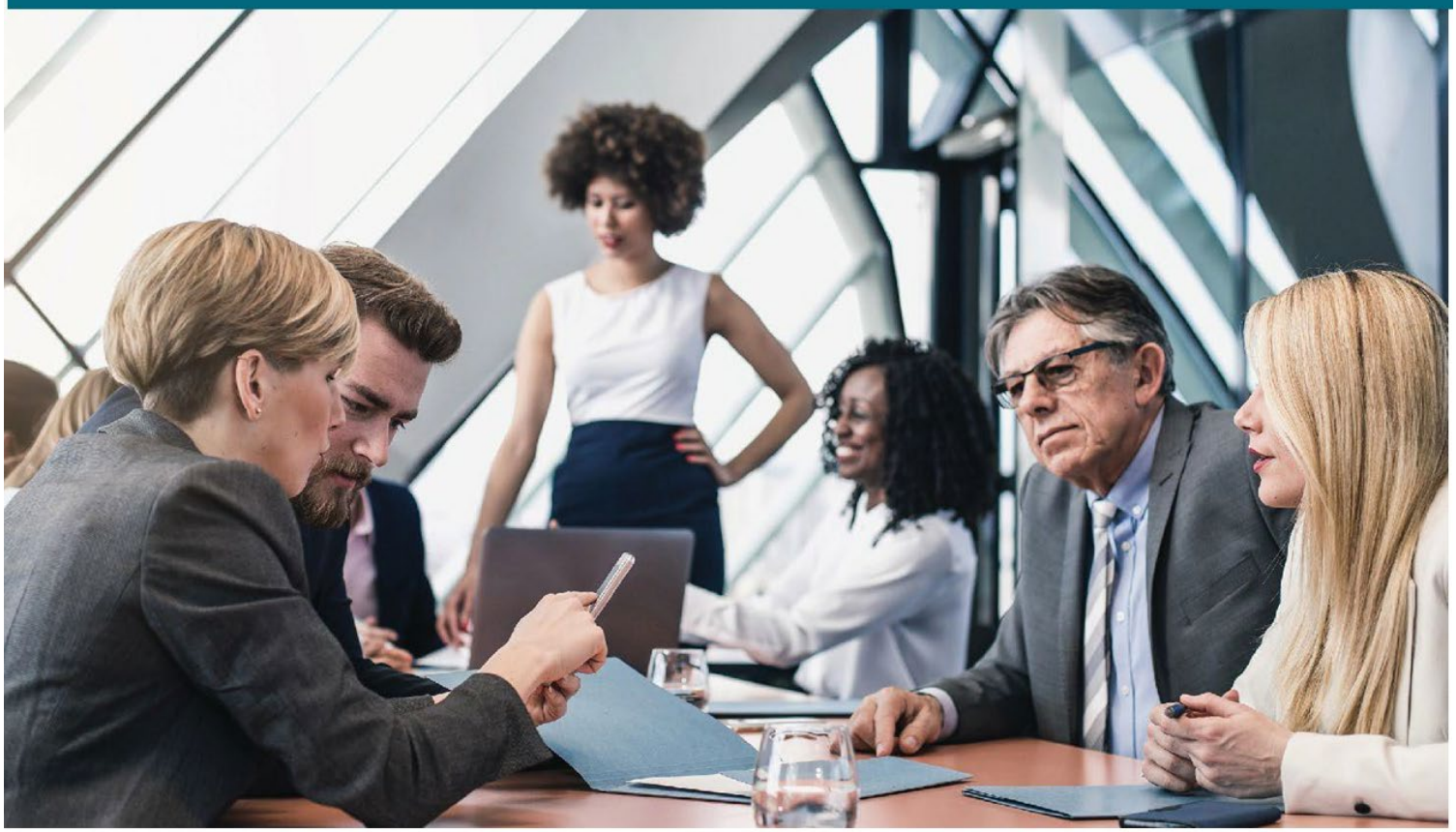

TABLE OF CONTENTS

I. INTRODUCTION & PURPOSE

The Standardized Control Assessment (SCA) is an objective set of testing procedures to be used and followed when performing third party control validation assessments. The SCA Procedures provide risk professionals a set of resources (tools, templates, checklists, guidelines) that can be used to plan, scope, and perform third party risk assessments.

A. PURPOSE OF THE VOLUNTARY GUIDELINES

These voluntary guidelines are intended for use by any third party risk assessor that utilizes the Shared Assessments Standardized Control Assessment (SCA) procedures – formerly known as the Shared Assessments' Agreed Upon (AUP) procedures.

SCA voluntary guidelines are provided in addition to other Shared Assessments materials and resources that are developed, released, licensed, and distributed for use in execution of third party assessments.

B. OBJECTIVES

These voluntary guidelines are provided to ensure consistency related to the execution and reporting of an SCA Engagement.

The use of the SCA procedures that are determined to be in scope for that engagement will be performed by an assessor/assessment team to validate the presence of expected controls in order to mitigate the risk associated with the products and services provided.

Note: The SCA procedures are reviewed annually and updated as needed by Shared Assessments

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 AFFILIATE	THE ASSESSEE	THE SUBCONTRACTOR
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 is any entity under the Outsourcer's direct control. Affiliates are Assessees when being evaluated by a parent organization.	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 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 Tools:
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 Shared Assessments Tools to assess its own internal processes.

Note: Arrows the diagram above depict workflow direction.

II. GLOSSARY OF DEFINED TERMS

Affiliate – An entity under the outsourcer's effective control.

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

Assessor, Assessor Team – 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 will perform the SCA procedures. An Assessor Team would be 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. Subject matter expert(s) who will perform the SCA procedures are typically those 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.

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: (1) leverage common services from an assessee; (2) and agree that the SCA scope meets the outsourcers' specific control requirements. Remediation activities are unique to each individual outsourcer and should be performed separately and not be shared among outsourcers. Such a standardized risk assessment approach improves the efficiency of 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 or internal);
- Utilizing a standardized set of control procedures for determining an assessee's risk posture in a way that accommodates individual outsourcers' risk tolerances; and
- Reducing time and expense of conducting multiple assessee control validation assessments.

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

Documentation Attributes – Identification of key documentation attributes reviewed in the engagement.

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 is conducting a self-assessment, the outsourcer also assumes the role of the assessee. The company which contractually engages an assessee to utilize their products and/or perform specific services 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.

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

Risk Control Domains	
A. Enterprise Risk Management	J. Cypersecurity Incident Management
B. Security Policy	K. Operational Resources
C. Organizational Security	L Compliance and Operational Risks
D. Asset and Information Management	M. Endpoint Device Security
E. Human Resource Security	N. Network Security
F. Physical and Environmental Security	P. Privacy
G. IT Operations Managment	T. Threat Management
H. Access Controls	U. Server Security
I. Application Security	V. Cloud Hosting Services

Scoping - Identifies the areas within the assessee's environment that will be included within scope of the assessment.

Subcontractor – An entity independent of and directly performing tasks for the assessee. The subcontractor (fourth/Nth party) is ultimately doing work on behalf of the outsourcer.

Testing/Sampling Procedures – Specific procedures that will be executed to:

- Capture and validate the presence and operational nature of the controls.
- Leverage standardized sampling parameters and methodologies for performing specific tests.

III. VOLUNTARY GUIDELINES FOR AN SCA ENGAGEMENT

A. PARTICIPANT RESPONSIBILITIES

1. **Participants planning and conducting an SCA engagement include:** outsourcer, assessee, and assessor. For terms and relationship details, see SA SIG and SCA Outsourcing Relationships and Definitions and Glossary of Terms.

2. **Who can use the SCA:**
   a. Members of Shared Assessments. Members may include outsourcers, assessees, assessors, and content licensees. The licensees are software and platform providers that utilize, in part, Shared Assessment's Tools content to keep their third party risk assessment offerings content up to the most current set of industry standard best practices.

   b. Outsourcers or assessees who are not members of the program must purchase a Standardized Control Assessment license to use the SCA Procedures.

   c. In order for an assessment firm to conduct an SCA engagement, either the outsourcer or the assessee must hold a license to the SCA. Membership or Tool purchase only entitles assessment firms to use the Tools for self- assessment purposes. Assessment firms will work with Shared Assessments to ensure all license requirements for the SCA Tool are met.

   d. Upon request by a client, the assessment firm will provide a copy of the lead assessors' certificate of successful Certified Third Party Risk Assessor (CTPRA) course completion. See note under III.2.c.

B. ACCEPTABILITY

1. To be deemed acceptable an SCA Engagement Report must, at a minimum, include the following:

   a. Be issued under a valid license to use the SCA Procedures (as noted under III, A above).

   b. Be issued by an assessment firm. Assessment firms that are members of Shared Assessments in good standing; and have agreed to adhere to these guidelines by submitting an acknowledgement form (a copy is available at the end of this document); and have been recognized and issued a Shared Assessments badge that can be found on the Shared Assessments website.

C. ENGAGEMENT PROCESS

1. Participant Preparation:

   a. The Assessee – Confirms internal resource availability in order to provide sufficient support to the assessor by ensuring the necessary documentation and assessment artifacts related to the controls being assessed are available for the engagement.

   b. The Outsourcer – Obtains senior management agreement to the approach to be utilized. Agrees that procedures to be performed will satisfy outsourcer's control requirements and confirms no pre-existing contractual requirements specify a different specific assessment methodology must be used.

   c. The Assessor – Confirms during planning phase that the current version of the SCA will be utilized and the procedures identified as in scope for conducting the SCA Engagement (see III.C.4.a). The Assessor performs the SCA Procedures.

2. Planning and Approach would include a-h below:

   a. All participants should agree on the version of SCA to be utilized:

      i. Identify and confirm the procedures that are in scope when conducting the SCA Engagement; and

      ii. 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. Identify and confirm that resources, budget, timing, etc., are adequate to perform the assessment.

c. Verify with participants that no restrictions exist on leveraging the SCA as the assessment approach to be used.

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.

d. If used, select, confirm, and engage an external assessment firm, 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, documented, and agreed by each of 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 meetings to report progress.

3. SCA Engagement Scoping:

a. The outsourcer and the assessee will define and agree upon the scope of work the SCA procedures will cover, to include:

i. Products/services provided to an outsourcer.

ii. Risk domains and control areas of the SCA to be performed which are pertinent for products/services provided and agreed with outsourcer.

iii. Documented requirements for validating the scoped controls for the procedures performed.

iv. Any sharing conditions/obligations and period of time the assessment covers, which should be specified in the contractual agreement between the assessee and the assessment firm.

v. Expected duration of the assessment.

vi. Agreement to use the SCA Report Template

b. The Assessee(s) and the assessor *will examine and jointly resolve* any considerations around, for example, such items as:

i. Understanding of the environment and documentation available to verify controls.

ii. Any systems associated with the provision of services to an outsourcer.

iii. Any software development associated with the provision of services to an outsourcer.

iv. Any information security, privacy or business resilience requirements associated with the provision of services to an outsourcer.

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

d. Utilize the SCA Control Panel (see the SCA User Procedure Guide) to identify and document any risk domains or procedures determined to be out of scope for the engagement. If any additional procedures are defined by those firms, consider providing the information to Shared Assessments for possible inclusion in future SCA releases.

4. Performing the SCA Engagement:

a. The SCA is performed by providing objective and consistent responses to the scoped procedures to evaluate key cybersecurity and risk management controls in each of the risk domains contained within the SCA Procedure Tools.

5. Report Issuance and Sharing Results:

a. The SCA Report does not express an opinion and covers whether the controls for those procedures performed under the scope of the assessment are implemented or not.

b. The appropriate SCA Report Template is used to document and report on the results of the SCA Engagement.

c. Report issuance and distribution should be conducted in accordance with the Protocols established in the SCA Procedure Tools Documentation.

d. The assessee and outsourcer will share the SCA Report, in accordance:

i. With any conditions/obligations specified in the contractual agreement between the assessee and the assessment firm; and

ii. With their internal procedures for sharing confidential material.

e. The assessee can provide a Management Response report to communicate why any procedures performed resulted in identified controls that were not present.

Note: If the assessee chooses to provide a Management Response document, it must be a separate document from and should not be included as part of the SCA Report.

f. The assessee(s) who engaged the assessment firm to conduct an SCA Engagement to create and distribute a report to multiple outsourcers should consider creating a record which shows which outsourcers have received the SCA Report and captures acknowledgments that:

i. Confirm the SCA Report meets their control requirements and risk appetite; and

ii. Maintain records for report receipt or acknowledgment.

g. Each outsourcer is responsible for definition of any remediation or corrective action plans with the assessee.

Note: Remediation plans must be a separate document from and not included in the SCA Report.

D. QUALITY ASSURANCE

1. The outsourcer or assessee will ensure that the assessment firm they engaged, has:

a. Executed a contractual agreement for the engagement.

b. Attained 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 (a member list can be obtained on the sharedassessments.org website).

2. These Quality Assurance requirements may not be applicable 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.
3. The assessor/assessment team to perform the SCA scope of work, will:

a. Ensure required certifications are present, which are:

i. The lead assessor for an SCA Engagement conducted by an independent assessment firm must hold a current Shared Assessments Certified Third Party Risk Assessor (CTPRA) Certification.

ii. Assessors who perform a control validation are encouraged to obtain the CTPRA Associate certification.

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.

iii. Assessors performing a Shared Assessments SIG or SCA are encouraged to complete the corresponding SIG and or SCA training courses.

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. Agree with the assessee and document:

i. Supporting documentation. requirements needed to validate the controls for the procedures performed.

ii. Sharing conditions/obligations, which should be specified in the contractual agreement between the assessee and the assessment firm.

iii. Restrictions, limitations or requirements for sharing the SCA Report.

E. LIMITATIONS

1. **The following items either limit performing an SCA or the distribution** of the resultant report:

2. **All parties must:**

a. Acknowledge that the SCA Report does not provide an opinion (attestation) and is designed solely to objectively 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, agreed upon, and documented prior to commencing work.

3. **The assessee would be able to leverage the resultant SCA Report if the assessee:**

I. Agrees on the independent assessment firm (assessor) to be used;

II. Confirms the economic model that will be used to pay for the independent assessment firm;

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

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

V. Agrees to the assessee location(s) to be included in the assessment; and

VI. Agrees to the period of time being covered for the assessment.

IV. ADMINISTRATION

A. CONTACT INFORMATION

Phone: (505) 466-6434

Fax: (505) 466-3111

Email: info@sharedassessments.org

B. RELEASE HISTORY

Version 1.0 – April 30, 2018

Version 2.0 – May 15, 2019

Version 3.0 – November 19, 2019

Version 4.0 – September 29, 2020

Version 5.0 - December 17, 2020

Version 6.0 – March 1st, 2021

Version 6.1 – September 29th, 2021

Revision	Date	Section(s) Affected	Rationale	Approved
6.1	092921	I. Updates to branding, legal entity, and copyright within guidelines and acknowledgement forms. II. Updates to terminology related and risk control domains due to Tool Release updates.	Branding Standards update	RS
6	030121	I. Change from required standards to voluntary guidelines II. Addition of 2021 acknowledgement form for those assessment firms agreeing to adhere to the guidelines. III. Addition of the fillable pdf form for acknowledgement.	Change from Standards to Voluntary Guidelines	RS

V. APPENDIX: ACKNOWLEDGMENT FORM

GUIDELINES FOR PERFORMING A SHARED ASSESSMENTS STANDARDIZED CONTROL ASSESSMENT MEMBER ACKNOWLEDGEMEMENT FORM

The undersigned assessment firm ("**Firm"**) member of Shared Assessments acknowledges that it has received and reviewed a copy of the Shared Assessments Voluntary Guidelines for Performing a 2021 or 2022 Shared Assessments Standardized Control Assessment (SCA) ("**Guidelines**") of The Santa Fe Strategy Center LLC, dba Shared Assessments ("**Program**") and agrees to use its best efforts to follow the Guidelines and all processes and procedures referenced therein. The Firm understands that the Program has the discretion to change, modify, or delete the Guidelines at any time. The Program will maintain a copy of the current Guidelines on its website and shall notify Firm within sixty (60) days if any changes are made to the Guidelines. The Firm also understands that any delay or failure by the Program to enforce any rule, regulation, or procedure contained in the SCA Voluntary Guidelines will not constitute a waiver of the Program's right to do so in the future.

By signing this acknowledgment, so long as the Firm is in good standing as a member of Shared Assessments, it will receive a badge identifying their organization as agreeing to adhere to the SCA Voluntary Guidelines. You must be a Shared Assessments member in good standing to continue to display a badge.

Shared Assessments will identify all Firms willing to comply with the Voluntary Guidelines on the Shared Assessments website and provide a Shared Assessments Badge which Firm can use to display on their website or in other marketing related information showing they have agreed to comply with the Guidelines.

Dated this ___ day of _____, 20__

_____
(Firm Name)

By: _____
(Signature) Lead Assessor or above

Name: _____

Title: _____

Email: _____