



## **Shared Assessments: Getting Started**

### ***A Step-by-Step Guide to Integrating Shared Assessments into Your Vendor Management Program***

Integrating the Shared Assessments Program into an existing vendor management program can be challenging. This guide was developed by leading financial institutions to help companies effectively integrate Shared Assessments into established programs. Here, we cover the executive and operational tasks involved, which should be executed by appropriate individuals according to organizational roles.

*Socializing the program with all internal stakeholders is critical to successful adoption.* Depending on the organization, stakeholders may include Vendor Management, Contract Management, Information Security, Disaster Recovery/BCP, Physical Security and other areas.

Once acceptance begins to take hold, your company will start to see the benefits of greater internal efficiencies and standardized industry engagement. Industrywide, as financial institutions leverage the Shared Assessments standards and encourage their service providers to do the same, we will all be able to devote more resources to services and fewer to redundant security assessments.

For more information about Shared Assessments, please contact Michele Edson, [michele@santa-fe-group.com](mailto:michele@santa-fe-group.com), or visit the Shared Assessments website at [www.sharedassessments.org](http://www.sharedassessments.org).

### **Phase I: Lay the Foundation**

- 1. Identify an executive sponsor inside your organization.** This might be a CIO or another high-level executive who has influence in your organization. Convince the executive sponsor that participating in the Shared Assessments Program is the right thing to do because:
  - Participation provides value to your organization. Within a few months of using the Agreed Upon Procedures (AUP) and the Standardized Information Gathering Questionnaire (SIG), your organization will see increased efficiencies and resource savings.
  - Participation keeps your organization on par with industry leaders. By using the Shared Assessments standards, your organization demonstrates it is relying on industry-accepted standards and best practices. Your organization will have the opportunity to interact with industry leaders and learn from their vendor risk practices.
- 2. Join the Shared Assessments Program Working Group.** The Working Group allows you to learn how your peers at other institutions and service providers are using the Shared Assessments Program. Regular, interactive meetings can be a significant asset in building your organization's vendor risk management knowledge. If you don't have a vendor management program in place (it's an FFIEC requirement), membership offers an outstanding foundation from which to launch a new program.

3. **Be an advocate.** Talk about Shared Assessments at every opportunity. Develop an internal marketing strategy that takes anticipated challenges into consideration, including internal politics and concerns specific to your organization. Believe in what you're doing and let people see your enthusiasm.
  - Identify all vendor management constituencies. Who do you need to recruit to make the process successful? Be sure to include internal auditors.
  - Discuss Shared Assessments with all constituencies. Talk about how this is an opportunity for the entire organization to streamline its processes and get in line with industry best practices.
  - If you're a vendor, conduct a self-assessment. Share it with clients and potential clients, and use it as a marketing tool.

## Phase II: Introduction of Shared Assessments

4. **Identify the group(s) in your organization responsible for conducting service provider assessments.** Assessments may fall under information security, contract management, vendor management or another area.
5. **Meet with these groups to understand the current vendor assessment process and introduce Shared Assessments.** Understand that some vendor managers may see Shared Assessments as a threat to their existing program. Clearly explain that Shared Assessments can enhance a proprietary process by introducing industry-standard practices and repeatable results. If necessary, engage your executive sponsor to spur buy-in. Focus on the tools and documents used in the current process, including process documentation and any proprietary questionnaires. Explain that the Shared Assessments SIG uses closed-ended questions and that the AUP conducts actual tests on service provider infrastructure and controls.
6. **Prepare your organization to accept Shared Assessments.** Gather all of the necessary approvals from all levels of management to use Shared Assessments. Continue your internal marketing and engage your executive sponsor, as this time is critical for buy-in from all constituencies.
  - Use existing Shared Assessments promotional materials and/or develop your own materials. Conduct training sessions with all affected parties. This may include assessors, vendor relationship managers, and/or information security officers within your organization.
  - Ensure all groups that have relationships with service providers in your organization understand Shared Assessments and are prepared to use the program.
7. Create a production schedule. A clearly delineated cycle established with input from all stakeholders is critical to sustaining internal adoption. A sample schedule might look like this:
  - Q1: Service providers receive the updated SIG and AUP and complete the SIG. Assessment firms perform AUP assessments with appropriate service providers and issue reports.
  - Q2: The financial institution incorporates the SIG and AUP results into its vendor management program.
  - Q3: Collect feedback from all internal users, including current events and risk and security threats. Prioritize and select appropriate SIG and AUP changes and enhance tools for the upcoming year.
  - Q4: SIT/ UAT and SIG and AUP approval are completed. The financial institution provides updates to service providers by the end of Q4.
8. **Encourage your existing service providers to participate in the Shared Assessments Program.** Some ways to do this include:
  - Mentioning Shared Assessments when conducting assessments.
  - Educating internal relationship managers so that they encourage their service providers to participate in Shared Assessments. Be sure relationship managers understand the program's benefits for service providers and are able to articulate those benefits.

- Providing program materials to relationship managers that they can distribute to service providers.

### Phase III: Operational Analysis

- 9. Create and maintain an inventory of your service providers.** Include the following minimum information for each:
  - Name
  - Address (location of site target data storage/processing)
  - Point of contact information (name, physical address, phone, e-mail, etc.)
  - Whether the data are classified, and if so, information classification level
  - Contract execution and renewal date (if assessments are conducted annually)
  - Last assessment date
  - Next assessment date
  - Issues identified in last assessment
  - Assessment issue remediation status (open, closed, or in progress)
- 10. Compare the Shared Assessments tools with your internal policies.** Conduct a detailed analysis (and document any gaps) that includes:
  - A gap analysis comparing the Shared Assessments tools (SIG and AUP) to your internal policy documents. In general, the internal policies should include your company's information security policy, physical security policy, DR/BCP/COB policies, and any other policies required by your service provider assessment program. (Consider using the *Shared Assessments Industry Positioning and Mapping Document*, which maps Shared Assessments standards to ISO, COBIT and PCI. Download the document at [bitsinfo.org/fisap](http://bitsinfo.org/fisap).)
  - A gap analysis of Shared Assessments tools (SIG and AUP) to your internal questionnaire.

### Phase IV: Deployment

- 11. Incorporate the Shared Assessments tools into your vendor assessment process.** Keep in mind that some service providers will provide an AUP final report, while others will complete the SIG.
  - Determine how the completed SIG and AUP final report will be analyzed. The SIG is a collection of closed-ended questions that covers many controls, so analyzing the SIG manually can be time consuming. A Binary Analysis Tool (BAT), which is provided as part of the SIG download from the Shared Assessments website, can help. A BAT analysis of the SIG will take only a few seconds. The analysis can then be entered into a Bridge Document (detailed below).
  - Use the gap analyses you created in step 9 to create a Bridge Document. This document should contain any questions from your proprietary questionnaire and/or any policy controls not addressed by the SIG and the AUP final report.
- 12. Execute your first assessment.** Allowing regulators to see the assessment creates an opportunity for them to comment to your management that they do accept Shared Assessments. Ensure that before the first assessment begins, your service providers clearly understand the program's advantages for *them*.
  - Provide the service provider with a SIG, allowing enough time for it to be completed.
  - Once the completed SIG is received, analyze the data. Document any areas of concern (in which the controls provided by the service provider are not aligned with your requirements) in the Bridge Document.
  - Review any areas of concern from the SIG analysis with the service provider. Use the Bridge Document to go over any gaps identified during the internal policy gap analysis. Determine whether the service provider has any compensating controls in place.

- Document all issues for which the service provider has either addressed the control or does not have any compensating controls in place.
- Discuss these issues with the service provider. Ask the service provider to commit to resolving the issues, including a timeline for remediation.
- Track all open issues until they are resolved.

**13. Maintain issue reporting and metrics for each service provider.**

- Reporting should include areas of concern, identified issues, and other issues that arise. Provide these reports to all parties involved with the service provider. Include documentation of the risk associated with each issue.
- Metrics should include the number of service providers with access to classified information, the number assessed, and the number in line to be assessed. Individual assessment metrics should include the number of issues identified, the risk associated with each issue, the status of each issue (remediated, remediation in-progress, risk accepted), and the target remediation date for each.

*Shared Assessments: Getting Started* was published by Shared Assessments Program members to guide financial institutions and service providers in successfully incorporating Shared Assessments into their programs. If you are using Shared Assessments, we'd like to hear about your experiences, including your challenges, successes, and ideas for improving the program. Provide your feedback at the Shared Assessments Program website, [www.sharedassessments.org](http://www.sharedassessments.org) (after login, click on the "General Feedback" link on the right-hand side of the page), or write to Michele Edson at [michele@santa-fe-group.com](mailto:michele@santa-fe-group.com).

For more information about the Shared Assessments Program, including free downloads of the assessment documents (AUP and SIG), visit [www.sharedassessments.org](http://www.sharedassessments.org) or contact Michele Edson, [michele@santa-fe-group.com](mailto:michele@santa-fe-group.com) or 831-637-1879.