Shared Assessments Program Case Study

A Collaborative Approach to Onsite Assessments Using the Shared Assessments AUP, the Standardized Testing Procedures for Onsite Assessments

April 2015

SHARED
ASSESSMENTS

Background

About the Shared Assessments Program

The Shared Assessments Program develops and provides resources to effectively manage the critical elements of the service provider lifecycle. Shared Assessments members represent industry outsourcers, vendors, and assessments firms that work together in a global, peer-to-peer community of information security, privacy, and third party risk management leaders. Members collaborate in sharing best practices and development of tools such as Shared Assessments AUP (Agreed Upon Procedures), an objective standardized set of testing procedures used to evaluate service provider controls related to IT data, security, privacy, and resiliency risk. Industry leaders work together to ensure Shared Assessments Program Tools are up-to-date and meet regulations and voluntary guidelines and standards for industries that include financial services, insurance, brokerage, healthcare, retail, and telecommunications.

Overview

Outsourcing organizations share a number of common key industry third party services, as well as risk profile concerns. While the AUP has helped streamline evaluation, many outsourcing organizations still utilize their own proprietary questionnaires and onsite audit criteria based on their individual need for assessment that accurately reflects their unique interpretation of regulations, divisional needs, and risk appetites. The demand for a tailored assessment frequently requires intensive, multiple, and overlapping information requests from clients to their service providers that result in grossly inefficient resource use for both outsourcing organizations and their third party service providers. These multiple assessments are also ineffectual in providing a tangible gain in risk management or improving the risk posture at the service provider level.

Together, these factors of commonality and inefficiency presented the opportunity for development of an augmented "Superset AUP" that would enable industry to build stronger third party risk management capability without diminishing the ability to manage the service provider relationship. As outsourcing organizations are largely assessing third party risk in very similar ways that evaluate the same types of controls, standardization of the process for use industry-wide is a logical progression in the advancement of assessment tools.

The Shared Assessment Collaborative AUP Project sought to augment the existing AUP for additional controls and test procedures required by top-tier financial institutions. Such a standardized risk assessment tool was expected to improve assessment-related economies and scalability for clients and their service providers alike by:

- Producing a robust, repeatable, consistent methodology that can be leveraged by any independent assessment firm or in-house auditor.
- Utilizing a standardized set of test procedures for determining a service provider's risk posture that accommodates individual organizational risk tolerances.
- Reducing time and expense of conducting multiple onsite service provider assessments.

In the initial pilot, the AUP was augmented to include the collective intelligence of three key multi-national financial services industry institutions - JPMorgan Chase & Company, Citigroup, and Morgan Stanley - using enhancements identified through mapping the AUP against their internal proprietary third party risk assessment questionnaires.[1] These three institutions joined together to perform a collaborative onsite assessment of a key industry service provider, Iron Mountain, a storage and information management company that serves more than 165,000 organizations in 36 countries.

Leveraging the prevailing industry standard augmented AUP as the common risk assessment framework, the banks and Iron Mountain collectively selected an independent assessment firm to perform a true, onsite collaborative assessment of Iron Mountain. The assessor reported the objective findings of the assessment to the service provider who then shared the report with the sponsoring financial industry institutions, each of which then evaluated the report from their individual risk tolerance viewpoint and worked individually with the service provider to determine remediation needs, if necessary.

[1] The initial pilot study conducted during 2013-2014 and reported in this paper is the first of three pilots. The second pilot was conducted and completed in 2014 with the third underway in early 2015.

Methodology

Project Approach

The Collaborative Onsite Assessments Program was created under the auspices of the Shared Assessments Steering Committee. Through 2013-2014, the Shared Assessment AUP Project developed and tested an augmented Shared Assessments Program Tool specifically geared to a collaborative assessment that profiles the full and complete control environment appropriate to the financial services industry using a substantiation-based, standardized, efficient methodology to evaluate:

- Viability of standardizing and using an augmented AUP as a common collaborative assessment vehicle for testing service provider information and data security, privacy, and business resiliency risk controls.
- Risk within the environments of both the outsourcing organization and service provider.
- Associated risk for common services offered to multiple financial services industry organizations.

The project leveraged the Shared Assessments AUP 2014, the Shared Assessments Program standardized testing procedures used for onsite assessments, as the common risk assessment methodology. This tool was augmented by incremental test procedures to ensure collective coverage of control requirements from all project participants. The resulting Superset AUP is valid, scalable, consistent, and repeatable regardless of the type of services provided by a specific service provider.

The Superset AUP provides assessment for the following objective and consistent key risk management control domains:

- IT and Infrastructure Risk Assessment Lifecycle
- Information Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance
- Fourth Party Controls Management
- Management of Privacy Programs
- Network Security, Operations, and Management

Study Methodology and Implementation

The Steering Committee, which is responsible for ensuring the overall success of the Shared Assessments Program, provided project oversight. Participating in the project were both members and non-members of the Shared Assessments Program. The study timeline was estimated at 90 to 120 days, which is not reflective of future pilots or future assessments. Study workflow of participant roles and order of progression for study tasks was as follows:

Step 1: Determine Participants. For this initial pilot, the Steering Committee guided the selection of the Participants, which included three top-tier financial institution Industry Sponsors, which in turn, identified one common industry Service Provider. The focus initially for the Service Provider was on services provided within the United States for which the Service Provider was common to the Industry Sponsors. The Service Provider was selected based on meeting project tactical objectives for: (1) being broadly used within the financial services industry to allow for leveraging of the resulting tool within the sector; and (2) the collective ability of multiple financial institutions to leverage a single shared "collaborative" assessment to evaluate the Service Provider's risk posture.

Step 2: Scoping. Scoping was performed to identify common services and locations. A total of five Service Provider locations for three distinct services were considered for assessment. Industry Sponsor representatives from the three banks and one Service Provider, following buy-in within their own organization's senior management, agreed to services and locations for assessment.

Step 3: Selection of Auditor. Shared Assessments and all four Participants agreed that Auditors could be selected from CPA or Non-CPA independent assessment firms. The Service Provider selected a Big 4 Auditor based upon the relationship held with the Service Provider. All Participants agreed upon an Auditor to conduct the assessment.

Step 4: Superset Modifications. Each of the Industry Sponsors worked collaboratively to develop a single augmented Superset AUP by mapping their internal risk assessment requirements against the AUP 2014. The AUP was found to include approximately 80% of the financial services organizational requirements. The additional mapped items included some non-IT, security, privacy, and resiliency components. The Industry Sponsors shared the resultant Superset AUP with the Service Provider and Auditor. The Auditor compiled the mapping from each institution and created a gap analysis. All components identified by both the Industry Sponsors and the Auditor were then added to meet outsourcing organizational needs. The Auditor then added test procedures for any additional controls necessary for the assessment.

Step 5: Assessment Prep. The Auditor and Service Provider narrowed the newly augmented Superset AUP to the specific services being assessed. Participants approved the pared version to ensure it met their need for completeness, sufficiency, and accuracy.

Step 6: Assessment Performed. Participants then scheduled and conducted the onsite assessment using this narrowed Superset AUP. Actual assessment took between 30-45 days, which is a timeline not considered to be representative of the process for future assessments.

Step 7: Post Assessment. Post assessment involved the presentation of Auditor findings to the Service Provider. In turn, the Service Provider presented comments and observations to the Auditor. The Auditor then compiled and released the final assessment report, which was distributed by the Service Provider to all Industry Sponsors. Each Industry Sponsor met separately with the Service Provider to review any issues and findings, responding to the Sponsor's own risk tolerance and needs and defining any remediation, resolution, and monitoring that might have been required to meet the risk parameters of each outsourcing institution.

Findings

Using an industry-accepted substantiation-based methodology of validating service provider controls, such as the AUP, allowed for a consistent, robust and objective set of controls, which allow for a high level of consistency and neutrality. Lessons learned that were incorporated into the process and the Program Tool were:

- The collaborative Superset AUP provides more extensive risk domain coverage than individual proprietary assessment sets.
- The Superset AUP is not an attestation and does not allow for any opinion or subjectivity, therefore allowing for objective review of the findings based on unique environments and risk appetites.
- The risk assessment auditor is selected by the service provider, ensuring the assessment is independent of the outsourcing institution.
- The participating organizations gain alignment of scope, control requirements, and testing procedures through shared assessment.
- The Superset AUP can be tailored to the services provided by the third party in advance of the onsite assessment.
- Control testing can be conducted by any independent assessor or internal auditor ensuring affordability for organizations of all sizes within a reasonable timeframe.
- One assessment can be leveraged by multiple outsourcing organizations.
- The assessment allows industry and service provider participants to allocate resources to risk management and mitigation activities, instead of participating in multiple redundant assessments.
- Individual service providers gain immediately through reduction in cost of duplicative assessments and reduced assessment fatigue, and robust and consistent findings of an AUP can be shared across multiple clients in multiple industries.
- While assessment can be performed by any independent assessment firm, when performed by a CPA firm, a universal acknowledgement letter that meets AICPA assessor standards would facilitate report delivery and allow for assessment sharing.

The detailed institutional input using clean, consistent methodology for mapping created a more potent service provider collaborative assessment tool that can provide ongoing long term cost savings and FTE efficiencies that will benefit both service providers and financial institutions. In part, these savings will be expressed as both sets of organizations redirect resources away from assessment costs and toward control and monitoring by limiting site visit and annual review man hours. An unanticipated outcome from a service provider viewpoint proved to be the creation of closer client relationships. Enthusiasm for the benefits of the collaborative assessment has been expressed at the highest levels among participants.

Conclusion and Next Steps

Benefits Summary

Benefits of using the collaboratively developed Superset AUP for a larger set of common service providers include:

- Speed, increased rigor, consistency, efficiency, and cost savings in the control assessment process for both the outsourcing organization and the service provider.
- Larger Tier 1 and 2 service providers would benefit most immediately from participating in collaborative assessments.
- For mid and small size institutions who cannot necessarily dedicate a high level of resources to meet the changing regulatory and evolving risk environment, there exist tangible cost savings and personnel efficiencies benefits through use of a consistent, reliable tool.
- More robust control sets developed through collective intelligence are expected to drive improvements in service provider programs internally through the strength of authority gained through having industry leaders guide the development of this Shared Assessments Program Tool.

The Superset AUP developed during this pilot represents an enhanced industry standard which covers both operational and reputational risk factors. It incorporates industry intelligence from multiple institutions that informs the assessment at the most robust level. Iron Mountain's generous assumption of the cost to complete both the Superset AUP mapping and the assessment audit has allowed us to develop a model mature and vigorous enough for broad distribution in its current form by mid-2015.

Currently seven of the top 10 banks have mapped their requirements to the Superset AUP and signed off that it meets their expectations. The Program Tool has expanded on the standard AUP while increasing inquiry into operational aspects of the service provider, which are most salient industry-wide for all financial services providers. For the service provider, this can broaden their customer base. For the outsourcing institution, such vigorous diligence will improve their reputation among customers as well through the use of standardized and tighter controls that meet industry needs. Gaining acceptance for the Shared Assessments Program Tool through use will confirm that the Superset AUP carries the highest standards for IT data, security, privacy, and resiliency risk, making it a definitive element of operations models.

Next Steps

Shared Assessments is continuing to work to develop a more broadly used Collaborative Onsite Assessment Program through:

- Ongoing development and refinement of the Superset AUP to ensure additional robustness by expanding the collective intelligence to include additional financial institutions.
- Develop additional strength, such as leveraging the enhanced tool for procurement purposes.
- Develop and broaden the collaborative onsite assessment program including project management services.
- Release the enhanced Superset AUP Program Tool in mid-2015.
- Promote adoption of the Program's Superset AUP as a best practice standard for each industry or sector as they are developed.

SHARED ASSESSMENTS

Conclusion

The Shared Assessments Superset AUP has identified risk profile gaps that ensure a higher level for testing service provider information and data security, privacy, and business resiliency risk controls. The Superset AUP is standardized to leverage responses recursively and collaboratively, which will improve the economies and scalability of service provider risk assessment for all parties. This level of targeted assessment is expected to yield a higher confidence for financial services organizations that their third party service provider is compliant and is more likely to remain compliant.

Thank You

We'd like to thank all those who have helped pioneer the Shared Assessments Collaborative Onsite Assessments Project especially: The Shared Assessments Steering Committee; Senior Third Party Risk staff at JPMorgan Chase & Company, Citigroup, and Morgan Stanley; Seth Bailey, Director, Information Security of Iron Mountain; The Staff of the Shared Assessments Program - Angela Dogan, Senior Project Manager of The Santa Fe Group; and Robin Slade, Executive Vice President and Chief Operating Officer of The Santa Fe Group.

Learn More

For more information on the Shared Assessments Program and the Collaborative Assessments Project, please contact Vicki Dean, Vice President of Member Relations and Sales, The Santa Fe Group, at vicki@santa-fe-group.com or visit sharedassessments.org.