SHARED ASSESSMENTS

AGREED UPON PROCEDURES (AUP): A TOOL FOR ONSITE ASSESSMENTS

THE AUP

The AUP is used by companies to evaluate the controls their vendors have in place for IT security, data protection, privacy, business continuity and other risk areas. The AUP consists of an objective test of controls, validation of vendor self-assessment(s), and standardized reporting requirements. This allows companies to view assessment results in the context of their vendor risk management requirements.

The AUP provides objective and consistent procedures which validate key controls in the following domains of risk management:

- 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

The AUP procedures were developed under the American Institute of Certified Public Accountants (AICPA) professional standards, adhering to Attestation Standard (AT) Section 201, which sets forth attestation standards and provides guidance to practitioners on performance and reporting in AUP engagements.

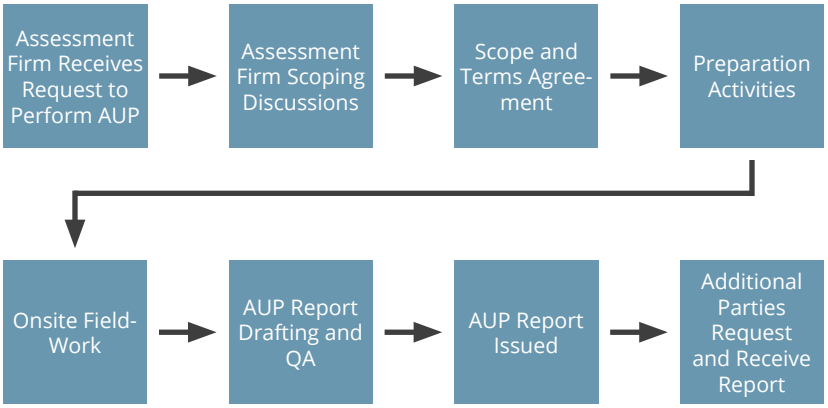
Objective results of the AUP are provided directly to the service provider by the auditor or assessment firm. The service provider may then share the report with a virtually unlimited number of clients, who evaluate the report in the context of their engagement(s) with the service provider and industry risk management and regulatory requirements.

AUP reports typically consist of population, sample size and number of failures within the sample. No subjective opinions are formed, allowing the outsourcing organization to form its own opinions of the results in the context of its own risk appetite. Depending on the recipient, AUP reports may be used in place of a costly onsite assessment, reducing assessment costs for both the service provider and the outsourcer. Anecdotal evidence indicates that medium-sized organizations can expect an onsite AUP assessment to be completed in approximately five days.

SHARED ASSESSMENTS

AGREED UPON PROCEDURES ENGAGEMENT

Typical AUP engagements proceed as diagrammed below.



Scoping the Assessment

The scope of an AUP engagement must be determined before any procedures are executed. The scope must take into account the type of service provider, its business, the type of target data, protected target data, privacy target data and protected privacy target data it collects, stores, uses, shares, transports, retains, secures and/or deletes. Given this information, the target systems or processes are defined along with their supporting hardware, software and procedures to be tested. The applicability of each procedure should be determined during scoping discussions, assisting the practitioner in:

- Understanding the service provider's environment
- Identifying the documentation the service provider will need to submit
- Determining the order in which the procedures will be executed

The procedures in this document have been developed by the Shared Assessments AUP Development Committee. Testing these procedures provides the validation clients typically expect, potentially saving time and effort for both the client and the service provider when clients are willing to accept the AUP report in lieu of their own onsite examination.

When all applicable procedures are completed, the audit or assessment firm provides the service provider with a report of its findings. This report does not express an opinion and covers only those procedures performed under the scope of the agreement.

After reviewing the report and providing it to clients, service providers are strongly encouraged to communicate with clients about the content of their report. Specifically, the service provider should:

- Identify any mitigating and compensating controls that were not tested during the AUP assessment. (This information may need to be tailored according to the services subscribed to by the client or in accordance with relevant contracts.)
- Describe any remediation plans, including how and when issues will be addressed and plans for testing to demonstrate the required changes have been implemented. (Service providers should understand that most clients will require remediation plans.)

SHARED ASSESSMENTS

AGREED UPON PROCEDURES FORMAT

Each AUP control area contains:

- **Objective(s):** Statement(s) describing the business interest behind assessing the domain
- **Control(s):** Statement(s) about the controls service providers should have in place
- **Procedure(s):** The action or actions a practitioner will perform to test each control area

Example Control Area

A. Risk Management

Domain Objective:
Organizations should create and maintain a continuous process for IT and infrastructure risk management to identify, quantify, and prioritize risks against defined risk acceptance levels and objectives relevant to the organization.

A.1 IT and Infrastructure Risk Governance

Objective:
An organization's risk management program should include a formal program, which documents the organization's assets and threats and evaluates associated risks.

Control:
A formal risk governance program is implemented.

Procedure:

A. Obtain from the service provider the document(s) that are part of the risk assessment program.

B. Inspect the document(s) for evidence of the following attributes:
   1. Risk governance plan
   2. Risk policy and procedures
   3. Range of business assets to be evaluated
   4. Range of threats
   5. Risk scoping
   6. Risk context
   7. Risk training plan
   8. Risk scenarios
   9. Risk evaluation criteria

C. Report the attributes listed in Step B not found in the risk program, the date of the last update, the business and technical owner of the risk program, or if the risk program documentation does not exist.

AUP REPORT TEMPLATE

The AUP Report Template was developed by the Shared Assessments Program to provide a standard methodology for reporting the results of the onsite assessment. The AUP Report Template allows the company being assessed to include any additional mitigating controls (and accompanying documentation) believed relevant to delivering a sound control environment.

It also allows the company to state and establish their full and complete control environment in one easy to use document. The company conducting the assessment can then easily identify any areas/controls they would like to have tested further.

LEARN MORE

To learn more or to purchase the Shared Assessments Program Tools, or to obtain information about membership opportunities, contact Julie Lebo, Vice President Member Relations, The Santa Fe Group, at **(703) 533-7256** or **julie@santa-fe-group.com.**