

Detroit Public Schools

Office of the Auditor General



SAS 70 VENDOR REVIEW

For the Year-Ending June 30, 2011

REPORT NO: 2011-012

REPORT DATE: October 17, 2011

BACKGROUND

Many companies and governmental entities outsource business tasks or functions to other businesses to save costs and gain efficiencies. The entity performing the outsourced service is called a service organization or third party service provider and the entity using that service is called a user entity. Detroit Public Schools (DPS) has business relationships with entities that perform tasks or functions on behalf of the District that impacts data reported in the Districts financial statements.

When management utilizes a third party service provider to process transactions or conduct record keeping on its behalf, management remains responsible for evaluating the service provider's internal controls and developing the appropriate user controls to ensure data integrity.

Statement on Auditing Standards Number 70 (SAS 70) addresses the user entity's responsibility for ensuring data integrity in an audit of the financial statements of a user entity that utilizes one or more third party service providers. Auditors for the third party service providers typically provide a SAS 70 report that expresses an opinion on the internal controls over the services being provided to the user for the period in question. When the SAS 70 report does not cover the entire accounting period, a Bridge Letter from the third party service provider must be obtained to account for or bridge the gap of time between the date of the SAS 70 report and the user entity's fiscal year-end.

Detroit Public Schools utilizes the services of a third party service provider - AssetWorks to provide record keeping of Capital Asset inventories and related values that are recorded in DPS's financial statements. In addition, it contracts with Automatic Data Processing, Inc (ADP) for its carrier enrollment services. Both providers process transactional data that impact the District's financial statements.

In the District's 2008 Single Audit Report, DPS received a significant deficiency audit finding in internal controls over financial reporting because the District's internal control procedures did not require an evaluation or independent verification of the service provider's internal control design or effectiveness. In addition, the auditors concluded that there were inadequate policies requiring the review and approval of the work performed by the District's third party service providers. This significant deficiency finding was removed in the District's 2009 Single Audit Report.

The audit finding was removed because the District agreed with the auditor's recommendation that the District should implement procedures for the periodic review and evaluation of third party service providers' internal control which should include obtaining Type II SAS 70 reports.

In addition, the District agreed to establish policy and procedures that would address a process to review the internal controls by their party service providers on a regular basis to ensure they met the control requirements of the District.

OBJECTIVE, SCOPE & METHODOLOGY

The objective of this audit was to (1) Determine that all third party service provider organizations that perform transactional processing of data that impacts the District's Financial Statements provide the District with the appropriate SAS 70 Report and related Bridge Letter, if required; (2) Determine whether the District has developed policy and procedures that include assessing the effectiveness of its third party service providers' internal controls over those processes which impact the District's Financial Statements and whether the District in compliance with its SAS 70 policies. The audit period covered the 2010-2011 School Year.

We requested copies of the SAS 70 Reports and Bridge Letters, Districts SAS 70 Policies and Procedures; and evidence of the Accounting Departments review and assessment of the SAS 70 Report and DPS User Controls over those processes. The OAG met with the Principal Accountant responsible for the SAS 70 review to obtain and understanding of the policies and procedures. Additional inquires regarding SAS 70 requirements were made to the Deputy Chief Financial Officer/Chief Accounting Officer. Our field work ended October 17, 2011.

AUDIT RESULTS

As part of its corrective actions to address the 2008 audit finding, District financial management agreed to develop policies and procedures to evaluate SAS 70 reports from third party providers and to determine which providers are required to submit such reports.

Management's evaluation of SAS 70 reports submitted by third party providers would determine whether testing was conducted on the provider's controls and the results of such testing, whether the application controls included in the report meet the District's requirements and whether methods employed by the third party provider such as the calculation method of depreciation was being performed in accordance with the District's requirement.

Once a determination is made by management on which third party providers are required to submit SAS 70 reports, obtaining such reports for evaluation is the next step in the process.

Management provided SAS 70 reports and bridge letters for AssetWorks and ADP who perform accounting for Capital Assets and Carrier Enrollment Services, respectively. However, the SAS

70 report provided for AssetWorks does not meet auditor's recommendation, as it is a SAS 70 Type 1 report. The bridge letter from this provider does not cover the entire fiscal year for the District.

AssetWorks

AssetWorks provides Capital Asset inventory balances and values that are used in the general ledger. It appears AssetWorks provided a SAS 70 Type I report and not a Type II report as required by the standard. A Type I report does not include the results of testing of the control objectives on the provider's internal controls – it only lists the provider's control objectives. Testing results from a Type II report would indicate whether or not there are in exceptions that could indicate weaknesses in the provider's control environment.

The SAS 70 Type I report provided covered the period January 1, 2010 – December 31, 2010. The Bridge Letter was dated April 7, 2011 and according a portion of the Districts fiscal year (May – June) is exposed. The letter indicates that there were no significant changes in the control environment or planned for the next 12 months. The service auditor's opinion basically stated that; controls objectives as described are suitably designed to provide reasonable assurance that the control objectives would be achieved including satisfactory results of complementary user control testing. Management could not provide any evidence of the review and testing of these complementary user controls.

Automated Data Processing (ADP)

ADP provides carrier enrollment services for the District. This service manages the processing of ongoing enrollment transactions between the District and its health plan carriers. A SAS 70 Type II report was provided to management for the period April 1, 2010 to March 31, 2011. A Bridge Letter covering the period April 1, 2011 to June 30, 2011 was also received. The testing result and opinion expressed by the provider was that; controls as described are suitably designed to provide reasonable assurance that the control objectives would be achieved including satisfactory results of complementary user control testing.

There was one exception noted in the test results of the control objectives listed. Complementary user control objectives were summarized at the bottom of each section of control objective tested. Management could not provide any evidence of reviewing the exception condition or testing of complementary user controls.

Evaluation of Provider Controls

In addition to not obtaining the appropriate SAS 70 report from AssetWorks, we found no documented evidence that management performed an assessment of the adequacy of the report on internal controls. The District should be reviewing the provider's controls to ensure that stated control objectives are being achieved. These control objectives cover activities such

as access controls, computer operations, data output, emergency enrollments, etc. The user has some responsibility for each of these control objectives, but the first task is to ensure that the provider's controls are in place and are being properly executed to address any risk related to the processing of District data.

User Control Considerations

Complimentary user entity controls are controls that management of the service entity assumes will be implemented by user entities which are necessary to achieve the control objectives stated by management. Included in each SAS 70 report is a section for user control considerations. This section suggests actions required by the management (the user) to ensure data integrity. For example, the ADP SAS 70 reports states

- Clients are responsible for sending data files to ADP in the agreed upon format via a secure transmission,
- Clients are responsible for sending ADP data files according to the established transmission schedule, with all of the required information, and with accurate data and for correcting errors detected by the load process before sending the file to ADP.

To meet these requirements, the District is responsible to ensure that controls over these processes exist and are operating effectively. Some organizations develop these controls and list them under the applicable control objective along with the provider's controls. However, these controls can be documented in a policy and procedure manual as well. Although it is likely the District has developed some of these controls, we were unable to verify that the controls exist because we never received a copy of the policy and procedures where such controls would be explained.

Policies and Procedures

In accordance with the corrective actions developed by management in response to this audit finding in 2008, management said it would develop policy and procedures that included requirements to evaluate the provider's controls and to discuss any required procedures for the District as part of its user controls over data being sent to and received from third party providers. On several occasions we requested copies of the policy and procedures financial management developed for SAS 70 activities, but as of the date of this report, management was unable to provide the manual. The employee responsible for this area told us that she had never seen the manual and she typically just provides our auditors with a copy of the SAS reports when requested.

CONCLUSIONS

The District obtained SAS 70 reports from its third party service providers indicating that the internal controls over the provider's activities were in place which provides some assurance that the data sent back to the District was processed in a controlled environment. For one of the third party providers the effectiveness of these controls was tested with one exception noted indicating that the controls were operating effectively. However, the other third party provider's SAS 70 report did not include testing, but rather an opinion from the provider indicating that the controls were effective without the added assurance of testing.

We found no evidence of management's evaluation of these controls. In addition, without policy and procedures that document the District's controls over data sent and received from third party providers we were unable to verify that such controls exist.

Ultimately, the District is responsible for ensuring the data integrity of information sent to and received from third party providers. Given that the dollar value of the transactions are significant, the risk exist that errors in the data can have a material impact on the District's financial statements and lead to an audit finding in future audits of the District's financial statements.

Financial management should be receiving the appropriate SAS 70 reports, documenting its evaluation of these reports and establishing internal controls to augment the provider's controls over District data to ensure the integrity.

RECOMMENDATIONS

To ensure the District is aware of all providers which are subject to SAS 70 reports, we recommend that the Chief Financial Officer direct his staff to:

- Perform an assessment of all third party service providers' to determine if services provided require SAS 70 treatment,

To ensure the data integrity over information sent and received from third party providers, we recommend the Chief Financial Officer;

- Request a SAS 70 Type II report from AssetWorks. AssetWorks provided a SAS 70 Type 1 Report where the service auditors list the control objective without any indication of the test results or exceptions. Type II SAS Reports Report includes detailed testing for each control objective and the disposition of exceptions noted during testing, which provides greater assurance that identified risks are mitigated.

- Document the department's review and assessment of testing exceptions that service auditors note in SAS 70 Type II reports. In addition, complementary user controls must be reviewed and evaluated in light of the SAS 70 report, as they are included within the total control environment of the process and procedures performed by third party service providers.
- Request a Bridge Letter from AssetWorks to cover the entire period of exposure through the District's fiscal year-end, June 30, 2011.
- Develop policies and procedures for evaluating SAS 70 reports and distribute the policy manual to the appropriate financial staff and the internal and external auditors,

MANAGEMENT RESPONSE

Management Response provided by the Chief Financial Officer:

1. The Finance Department will perform an assessment of all of its third party service providers to determine if services provided require SAS 70 treatment.
2. Develop policies and procedures for evaluating SAS 70 reports and distribute the policy manual to the appropriate staff and the internal and external auditors. The policies and procedures manual will include among other topics, overview of SAS 70, report requirements, assessment of third party service providers, review and assessment of testing exceptions, complementary user controls, etc.

Our review was performed in accordance with U.S. General Accounting Office Government Auditing Standard and Standards of the Institute of Internal Auditors.

This report is intended solely for management and should not be used for any other purpose. This restriction is not intended to limit the distribution of the report which is a matter of public record.

Odell W. Bailey, CIA

A handwritten signature in blue ink, appearing to read 'Odell W. Bailey', is positioned above the title 'Auditor General'.

Auditor General