Fort Worth
INDEPENDENT SCHOOL DISTRICT

IT Risk Assessment
Audit Report
AUDIT #1604

August 10, 2016

INTERNAL AUDIT DEPARTMENT

Internal Audit Department
100 N. University Dr., Ste. 171
Fort Worth, Texas 76107
OFFICE: 817.814.1964
FAX: 817.814.1973
www.fwisd.org

Fort Worth
INDEPENDENT SCHOOL DISTRICT

Jacinto Ramos
Board of Education President
100 N. University Drive
Fort Worth, TX 76107

August 10, 2016

Dear Mr. Ramos:

Attached is your copy of the IT Risk Assessment Audit report (Audit #1604). As noted in the report, we identified several areas for improvement, including preparing a formal disaster recovery plan, using offsite storage for backed up files, preparing written policies and procedures, and developing a change management process.

We consider all responses received from staff to be adequate in addressing all issues noted in the audit. Loretta Salvatore was the lead auditor for this audit. Please do not hesitate to call me if you have questions or need additional information regarding any of the issues in the report. I look forward to assisting you and District management in the future in our efforts to develop a system of internal controls which will help safeguard the District's assets.

Respectfully,

Steve Shepherd, CPA, CIA, CGAP, CFF
Chief Internal Auditor

Cc: Members of the Board of Education
Dr. Kent Scribner, Superintendent
Kyle Davie, Chief of Department of Technology

FORT WORTH INDEPENDENT SCHOOL DISTRICT

AUDIT #1604

IT RISK ASSESSMENT

OVERALL EVALUATION

The overall organizational risk as it relates to technology was reviewed by a consultant, BDO. We identified several areas for improvement, including but not limited to:

- A formal disaster recovery plan is needed
- Offsite storage for backed up files is needed
- Written policies and procedures are needed
- A change management process is needed

BACKGROUND

The Fort Worth Independent School District Division of Technology is housed in the I.M. Terrell Way facility near downtown Fort Worth. This facility contains a state of the art data center, offices for support personnel, and training labs.

The Division of Technology group provides support for connectivity to over 140 sites that include schools, community centers, and administrative buildings in the District. This connectivity includes network connections for over 25,000 client computers and printers at these facilities. DoT supports the computer applications that collect demographics, attendance, grading, and associated data for the District's nearly 80,000 students. Additionally, DoT supports the computer applications for managing the District with over 10,000 employees.

SCOPE AND OBJECTIVES

This risk assessment was conducted in accordance with the Institute of Internal Auditors *International Standards for the Professional Practice of Internal Auditing.* The audit objective was to analyze the overall risk associated with the District's technology.

METHODOLOGY

The risk assessment involved interviews with Division of Technology personnel by the consultant and Internal Audit staff in order to provide focused information on the District's current security posture. Other testing was performed as deemed necessary under the circumstances.

AREAS FOR IMPROVEMENT

1. DISASTER RECOVERY PLAN

The District does not have a formal, up-to-date disaster recovery plan, even though it maintains critical financial and student information on its systems and network. A written and properly designed disaster recovery plan would help ensure continued operations in the case of a system or equipment failure or interruption.

RECOMMENDATION

Department of Technology should create a written disaster recovery plan and test it periodically.

RESPONSE

The Division of Technology concurs that there is not a centrally located, formal, written disaster recovery plan for *internally hosted applications*. While there is no comprehensive set of procedures, procedures do exist for many applications and systems, some formal and others informal.

The decision was made to leverage a hosted and on premise hybrid solution for disaster recovery in the most cost effective way possible. Applications which are hosted in the *cloud* or provided via *Software as a Service (SaaS)* include requirements that the application data be maintained and backed up regularly by the service provider.

The Division of Technology is committed to providing phase one of a centralized, electronic resource that will collect all documents related to disaster recovery, including existing and informal procedures and codifying them into formalized procedures for mitigation and recovery to satisfy this requirement by December 2016.

2. DATA BACK-UP

Although the District stores backup information, critical data is stored on storage devices in the same building as the District's servers. A plan is in place to create offsite storage later this year, however the District has been at risk for complete data failure until now. As a result, the District may not be able to restore data in the case of an emergency.

RECOMMENDATION

Department of Technology should store all backup data in a secure location that is not at the same site as the District's servers.

RESPONSE

There are two primary mission critical applications at Fort Worth ISD, the MUNIS Enterprise Resource Planning (ERP) and Focus Student Information System (SIS) applications. Only the MUNIS software and its associated data is hosted at the I.M. Terrell Way location.
At the time the interviews were being conducted, this assertion was true as it related to MUNIS. The Division of Technology corrected the issue as soon as it was identified and provide an immediate solution along with a long-term strategic remedy. To mitigate the risk, the MUNIS database and MUNIS software and configuration is now being backed up to the cloud. Plans are also underway to provide a full back-up replication at an off-site location.
The second mission critical system, the Focus Student Information System is hosted offsite and is backed up by the hosting vendor. Additionally, the District has a backup located at the I.M. Terrell Data Center for Focus Data.
As we move into the Region XI Data Center and eventually occupy the new facility location, the District will have two, geographically separate facilities for hosting offsite backups of data.
It is important to note that MUNIS is the only critical application that is locally hosted and locally backed up. All other critical systems such as the Focus Student Information System (SIS) are hosted and backed up via the cloud or service provider. The specific issue with MUNIS has been remedied as noted above.

3. POLICIES AND PROCEDURES

Department of Technology does not have procedures for all operations in a written format. The purpose for creating an internal control system through defining and documenting processes with well-written procedures boils down to a few very basic reasons.

- Compliance
- Consistency
- Operational Needs
- Managing Risks

While procedures themselves may not demonstrate compliance, well-defined and documented processes (i.e. procedures, training materials), along with records that demonstrate process capability, can make evident an effective internal control system and compliance to regulations and standards.

In addition, procedures are important to ensure that processes fundamental to the organization's success are properly guided by management, are performed in a consistent way that meets the organization's needs, and that important related information and data are captured and communicated. Procedures provide consistency in performing

transactions. The more consistent the process is from person to person, the less chance there will be quality problems. A written procedure is like a set of instructions for performing a task.

Procedures are important for managing risks by controlling processes, documenting the standard work that was performed at a point in time, and dependably training workers on the standardized business process. Policies and procedures help by providing employees with a handy reference to daily business operations, common company activities, and routine organizational tasks. Written procedures also help new employees get trained more quickly and up to speed on such things as management's expectations and internal controls.

Reduction of defects is another reason for written procedures. Due to staff turnover, knowledge base could be lost without written procedures.

RECOMMENDATIONS

a) The Department of Technology should ensure that procedures for all operations are documented in a written format.
b) The Department of Technology should document policies, procedures and processes to act as guidelines for use by those responsible for the logging, tracking, reporting, resolution and implementation of changes.
c) The Department of Technology should also document policies and procedures related to user access controls to protect the confidentiality, integrity, and availability of the information handled on the information systems.
d) The Department of Technology should document policies and procedures related to security events.
e) The Department of Technology should document policies and procedures related to the purchase of IT assets.
f) The Department of Technology should document policies and procedures to safeguard sensitive data as intellectual property and knowledge where all data/information resides.
g) The Department of Technology should document policies and procedures on system development and software usage.

RESPONSES

By January 2017, the Division of Technology is committed to developing a centralized location to store existing written procedures and existing unwritten procedures for:
a) All standard operational procedures (SOP).
b) Guidelines for logging, tracking, reporting, resolution and change implementation.
c) User access control procedures.
d) Security event management.
f) Procedures used to safeguard sensitive data, protect intellectual property and document data and information locations.
g) Document system development and software usage.

The Division of Technology assists customers with making technology procurement decisions and complies with the purchasing policies and procedures set forth by District policy and the Purchasing Department. Since the authority for these items rests solely with the Purchasing department, the Division of Technology requests that item e) should be reassessed as a finding.

4. CHANGE MANAGEMENT PROCESS

Developers in the IT department have access to production in MUNIS, but nobody is monitoring this access. In addition, the Department of Technology does not have a process to routinely review Audit Logs. Currently Audit Logs are reviewed only when there is suspicion of an attempt to access the network inappropriately. Audit Log data can identify what accounts are associated with certain events. This information then can be used to highlight where training and/or disciplinary actions are needed. Audit Log data can be reviewed chronologically to determine what was happening both before and during an event. For this to happen, the accuracy and coordination of system clocks are critical. To accurately trace activity, clocks need to be regularly synchronized to a central source to ensure that the date/time stamps are in synch. Unusual or unauthorized events can be detected through the review of log data, assuming that the correct data is being logged and reviewed. Unusual activity can include failed login attempts, login attempts outside of designated schedules, locked accounts, port sweeps, network activity levels, memory utilization, key file/data access, etc. In the same way that log data can be used to identify security events, it can be used to identify problems that need to be addressed. For example, investigating causal factors of failed jobs, resource utilization, trending and so on can help to identify problems that need to be addressed. A lack of routine monitoring of security events recorded on Audit Logs may lead to the potential for security breaches and result in a loss of critical data.

The District needs to assure that the negative impact of change to its information technology change management system is minimized in order to avoid disruption to the development and production processes. The only way to do this effectively is through a system for IT change management that is sanctioned by upper management.

In addition, lack of change management may lead to incorrect or unauthorized changes made to the District's production system environment, leading to errors in part from potential security breaches. Also, lack of change management practices may lead to the inability to detect incidents quickly, contain and mitigate impact, and restore and reconstitute services in a trusted manner to address security violations and prevent system downtime.

RECOMMENDATION

Department of Technology should monitor change logs to help ensure that access to the network is appropriate.

RESPONSE

We concur the coordination of system clocks are critical to ensure the entire enterprise is accurate on the network. This practice was implemented by the Division of Technology since converting to Active Directory several years ago. The Division of Technology maintains log file for various systems including: server and desktop operating systems, application, system services, network switching equipment, firewalls, and content filtering among many other logs. These logs are comprised of enormous volumes of data which can be complex to review on a daily basis.

To address the issue of the quantity of data, the Division of Technology has adopted a more stratified and focused approach to log file auditing and management. First the District relies on Microsoft Active Directory to provide authorized users access to the network. I t enforces a specific authentication policy during login and places limitations around the number of failed login attempts before an account becomes deactivated. Additionally, the District uses Active Directory to assign detailed user access privileges to applications based on roles defined within Active Directory. This keeps unauthorized users from accessing unauthorized District information.

In terms of auditing of logs, the Division of Technology relies on individual application owners to review access logs for their systems. If those owners identify an issue, the Division of Technology and the application owner work with the application vendor to utilize the log files to resolve the issue.

Finally, network component logs are recorded through an analysis tool which can be used for mitigation if a threat is identified.