Houston Independent School District

2018-2019 Information Technology Risk Assessment Report and IT Audit Plan

Issue Date: April 24, 2018

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

1.0 INTRODUCTION

BDO USA, LLP (BDO) was engaged to update the IT risk assessment of the applications, processes, infrastructure and projects at Houston Independent School District (HISD). The IT risk assessment provides management with an evaluation of IT related elements and their potential to negatively impact the organization. Elements identified as having a significant potential impact are considered in the annual audit plan. The IT risk assessment evaluated IT related elements based on their potential impact to the five following business areas:

- Strategy
- Financial
- Reputation
- Compliance
- Operational

In addition, the following IT risk areas were also assessed for each entity:

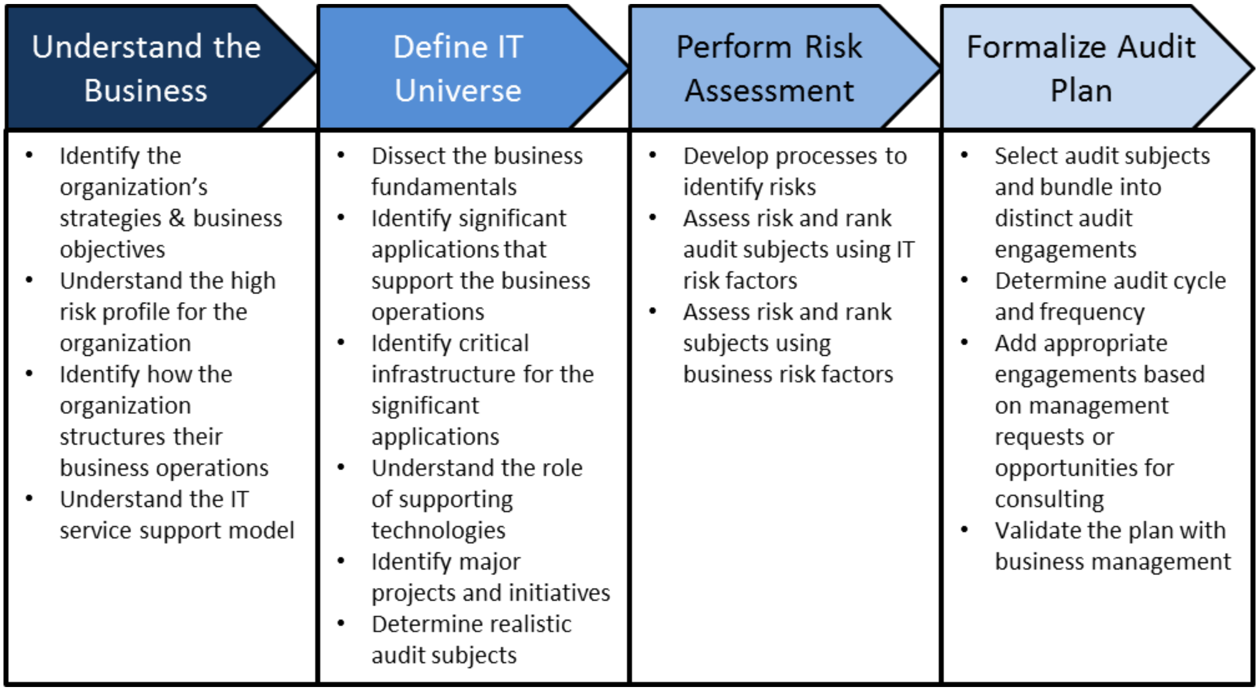
- Major changes to the entity
- Availability
- Integrity
- Confidentiality
- Privacy

The purpose of this IT risk assessment is two-fold.

- Identify risks that IT presents to the District that could have an adverse effect; and
- Identify the IT audit universe, examine the IT auditable units and select areas with the greatest risk exposure to review and include in a one year IT audit plan.

1.1 OUR APPROACH

BDO followed a standard four-step risk assessment methodology that is based on Institute of Internal Auditors (IIA) and Information Systems Audit and Control Association (ISACA) recommended best practices for IT risk assessments. This process ensures that the foundation of the IT audit plan is based on the organization’s objectives, strategies, and business model. Figure 1 depicts the logical work-flow progression using a top-down approach to define the IT audit plan that was used.



Understand the Business

- Identify the organization’s strategies & business objectives
- Understand the high risk profile for the organization
- Identify how the organization structures their business operations
- Understand the IT service support model

Define IT Universe

- Dissect the business fundamentals
- Identify significant applications that support the business operations
- Identify critical infrastructure for the significant applications
- Understand the role of supporting technologies
- Identify major projects and initiatives
- Determine realistic audit subjects

Perform Risk Assessment

- Develop processes to identify risks
- Assess risk and rank audit subjects using IT risk factors
- Assess risk and rank subjects using business risk factors

Formalize Audit Plan

- Select audit subjects and bundle into distinct audit engagements
- Determine audit cycle and frequency
- Add appropriate engagements based on management requests or opportunities for consulting
- Validate the plan with business management

Figure 1 – IT Audit Plan Development Process

In order to execute the IT risk assessment in an efficient manner while also ensuring a comprehensive review, the Control Objectives for IT and Related Technologies (COBIT[1]) framework developed by ISACA was leveraged to select the IT process areas for review, based on their potential to introduce or remediate risks within the HISD environment. Additionally, key applications as well as the network architecture, security monitoring processes and disaster recovery were incorporated into the review.

The resultant risk assessment data leverages prior year’s IT risk assessment, our understanding of the technical environment as well as interviews with HISD personnel during October and November 2017.

[1] COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise information and technology assets (IT).

1.2 KEY PARTICIPANTS

The project team received valuable input from various HISD IT personnel in order to understand: the key strategic objectives planned for the coming year, how IT enables the business to achieve those objectives and each individual's perspectives on the critical IT risks that will be facing HISD. Their input contributed to the development of the risk summary abstracts provided in this report.

Table 1 lists the HISD personnel who were interviewed and/or provided feedback on the identified risk areas and the associated assessment of their risk ratings.

Person	Responsibilities
Dr. Grenita Lathan	HISD Interim Superintendent
Lenny Schad	Chief Technology Officer
Garland Blackwell	Chief Audit Executive
Scott Gilhousen	Director IT Infrastructure Engineering & Operations
Cindy Rae Fancher	Director IT PMO
Patrick Porter	Director IT Data and Business Solutions
Pat Collins	Director IT Administration & Strategic Planning
Frank Williams	Director IT Student Management Systems
Preeti Burns	Director IT Customer Service
Kristy Sailors	Director IT Education Technology
Glenn Johnson	Manager, Financial and Operational Audit

Table 1 – IT Risk Assessment Participant List

1.3 METHODOLOGY

BDO's standard IT risk assessment approach follows best practices established by the IIA and ISACA as published in the IIA's Global Technology Audit Guide (GTAG), and as illustrated previously in Figure 1 on page 4. The purpose of the IT risk assessment was to identify all relative IT risks and determine the scope of IT audits over the next year. The risk assessment will allow the IT audit team to focus on areas of higher risk and reduce audit efforts in areas of lower risk.

The process began with interviewing key stakeholders to identify the critical business processes and the supporting IT processes and systems. BDO independently risk assessed each of the IT applications, processes and projects based on the information gathered from HISD, including prior audit history. The high level steps involved in this assessment included the following.

- Understand the Business
- Define the IT Universe
- Perform the Risk Assessment
- Develop/Update the IT Audit Plan

1.3.1 Understanding the Business – An important perspective in performing the IT risk assessment is to understand that IT only exists to support and further an organization's objectives, and that IT is a risk to the organization if its failure results in the inability to achieve a business objective. Thus it is important to first understand HISD's objectives, strategies, business model, and the role that technology has in supporting the business. This was accomplished by identifying the risks found in the technologies used and how each risk might prevent the organization from achieving business objectives.

Please refer to Figure 2 below for a depiction of the IT environment in a business context.

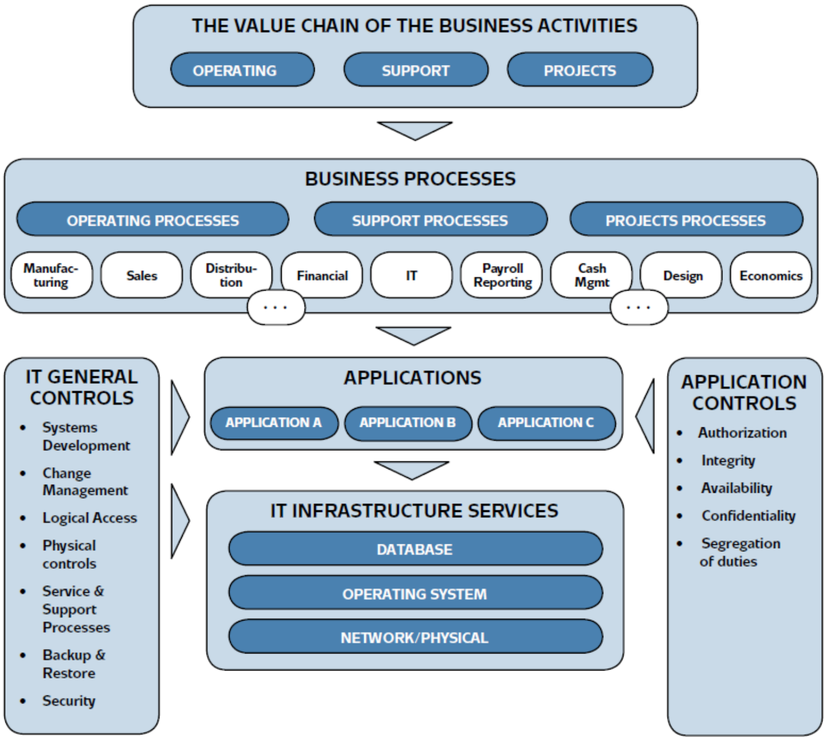


Figure 2 – IT Environment in a Business Context

Figure 2 was leveraged from: *Developing the IT Audit Plan*, The Institute of Internal Auditors, 2008.

1.3.2 Define IT Universe – We started with the prior year's IT Audit universe, and:

- Obtained current application, project and integration listings and added them to the universe.
- Conducted key interviews with management.
- Met with management to review the updated IT Audit Universe and obtained their input regarding risk.
- Performed an independent risk ranking of the components in the IT Audit Universe.
- Reviewed and agreed upon the high risk components with management.

Referring to Figure 2 on page 6, the IT audit universe includes: IT Management Processes, IT General Controls, Applications, Projects, and IT infrastructure. The following specific audit entities comprise the IT audit universe for each of the aforementioned categories. Some examples of the Categories in the IT Audit Universe are shown below.

1.3.2.1 IT Audit Universe – IT General Controls

IT General Controls
Disaster Recovery
Change Management
Systems Development
Data Center Security
Backup & Restore
Physical Security of IT Assets
Patch Management

Table 2 – Significant IT General Controls included in the IT Audit Universe

1.3.2.2 IT Audit Universe – Significant Applications

Application/System
OneSource (SAP)
HISD Connect
Enterprise Data Warehouse
TADS
Find A School
Budgets Online
SharePoint 2013
HUB (ItsLearning)
OnTrack

Table 3 – Significant Applications included in the IT Audit Universe

1.3.2.3 IT Audit Universe – Significant Projects

Projects
HISD Connect
SAP GRC Process Controls
SAP Maintenance Upgrade
SAP PBC
SAP SRM Enhancements
Volunteer Connect

Table 4 – Significant Projects included in the IT Audit Universe

1.3.2.4 IT Audit Universe – Supporting IT Infrastructure

IT Infrastructure
Network Administration and Security (IT Security Maturity Assessment)
MS SQL Database Administration and Security
Cloud Computing
Enterprise Data Network
Mobile Devices

Table 5 – Significant IT Infrastructure included in the IT Audit Universe

1.3.2.5 IT Audit Universe – Supporting IT Management

IT Management
IT Governance
Data Management
In-House Software Development
Vendor Management
Security Event Management
Compliance Management
Staffing/Recruiting

Table 6 – Significant IT Management included in the IT Audit Universe

1.3.3 Perform Risk Assessment – Once an inventory of the IT universe was completed, the next step was to evaluate the risks and likelihood of the risks being exploited across several business and technical risk areas. The risks were assessed on the likelihood of the risk being exploited as well as the impact. Both the likelihood and impact were evaluated as either High=3, Medium=2 or Low=1. Table 6 provides definitions for the risk levels for the likelihood of the risk occurring and Table 7 provides a definition of the impact of the risk.

Likelihood Scale		
H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low probability that the risk will occur.

Table 6 – Risk probability matrix

Impact Scale		
H	3	The potential for material impact on the organization's financials, assets, reputation, or stakeholders is high.
M	2	The potential for material impact on the organization's financials, assets, reputation, or stakeholders may be significant to the audit unit, but moderate in terms of the total organization.
L	1	The potential impact on the organization is minor in size and/or limited in scope.

Table 7 – Risk impact matrix

The likelihood and impact ratings were multiplied for each risk area and the resultant values were summed across all risk areas to arrive at a numerical composite risk factor. Based on this formula and risk areas assessed, the maximum risk rating is 99 and the minimum is 11. The composite values were categorized as a High risk (71-99), Medium risk (39-70) or Low risk (11-38).

The following business risk areas were assessed for each IT audit universe element:

- **Strategic** – Evaluated based on the potential to impact HISD's strategic objectives.
- **Financial** – Considered the potential financial impact of the identified IT risk areas.
- **Reputational** – Evaluated the potential exposure of negative events in relation to IT systems, processes, and projects that can affect the reputation of HISD.
- **Compliance** – Identified the areas that could have a negative impact on HISD's compliance to external requirements.
- **Operational** – Weighed the impact that IT systems, processes, and project risks would have on daily HISD operations.

Audit entities were also assessed based on historic audits and changes:

- **Changes (Major/Minor)** – Significance of changes during the period of review applied to the element being reviewed.
- **Time Since Last Audit** – Used to understand if or when the universe element was last audited.
- **Prior Audit Results** – The significance of findings from prior audits.

Finally, each element was also reviewed based on information risks considered:

- **Availability** – The impact and importance of the availability of systems.
- **Integrity** – Maintaining and assuring the accuracy and consistency of HISD data over its entire life-cycle.
- **Confidentiality** – Measures that were undertaken to ensure confidentiality is designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it.
- **Privacy** – Measures in place to ensure that appropriate levels of protection were in place relative to identifying and addressing legislative and regulatory requirements for protecting personal information, including:
  - PII - Personally identifiable information, e.g. name, social security number, date and place of birth, mother's maiden name, biometric records.
  - PHI - Protected Health Information - individually identifiable health information.
  - PCI - Payment Card Information - primary account number (PAN), and may also include cardholder name and expiration date. Can also include Security-related information used to authenticate cardholders and/or authorize payment card transactions stored on the card's magnetic stripe or chip.

1.3.4 Develop IT Audit Plan – In order to arrive at a suggested audit plan, the audit universe items with a composite score of Medium or High risk were further evaluated to identify similarities and synergies that could decrease the total hours required to audit the group of items versus the sum of hours required for each discreet audit; this resulted in the identification of several group audits. Finally, estimated hours were applied to the group audit areas. The audit plan was selected by summing the hours of the risk-ranked group audits until the established budget was fully allocated.

Table 8 identifies the IT audit universe entities that were grouped into the suggested audits.

Audit Entity	Risk Total	Monte Carlo Risk Evaluation* (90% Probability)	Comment
OneSource (SAP)	81	$20,000 to $110,000	Risk rating based on the new implementation of SAP as well as incidents identified in current year related to SAP data.
IT Vendor Management	75	$15,000 to $350,000	Risk rating based on the District's risk management processes to establish, manage, and monitor IT outsourcing relationships.
Network Administration and Security (IT Security Maturity Assessment)	74	$80,000 to $2,000,000	Assess security maturity against a security framework, e.g. NIST. Risk rating and Monte Carlo evaluation based on cost of breaches at like organizations.
HISD Connect (SIS)	72	$45,000 to $1,500,000	Post-implementation review with a focus on security in the hosted application environment. Risk rating based on sensitivity of data stored within the application.
Data Privacy	71	$80,000 to $2,000,000	Validate data management model is in compliance with data privacy regulations. Risk rating and Monte Carlo based on cost of violating regulatory requirements. Fines for violating these regulations can be heavy. Some examples of the regulatory requirements are: - COPPA - $15,000 to $40,000 fine per individual violation - CIPA – Withholding funds/grants. - FERPA – Withholding of funds/grants.
Cloud Computing	71	$20,000 to $1,000,000	Review the cloud strategy for HISD and one Cloud solution in place. Risk rating based on unknown cloud solutions and the possibility of the storing of sensitive data in a cloud environment not subject to HISD controls.

Table 8 – IT audit universe suggested audits

*To evaluate the financial risk exposure of the selected audits, Internal Audit performed the Monte Carlo risk analysis. This was done using the expected ranges of financial exposure for the given risk area and performing a statistical analysis model on each area to determine what the risk exposure is within a 90% probability. For each assessment we performed 10,000 random evaluations of the exposure and determined where 90% of that exposure was captured. For example, the probability that SAP has an incident during the year is 100%. That incident can range in cost to remediate from $500 to $1M. There is a 70% probability that the incident will cost below $1,000 to remediate. However, there will be potentially multiple occurrences of these incidents per year. Based on the Monte Carlo analysis, there is a 90% probability that the total number of incidents related to SAP will range from $20,000 to $110,000 during the year.

2.0 SUMMARY RISK ASSESSMENT RESULTS

The IT risk universe was ranked using a number of risk factors based on HISD input and BDO observations. These risk factors were combined into two overall risk categories.

1 Impact: The criticality of the IT risk element to the business operations as a whole. Stated differently, what impact does the IT risk element have on the strategic, operational, legal/regulatory and/or financial reporting performance of the District?

2 Probability: The perceived inherent IT risk related to applications, infrastructure/architecture, IT processes and projects.

The following diagram illustrate the risk assessment results based on these two categories. The top 15 IT risks identified are shown below, in order of descending risk and priority.

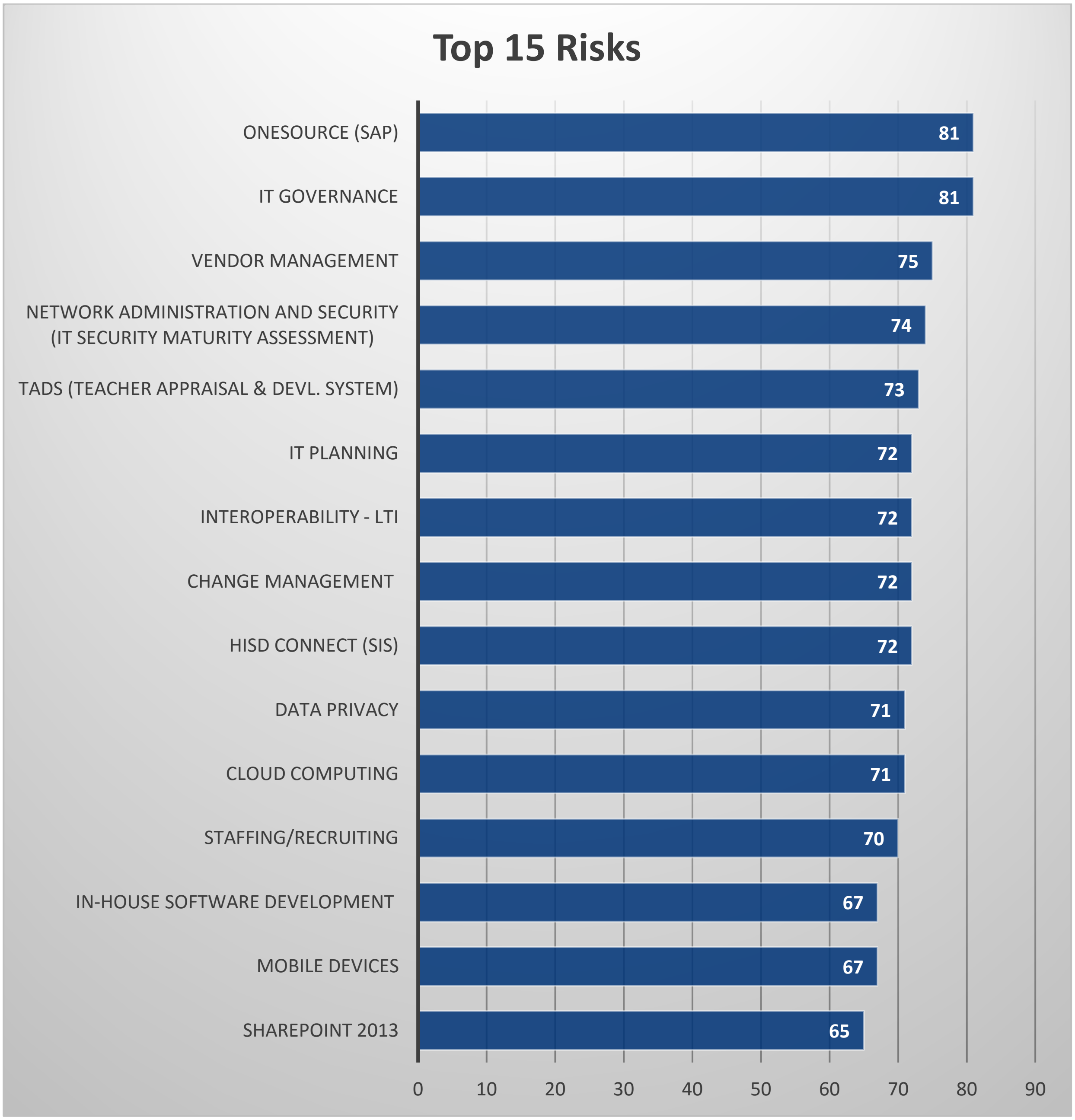


Figure 4 - Summary Risk Assessment Results – IT Risk Chart

The scores were calculated as described in section 1.3.3 of this document. The scale for the scores were from a low of zero (0), representing no risk, to a high of 100, representing maximum risk and exposure.

Note(s):

1. Given the District-wide cuts in budgets and staff in key areas such as IT, the Controller's area and Internal Audit, the District could be exposed to an increase in fraud, waste and/or abuse.

2. By definition, IT Governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives, including how emerging technologies are managed (i.e. the Internet of Things (IoT), Artificial Intelligence (AI), and robotics etc.).
3. Data Privacy is a subset of IT Governance, but has been identified separately due to the high volume of sensitive student data that is processed, transmitted and stored by HISD.

3.0 IT AUDIT PLAN

The table below shows the proposed 2018-2019 IT audit plan based on this IT risk assessment.

2018-2019 IT Audit Plan				
Priority	**IT Audit**	**Hours**	**Start**	**Duration**
1	OneSource (SAP)[2]	300	July	8 - 10 Weeks
2	Network Administration and Security (IT Security Maturity Assessment)	300	Mar	6 – 8 Weeks
3	HISD Connect (SIS)	350	Nov	6 – 8 Weeks
4	Cloud Computing	300	Sept	6 – 8 Weeks
5	Data Privacy	250	Jan	6 – 8 Weeks
6	IT Vendor Management	220	Jul-Sep	4 – 6 Weeks
7	IT Risk Assessment/Update	100	May	2 – 3 Weeks
8	Follow-up Audit	80	Jun	1 – 2 Weeks
	Total	**1,900**		

Table 10 – IT Audit Plan

Audit	Background/Reason for Selection
OneSource (SAP)	Recurring validation of the effectiveness of HISD's SAP controls in place to carryout management's objectives for the District, in terms of finance, human resources, procurement and other supported processes.
Cloud Computing	Review the cloud strategy for HISD and review a cloud solution, e.g. eSHARS[3] (Chancery to eSHARS cloud) as part of this audit.
HISD Connect (SIS) Review	Due to the significance of this new application, a post-implementation assessment is scheduled to be performed.
IT Security Maturity Assessment	To determine the maturity level of the District's IT Security with the goal of integrating security controls into architectural approaches that increase security while reducing risks, costs, and breakage experienced in reacting to ever-changing threats.

[2] Specific SAP module(s) will be selected for review based on risk.

[3] School Health and Related Services is a Medicaid Program that is designed to reimburse the District for providing direct services to their Special Education students.

IT Vendor Management	To evaluate the District's risk management processes to establish, manage, and monitor key IT outsourcing relationships, allowing the District to offer cost effective alternatives to in-house capabilities. However, outsourcing does not reduce the fundamental risks associated with IT or the organizations that use it. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information, and regulatory action remain. [4]
Data Privacy	Validate that the data management model is in compliance with data privacy regulations, particularly student information, as the lack of compliance with FERPA[5], CIPA[6], and COPPA[7] could lead to issues with federal funding.

[4] FFIEC IT Booklet Outsourcing Technology Services

[5] FERPA - Family Educational Rights and Privacy Act

[6] CIPA- Children's Internet Protection Act

[7] COPPA - Children's Online Privacy Protection Act from the Federal Trade Commission (FTC)