HOUSTON INDEPENDENT SCHOOL DISTRICT
HATTIE MAE WHITE EDUCATIONAL SUPPORT CENTER
4400 WEST 18th STREET • HOUSTON, TEXAS 77092-8501

RICHARD A. PATTON, CPA, CFE
Chief Audit Executive
Tel: 713-556-7500 • Fax: 713-556-6374

February 9, 2015

Dear Board Audit Committee Members,

Please see the attached report for your approval.

The Office of Internal Audit has completed a formal risk assessment of information technology (IT) within the Houston Independent School District (HISD). As you are aware, we developed a co-sourcing arrangement with BDO USA, LLP (BDO) to assist in the assessment process under my direction. The risk assessment results provide vital data to HISD leadership and to Internal Audit for the development of an annual audit plan. The results are important to enable an understanding of the level of IT risk tolerance acceptable by HISD leadership and the Board of Education.

I appreciate the level of passion and cooperation from all the Chiefs, and especially the time and energy from the IT group.

Regards,

Richard Patton
Chief Audit Executive, Office of Internal Audit

Attachment

cc: Terry B. Grier, Superintendent of Schools
Leo Bobadilla, Chief Operating Officer
Daniel Gohl, Chief Academic Officer
Shonda Huery Hardman, Chief School Support Officer
Don Hare, Chief Major Projects
Andrew Houlihan, Chief Human Resources Officer
Kenneth Huewitt, Chief Financial Officer
Lenny Schad, Chief Technology Officer
Mark Smith, Chief Student Support
Helen Spencer, Chief Communications Officer
Jason Spencer, Chief of Staff
Elneita Hutchins-Taylor, General Counsel

OFFICE OF INTERNAL AUDIT

Information Technology Risk Assessment Report

Houston Independent School District

Board Audit Committee

Date Issued:
2/9/2015

ATTACHMENT

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

1.0 INTRODUCTION

BDO USA, LLP (BDO) was engaged to conduct a risk assessment of the IT applications, processes, infrastructure and projects at Houston Independent School District (HISD). The 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 will be considered for inclusion in the next 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

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

- Identify risks that IT presents to the business that could adversely affect the business; and
- Identify the IT audit universe, examine the IT auditable units and select areas with the greatest risk exposure to review and include in the IT audit plan.

1.1 OUR APPROACH

BDO followed a standard four-step risk assessment methodology that is based on the 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.

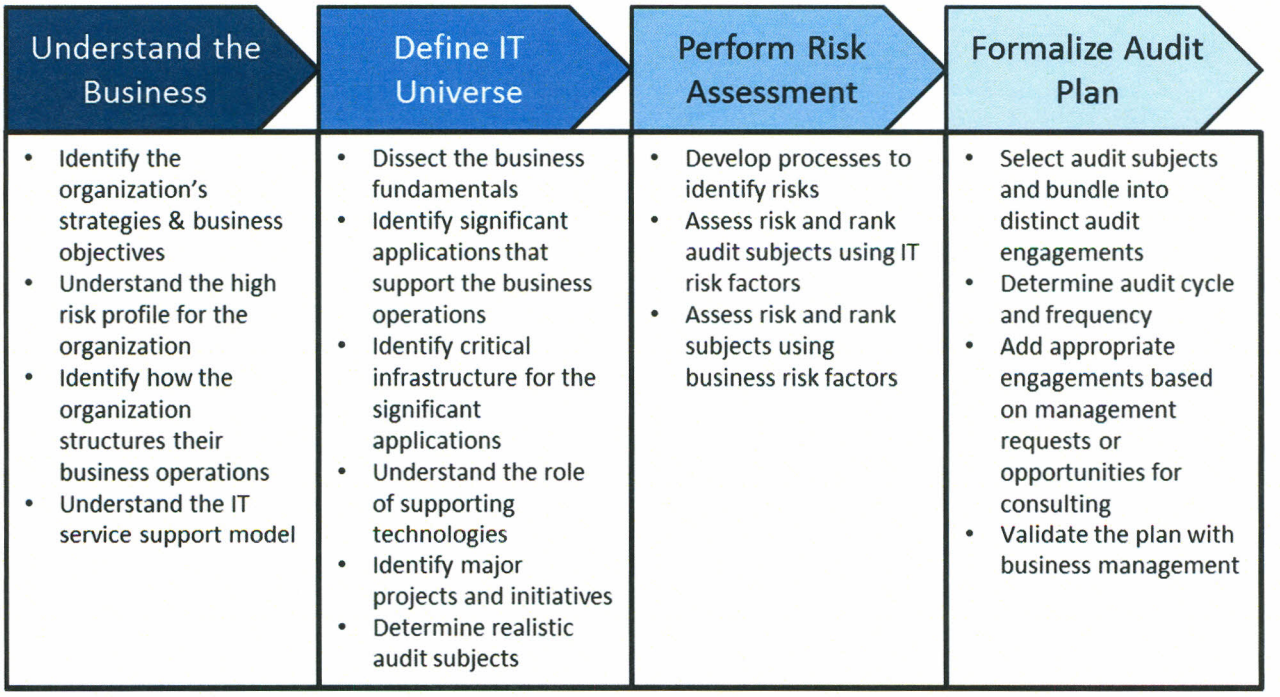

Figure 1 – IT Audit Plan Development Process

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) 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 business continuity were incorporated into the review.

The resultant risk assessment data is based on BDO's understanding of HISD's technical environment that was derived from interviews with HISD personnel, prepared by client (PBC) documents provided to BDO, and risk self-assessments that were facilitated by BDO and reviewed with HISD personnel. Additionally, BDO leveraged our experience with other entities as a benchmark for identifying key risk areas to ensure that areas that traditionally have a potential to introduce measurable risk were evaluated and their resultant risk ratings were within tolerance of expected results.

1.2 KEY PARTICIPANTS

The project team received valuable input from various HISD IT and business management level 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 facing HISD. Their input contributed to the development of the risk summary abstracts provided in this report.

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

Person	Responsibilities
Leo Bobadilla	Chief Operating Officer
Daniel Gohl	Chief Academic Officer
Don Hare	Chief Major Projects
Andrew Houlihan	Chief Human Resources Officer
Shonda Huery	Chief School Support Officer
Kenneth Huewitt	Chief Financial Officer
Richard Patton	Chief Audit Executive (and acting ECO)
Lenny Schad	Chief Technology Information Officer
Mark Smith	Chief Student Support Officer
Helen Spencer	Chief Communications Officer
Jason Spencer	Chief of Staff
Beatriz Arnillias	Sr. Mgr. IT Instructional Technology
Pat Collins	Sr. IT Mgr. IT Administration & Strategic Planning
Cindy Rae Fancher	IT Director PMO
Scott Gilhousen	Director IT Infrastructure Engineering & Operations
Elneita Hutchins-Taylor	General Counsel
Veronica Mabasa	Board Services Team Lead
Christina Masick	IT General Manager
Raymond McDonald	IT Customer Service
Patrick Porter	Sr. IT Manager Data Governance
Suzanne Tyrell	Director Information Technology Business Solutions

Table 1 – IT Risk Assessment Interviewee List

1.3 METHODOLOGY

This effort was based on BDO's standard IT risk assessment approach, which 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. The purpose of the IT risk assessment was to identify all relative IT risks and determine the scope of IT audits over the next few years. 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 IT Universe
- Perform Risk Assessment
- Develop/Update 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.

In order to gain an understanding of the business, a prepared by client (PBC) list of organizational documents was requested from HISD at the beginning of the IT risk assessment. The PBC items requested and received included organizational charts, HISD strategy documents (e.g., mission, vision and value statements), strategic plans and business plans. After reviewing the aforementioned information, an exercise was performed with Internal Audit to identify the key processes that are critical to the objectives' success. Please refer to Figure 2 for a depiction of the IT environment in a business context.

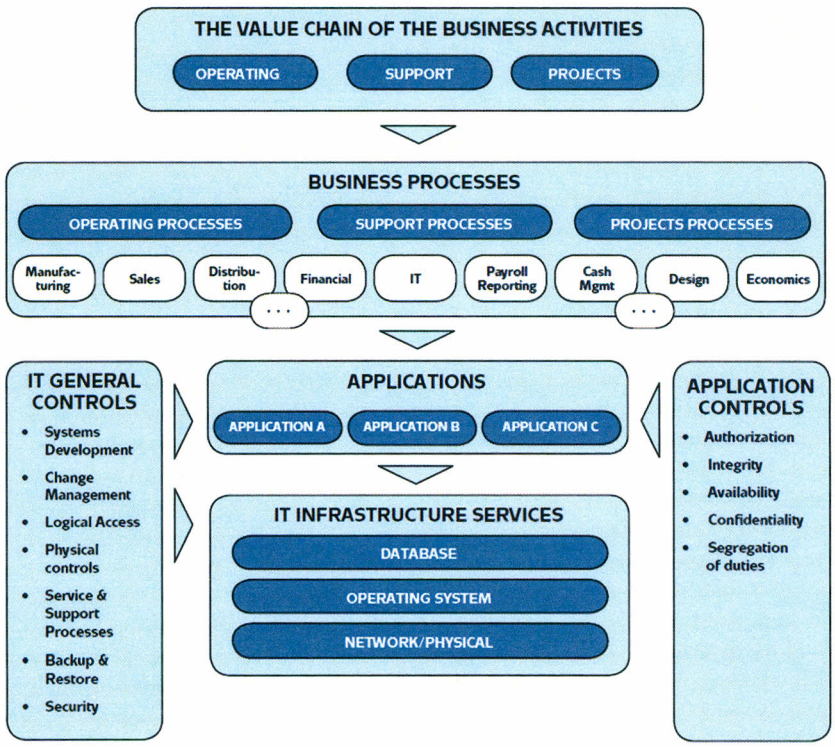

Figure 2 – IT Environment in a Business Context

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

IT environmental factors also have an impact on a processes ability to support objectives. The environmental factors considered included:

1. The degree of system and geographic centralization
2. The technologies deployed
3. The degree of customization
4. The degree of formalized company policies and standards (i.e., IT governance)
5. The degree of regulation and compliance
6. The degree and method of outsourcing
7. The degree of operational standardization
8. The level of reliance on technology

1.3.2 Define IT Universe – One of the first steps to building an audit plan is to define the IT universe, a finite and all-encompassing collection of audit areas, organizational entities, and locations identifying business function that could be audited to provide adequate assurance on the organization's risk management level. Defining the IT audit universe requires knowledge of the organization's objectives, business model and the IT service support model – all of which were identified in the prior step.

The information gathered was consolidated into the IT audit universe. Data was normalized, negligible components/systems were eliminated from review, and all components were flagged as critical or non-critical where non-critical components neither supported an important business function nor had the potential to negatively impact any business or technical functions.

Referring to Figure 2, 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.

1.3.2.1 IT Audit Universe – IT Management Processes

CoBIT IT Management Processes		
Evaluate, Direct and Monitor	**Align, Plan and Organize**	**Build, Acquire and Implement**
*Ensure Governance Framework & Maintenance Ensure Benefits Delivery Ensure Risk Optimization Ensure Resource Optimization Ensure Stakeholder Transparency	*Manage the IT Management Framework Manage Strategy Manage Enterprise Architecture Manage Innovation Manage Portfolio Manage Budget and Costs *Manage Human Resources Manage Relationships Manage Service Agreements *Manage Suppliers Manage Quality Manage Risk *Manage Security	*Manage Programs and Projects Manage Requirements Definition *Manage Solutions Identification and Build Manage Availability and Capacity Manage Organizational Change Enablement *Manage Changes Manage Change Acceptance and Transitioning Manage Knowledge *Manage Assets Manage Configuration
Deliver, Service and Support	**Monitor, Evaluate and Assess**	
*Manage Operations *Manage Service Requests and Incidents *Manage Problems *Manage Continuity *Manage Security Services Manage Business Process Controls	Monitor, Evaluate and Assess Performance and Conformance Monitor, Evaluate and Assess the System of Internal Controls *Monitor, Evaluate and Assess Compliance With External Requirements	

Figure 3 – CoBIT Based IT Management Processes

*Processes included in risk assessment scope. Manage Assets was further defined to explicitly include Data Assets and Software License Assets.

1.3.2.2 IT Audit Universe – IT General Controls

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

Table 4 – Significant IT General Controls included in the IT Audit Universe

1.3.2.3 IT Audit Universe – Significant Applications

Application/System	
AppliTrack	Primero
Approva One	Prolog
AS400 Student Data	PSC - Parent Student Connect
Board Agenda Builder (BAB)	SAP
Catamaran	SchoolMessenger
Centricity2 (School Wires)	Security Provider
Certify (by Certica)	SharePoint
Chancery SMS	SIS Security database (Gradespeed)
CROSE - Check Register Online	SPATS
DAEP and JJAEP	Summer School - Chancery
Dreambox	Summer School - Gradespeed
EasyIEP	Summer School - PSC
eSHARS	Synovia
ED Plan	TADS
Find A School	Texas State Unique ID - Students
HFWE - High Frequency Word Evaluation	TimeClock (Primero)
Houghton Mifflin - Write Source	Tipweb Academic Inventory (Textbooks)
iStation	Tipweb IT Asset Tracking
JDP	Trapeze
Moodle	Vignette
MSHP - Membership Reporting	VISITS/VIPS
My HISD Apps	Employee Services - SB9 Finger printing
Office 365	ODS
PEIMS	HISD Connect - Employee Portal
PeopleSoft HCM	HISD Website

Table 2 – Significant Applications included in the IT Audit Universe

1.3.2.4 IT Audit Universe – Significant Projects

Projects
District Online Payment System
eContracts & Purchase Orders for Services Initiative
Edulog - Software Implementation
Medicaid Revenue Maximization System
PowerUP:HUB - 3rd Party Applications
PowerUP:HUB - Phase II
Riverside - IOWA Integration
SAP Reimplementation
Infrastructure Refresh

Table 3 – Significant Projects included in the IT Audit Universe

1.3.2.5 IT Audit Universe – Supporting IT Infrastructure

IT Infrastructure
Network Administration and Security
MS SQL Database Administration and Security
Cloud Computing
Remote Network Access
Windows Administration and Security
Enterprise Voice Network
Enterprise Data Network
Mobile Devices
IT Hardware
Network Administration and Security
MS SQL Database Administration and Security
Cloud Computing

Table 5 – Significant IT Infrastructure 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 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 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:

- **Availability** – Considered the impact and importance of the availability of systems.
- **Integrity** – Considered maintaining and assuring the accuracy and consistency of HISD data over its entire life-cycle.
- **Confidentiality** – Considered measures were undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it.

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	Audit Priority	Audit Objective
Compliance Management	58	1	IT Control Environment Review
In-House Software Development	51	1	IT Control Environment Review
IT Governance	51	1	IT Control Environment Review
IT Resources	50	1	IT Control Environment Review
Staffing/Recruiting	50	1	IT Control Environment Review
Large-Scale IT Project Management	46	1	IT Control Environment Review
IT Support and Problem Management	40	1	IT Control Environment Review
SAP Reimplementation **- Approva Upgrade v10.0.2** **- Peoplesoft Account String Modification** **- OCM & Training**	76	2	PMO Review
PowerUP:HUB **- Phase II** **- 3rd Party Applications**	72	2	PMO / PIR Review
Medicaid Revenue Maximization System	50	2	PMO / PIR Review
Infrastructure Refresh	49	2	PMO / PIR Review
District Online Payment System	44	2	PMO / PIR Review
Edulog - Software Implementation	44	2	PMO / PIR Review
Voice over IP Project	41	2	PMO / PIR Review
eContracts & Purchase Orders for Services Initiative	40	2	PMO / PIR Review
		2	Select PIR Review (s)
Network Administration and Security	71	3	Security / VAPT
MS SQL Database Administration and Security	64	3	Security / VAPT
Remote Network Access	53	3	Security / VAPT

Audit Entity	Risk Total	Audit Priority	Audit Objective
Windows Administration and Security	51	3	Security / VAPT
Enterprise Voice Network	45	3	Security / VAPT
Enterprise Data Network	45	3	Security / VAPT
Bus Cameras	42	3	Security / VAPT
Business Continuity	80	4	ITGC Controls Review
Data Center Security	71	4	ITGC Controls Review
System Operations	55	4	ITGC Controls Review
Backup & Restore	52	4	ITGC Controls Review
Systems Development	51	4	ITGC Controls Review
Vendor Management	44	4	ITGC Controls Review
Physical Security of IT Assets	43	4	ITGC Controls Review
Software License Management	42	4	ITGC Controls Review
Change Management	40	4	ITGC Controls Review
Chancery SMS	72	5	Application Audit(s)
Summer School - Chancery	72	5	Application Review / Audit
eSHARS	60	5	Application Review / Audit
ED Plan	54	5	Application Review / Audit
Vignette	54	5	Application Review / Audit
TADS	53	5	Application Review / Audit
PEIMS	48	5	Application Review / Audit
AS400 Student Data	47	5	Application Review / Audit
PeopleSoft HCM	46	5	Application Review / Audit
Approva One	44	5	Application Review / Audit
ODS	42	5	Application Review / Audit
EasyIEP	41	5	Application Review / Audit
Find A School	40	5	Application Review / Audit
SAP	40	5	Application Review / Audit
Houghton Mifflin - Write Source	39	5	Application Review / Audit
SIS Security database (Gradespeed)	39	5	Application Review / Audit
Summer School - Gradespeed	39	5	Application Review / Audit
HISD Website	39	5	Application Review / Audit
Data Management	72	6	Sensitive Data Review
Security Event Management	80	7	Event Monitoring & Response Review
IT Asset Management & Procurement			

Audit Entity	Risk Total	Audit Priority	Audit Objective
	62		
Cloud Computing	60		
			2015 IT Risk Assessment
			Planning and Review

Table 8 – IT audit universe suggested audits

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 business?

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

The following diagrams illustrate the risk assessment results based on these two categories. The IT elements in the upper right quadrant represent the most likely items to consider for coverage on audits. Those elements in the remaining quadrants have a lesser risk and should be considered in conjunction with other integrated assessment efforts.

Projects	
1	SAP Reimplementation
4	PowerUP:HUB
10	Medicaid Revenue Maximization System
11	Infrastructure Refresh
16	District Online Payment System
17	Edulog - Software Implementation
20	Voice over IP Project
23	eContracts & Purchase Orders for Services Initiative

Applications	
2	Chancery SMS
3	Summer School - Chancery
6	eSHARS
7	ED Plan
8	Vignette
9	TADS
12	PEIMS
13	AS400 Student Data
14	PeopleSoft HCM
15	Approva One
18	ODS
19	EasyIEP
21	Find A School
22	SAP
24	Houghton Mifflin - Write Source
25	SIS Security database (Gradespeed)
26	Summer School - Gradespeed
27	HISD Website

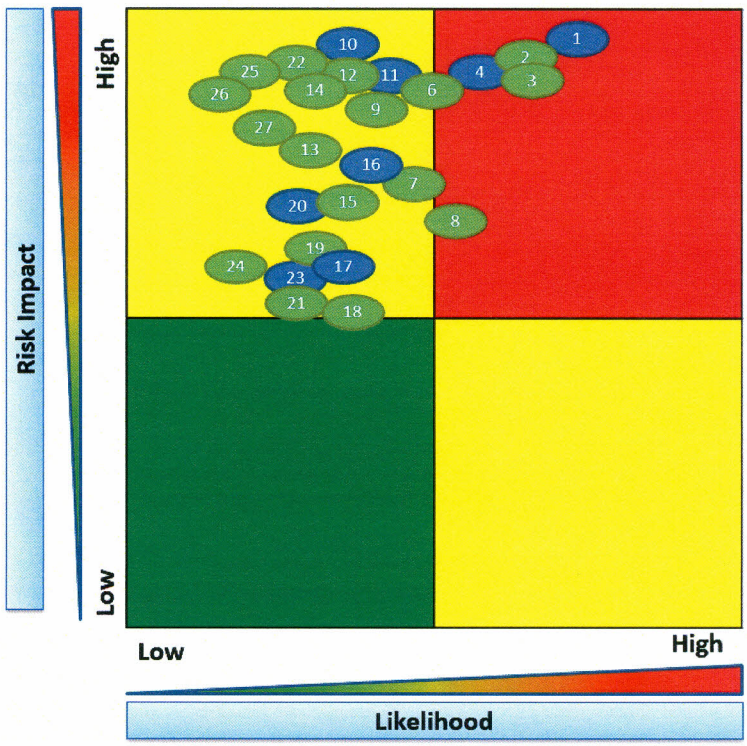

Figure 4 - Summary Risk Assessment Results – IT Risk Heat Map #1

	IT General Controls
28	Business Continuity
31	Data Center Security
39	Backup & Restore
40	Systems Development
50	Physical Security of IT Assets
53	Change Management

	IT Management
29	Security Event Management
30	Data Management
34	IT Asset Management & Procurement
36	Compliance Management
37	System Operations
42	In-House Software Development
43	IT Governance
44	IT Resources
45	Staffing/Recruiting
46	Large-Scale IT Project Management
49	Vendor Management
52	Software License Management
54	IT Support and Problem Management

	IT Infrastructure
32	Network Administration and Security
33	MS SQL Database Administration and Security
35	Cloud Computing
38	Remote Network Access
41	Windows Administration and Security
47	Enterprise Voice Network
48	Enterprise Data Network

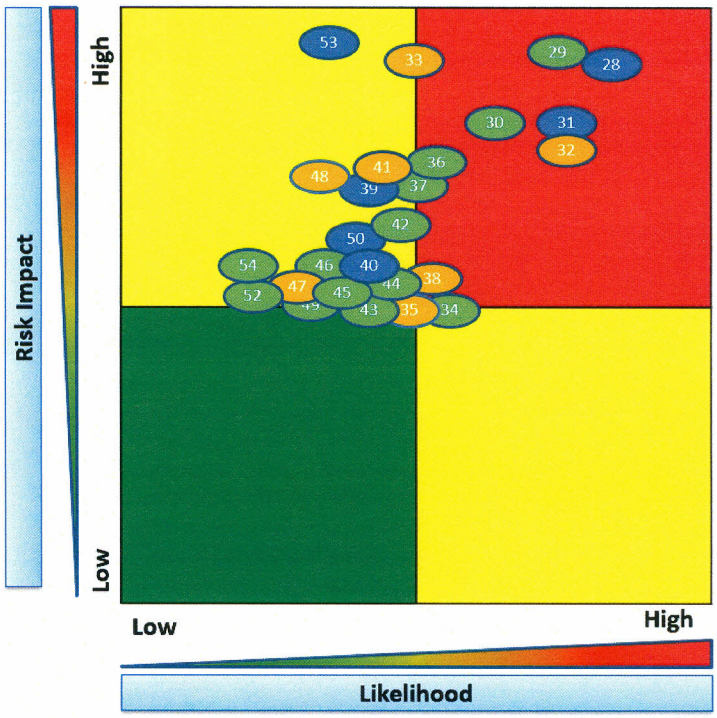

Figure 5 - Summary Risk Assessment Results – IT Risk Heat Map #2

3.0 FINAL IT AUDIT PLAN

The table below enumerates the IT audit universe items grouped into specific suggested audits based on the IT risk assessment results.

2015 IT Audit Plan				
Priority	**IT Audit**	**Hours**	**Start**	**Duration**
1	IT Entity Level Controls Review	120	Jan	6 - 8 weeks
2	PMO Review	120	Feb	6 - 8 weeks
3	Select PIR Audit (s)	180	Mar	9 months
4	Security / VAPT Assessment	360	Apr	8 - 12 weeks
5	ITGC Controls Review	200	Mar	8 - 12 weeks
6	Sensitive Data Review	360	Jul	3 months
7	Event Monitoring and Response Review	120	Aug	6 - 8 weeks
	IT Risk Assessment	120	Oct	4 – 6 weeks
	Planning, Monitoring and Reporting	240	Jan	12 months
	Total	**1,820**		

Table 9 – Final IT audit plan

Following are the detailed audit objective and the risks associated with each entity reviewed.

1. IT Entity Level Controls Review	
IT Audit Objective	**Risks**
The objective of this review is to assess the design and effectiveness of the IT organization's control environment.	Weak, inadequate, or nonexistent IT entity level controls, can lead to ineffective IT control activities which would increase the likelihood of an event that would have a negative impact to HISD or its students.

2. PMO Review	
IT Audit Objective	**Risks**
The objective for this review is to assess the design and effectiveness of the IT Program Management Office (PMO). Is IT focused on key projects that bring the most value to the business?	IT is working on non-key projects. IT doesn't have the ability or capacity to deliver on the key projects. Project objectives are not met. Budget overruns, timeline slippage, and over consumption of resource time is experienced.

3. Select PIR Audit (s)	
IT Audit Objective	**Risks**
The objective of a Pre-Implementation Review (PIR) audit is to focus on the project team's ability to deliver an implemented system that meets the business needs, on schedule and within budget.	A new system could be implemented that doesn't meet the business needs, comes in late and/or is over budget.

4. Security / VAPT Assessment	
IT Audit Objective	**Risks**
The objective of this assessment is to evaluate the design of the security environment, look for vulnerabilities in the network and understand the depth of the impact if the network is penetrated via a Vulnerability Assessment and Penetration Test (VAPT). How secure is the HISD network and its internal systems?	Unauthorized access to the network, systems and/or data that could have a negative impact on HISD or its students.

5. ITGC Controls Review	
IT Audit Objective	**Risks**
The objective of this review is to assess the design and effectiveness of the IT organization's controls activities.	Weak, inadequate, nonexistent or ineffective IT control activities would increase the likelihood of an event that would have a negative business impact.

6. Sensitive Data Review	
IT Audit Objective	**Risk**
The objective of this review is to assess the design of the controls around sensitive data within the HISD IT environment and its associated 3rd party providers or partners.	A lack of controls could potentially lead to data leakage, where sensitive data is disclosed to unauthorized personnel either by malicious intent or inadvertent mistake which could have a negative impact on HISD or its students.

7. Event Monitoring and Response Review	
IT Audit Objective	**Risk**
The objective of this review is to assess the design and effectiveness around the process for monitoring possible unauthorized access to the network, systems and/or data.	Unauthorized access to the network, systems and/or data that could have a negative impact on HISD or its students.

IT Risk Assessment	
Objective	**Risk**
Identify risks that IT presents to the organization that could adversely affect strategic goals. Identify the IT audit universe, examine the IT auditable units and select areas with the greatest risk exposure to review and include in the IT audit plan.	Unidentified or unaddressed IT risks could have a negatively impact HISD or its students.

Planning, Monitoring and Reporting	
Objective	**Risk**
An effective planning, monitoring and reporting mechanism ensures that the audits being performed address the audit objectives in an efficient and timely manner.	Failure to effectively plan, monitor and report on each engagement could result in budget over-runs and scope not being met.