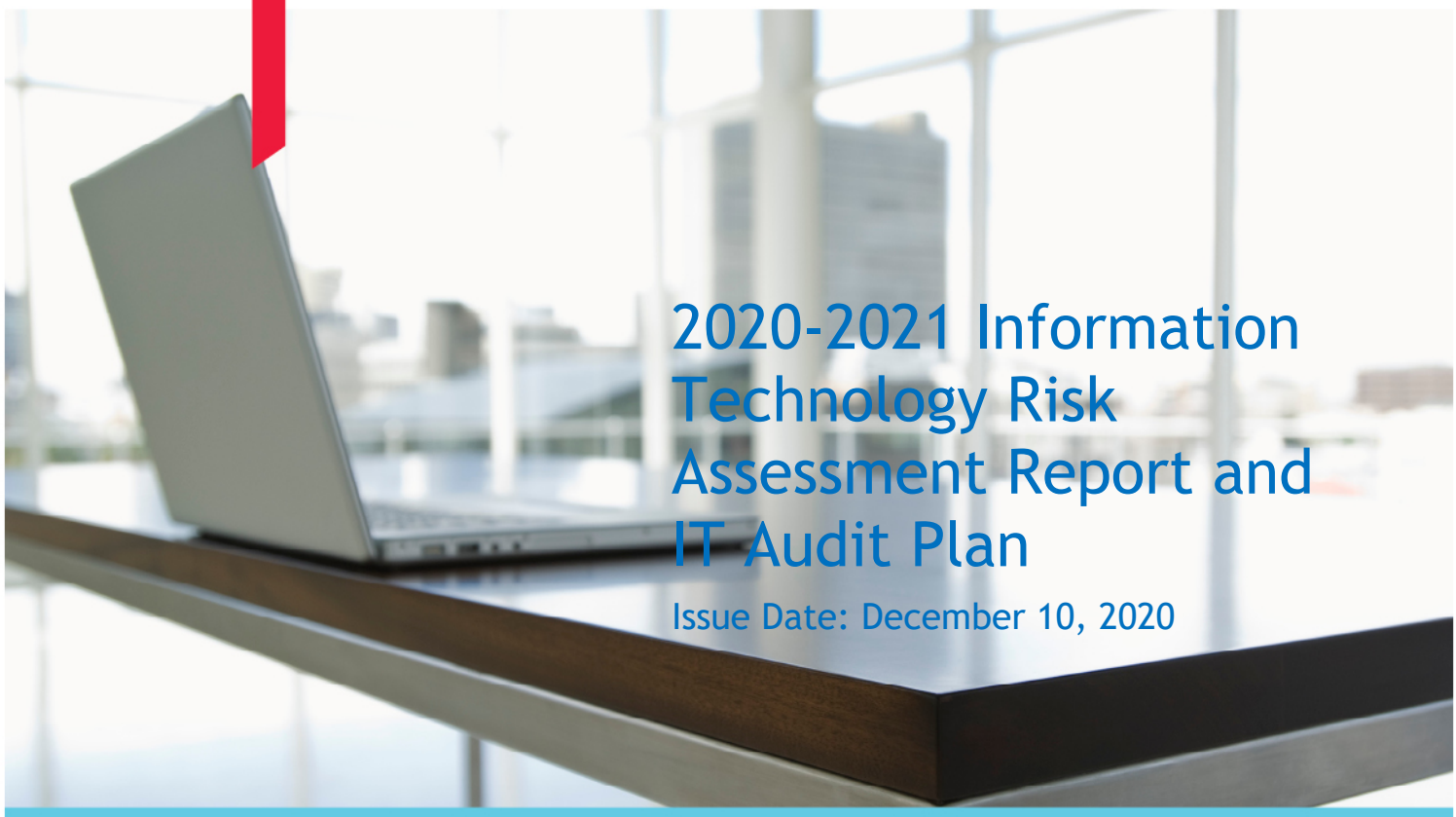


2020-2021 Information Technology Risk Assessment Report and IT Audit Plan

Issue Date: December 10, 2020

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY 3
1.1 INTRODUCTION 3
1.2 OUR APPROACH 3
1.3 KEY PARTICIPANTS 4
1.4 METHODOLOGY 5
2.0 SUMMARY RISK ASSESSMENT RESULTS 8
3.0 IT AUDIT PLAN 9

1.0 EXECUTIVE SUMMARY

1.1 INTRODUCTION

BDO USA, LLP (BDO) was engaged to conduct the Information Technology (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 for inclusion in the annual IT audit plan. The IT risk assessment evaluated IT related elements based on BDO's knowledge and understanding of the IT environment through interviews with key members of the IT department, input from the District's process owners, and input from HISD's Office of Internal Audit.

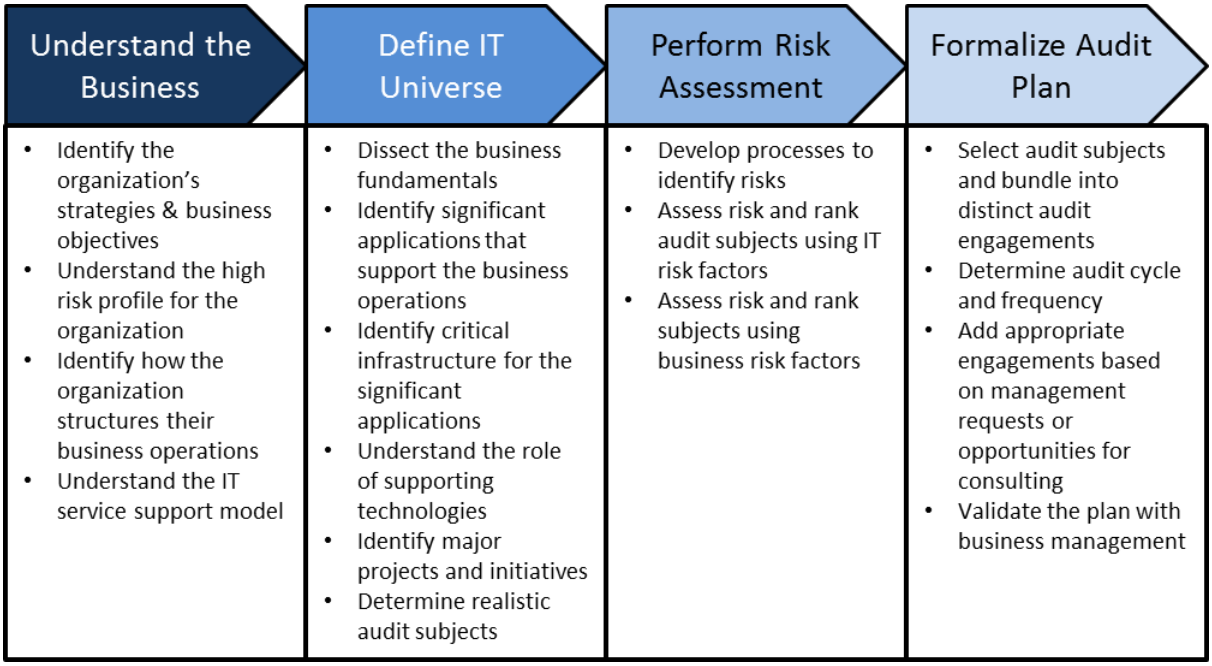
The purposes of this IT risk assessment are two-fold, including to:

- Identify the IT Audit Universe to identify auditable entities;
- Evaluate the auditable entity's risks and select areas with the greatest risk exposure to review and include in the IT audit plan.

1.2 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's (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 on the next page 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



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 HISD's IT 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 2020.

1.3 KEY PARTICIPANTS

The project team received valuable input from various HISD IT personnel to understand: the key strategic objectives planned for the coming year, how IT enables the District 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.

[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).

Table 1 – IT Risk Assessment Participant List

Person	Responsibilities
Scott Gilhousen	Chief Technology Officer
Patrick Porter	Director, IT Data and Business Solutions
Frank Williams	Director, IT Student Management Systems
Preeti Burns	Director, IT Customer Service
Tanya Pridgeon	Senior Manager, IT Administration and Strategic Planning
Brian Sailors	Senior Manager, IT System Engineering
Kevin Hodges	Manager, IT PowerUP
EJ Machicek	Senior Manager, IT Operations
Thomas Wright	Senior Manager, IT Network Engineering

1.4 METHODOLOGY

BDO's standard IT risk assessment approach follows best practices that were 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 is 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 that was 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

1.4.1 Understanding the District – An important perspective in performing the IT risk assessment is to understand that IT primarily 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 District objective. Therefore, it is important to first understand HISD's objectives, strategies, business model, and the role that technology has in supporting the District. This was accomplished by identifying the risks that were found in the technologies used and how each risk might prevent the organization from achieving the District's objectives.

1.4.2 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 interviews with key members of the District's management team.
- 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.

1.4.3 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 2 provides definitions for the risk levels for the likelihood of the risk occurring and Table 3 provides a definition of the impact of the risk. The IT risk assessment evaluated IT related elements based on their potential impact to the five following business areas:

- Strategy
- Financial
- Reputational
- Compliance
- Operational

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

- Availability
- Integrity
- Confidentiality
- Major Changes to the Entity
- Time Since Last Audit

Table 2 – Risk Likelihood Matrix

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 3 – Risk Impact Matrix

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

1.4.4 Develop IT Audit Plan – In order to arrive at a suggested IT audit plan, the IT audit universe items with a composite score of High or Medium 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.

2.0 SUMMARY RISK ASSESSMENT RESULTS

The IT audit universe was ranked using key 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. 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/Likelihood: The perceived inherent IT risk related to applications, infrastructure/architecture, IT processes and projects.

The following diagram illustrates the risk assessment results based on those two categories. The top 10 IT risks identified are shown below, in order of descending risk and priority.

Figure 2 - Summary Risk Assessment Results – Top 10 IT Risk Chart

The scores were calculated as described in section 1.4.3 of this report. The scale for the scores were from a low of zero (0), representing no risk, to a high of 60, representing the maximum risk exposure.

3.0 IT AUDIT PLAN

The table below shows the proposed 2020-2021 IT audit plan based on this IT risk assessment.

Table 4 – IT Audit Plan

2020-2021 IT Audit Plan				
IT Audit	**Hours**	**Start**	**Duration**	**End**
Close Out Previous Year Audits	170	Oct	Ongoing	Jan
Enterprise Risk Assessment	60	Nov	4-6 Weeks	Jan
Remote Network Access / COVID-19	300	Nov	8-10 Weeks	Feb
IT Governance / IT Strategic Planning – LBB Report Follow-up	80	Jan	2-3 Weeks	Feb
Prior Issue Follow-up Audit	200	Jan	4-6 Weeks	Mar
Security Event Monitoring and Incident Response (Vulnerability Assessment and Penetration Test)	275	Feb	8-10 Weeks	April
IT Asset Management / Software License Management	300	Mar	8-10 Weeks	May
OneSource (SAP)	325	April	9-11 Weeks	June
PowerSchool	315	May	10-12 Weeks	July
IT Risk Assessment/Update	75	Jun	2-3 Weeks	July
Total	**2,100**			

Note: The objectives for each proposed audit in the chart above are presented on the next page.

Audit	Objective
PowerSchool	To provide management with an assessment of the efficiency and effectiveness of the design and operation of internal controls associated with this newly implemented Student Information System.
IT Governance / IT Strategic Planning	To validate that the District has appropriate policies and procedures in place as it relates to the governance of key IT processes. BDO will review the LBB report from November 2019 to validate and follow up on the findings related to IT Governance.
Remote Network Access / COVID-19	To determine the adverse impacts of COVID-19 on the District's logical and remote access, and the effectiveness of the District's existing procedures already in place.
IT Asset Management / Software License Management	To evaluate the District's asset management processes for schools to ensure schools are following the correct procedures to purchase, report, inventory, and decommission their IT assets.
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, payroll, and other supported processes.
Security Event Monitoring and Incident Response (Vulnerability Assessment and Penetration Test)	To identify and exploit vulnerabilities that an attacker could use to gain unauthorized access to internal HISD systems or impact the integrity and availability of HISD systems and applications.
IT Risk Assessment/Update	To 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.