Data Governance Audit

Internal Audit Report

June 24, 2020

Orange County Public Schools
Internal Audit

Linda J. Lindsey, CPA, CGAP, Senior Director
Luis E. Aponte Santiago, CISA, IT Auditor

Table of Contents

EXECUTIVE SUMMARY

Why We Did This Audit

Our objective was to evaluate the District's' Data Governance Management as compared to industry's best practices.

Effective data governance is designed to ensure that an organization has the right data available at the right time and that the data is accurate and in the correct format required to satisfy specific business needs.

This audit was included in the 2019-2020 Annual Audit Plan.

Observations and Conclusion

Audit Results at a Glance			
	Risk / Impact Rating		
Results and Observations	**Significant**	**Moderate**	**Minor**
IA - Internal Audit or M - Management	–	IA – 1	
D - Deficiency or O - Opportunity	–	D – 1	

We evaluated data governance in four areas as listed below:
- Data Governance Policies
- Data Governance Strategy
- Unknown applications, devices, and networks
- Data Governance Feedback

Results and Recommendations

We evaluated Data Governance maturity level based on the IBM Maturity Model. The model identifies 11 domains of the data governance function and with scoring from 1 to 5 on each domain. The overall score was 2.36, with the domain that scored highest being *Information Security and Privacy* with a 4. The domains that scored lower were *Data Risk Management and Compliance*, *Value Creation*, and *Audit Information, Logging and Reporting* with scores of 1. A graphic with more details is in the report.

Based on the results of our audit, we made the following recommendation:
- Complete development of the Business Impact Analysis (BIA) and Risk Assessment (RA) to include an inventory of all mission critical systems, and assets of the District, as well as other significant information and add wording to the School Board Policy EHB Data and Records Retention to reflect how the District manages non-student electronic files and records.

This report has been discussed with management and they have prepared their response which follows.

DEFINITIONS:

Risk / Impact Ratings

Minor	Low risk with a financial impact of less than one percent and/or an isolated occurrence limited to local processes (low impact and low likelihood)
Moderate	Slight to moderate risk with a financial impact between one and five percent and/or a noticeable issue that may extend beyond local processes (low impact and high likelihood or high impact and low likelihood)
Significant	High risk with a financial impact greater than five percent and/or a significant issue that occurs in multiple processes (high impact and high likelihood)

Observations Categories

Deficiency	A shortcoming in controls or processes that reduces the likelihood of achieving goals related to operations, reporting and compliance
Opportunity	A process that falls short of best practices or does not result in optimal productivity or use of resources

Criteria for Observations Sourced to Management

- Internal audit was informed of the issue prior to starting detailed testing
- Management identified, evaluated, and communicated the issue to appropriate levels of the district
- Management has begun corrective action with clear, actionable plans and targeted completion dates

None of the observations resulting from this audit were sourced to management.

BACKGROUND:

Data governance is a wide set of management and technical disciplines designed to ensure that an organization has the right data available at the right time and that the data is accurate and in the correct format required to satisfy specific business needs.

OBJECTIVES, SCOPE AND METHODOLOGY:

Objective
Evaluate the District's Data Governance Management as compared to best practices to determine the maturity level on the subject.

Scope
Assess the District's current Data Governance stance.

Methodology

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* of the Institute of Internal Auditors and included such procedures as deemed necessary to provide reasonable assurance regarding the audit objective. Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

We are required to note any material deficiencies in accordance with Florida Statutes, School Board Policy and sound business practices. We also offer suggestions to improve controls or operational efficiency and effectiveness.

Due to the COVID-19 pandemic and the changing work environment during this period, the ITS department's priority was to take care of staff and students. Because of this, our audit approach used four questionnaires covering the risks addressed by this audit as listed below.

Our scope was to assess the District's current data governance state.

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

Due to COVID-19 pandemic we used an audit approach involving questionnaires to cover the risks addressed by this audit.

1) Data Governance Policies
2) Data Governance Strategy
3) Unknown applications, devices and networks
4) Data Governance Feedback

We also interviewed personnel from the ITS Department and the District's Records Office.

AUDIT RESULTS & RECOMMENDATIONS:

Data maturity models help organizations understand their data capabilities, identify vulnerabilities, and know in which particular areas, employees need to be trained for improvement. They also help organizations compare their progress among their peers. As part of this audit, we assessed the district's maturity across 11 domains (functions) of data governance using a five level scale. Our evaluation was based on an IBM Data Governance Maturity Model.
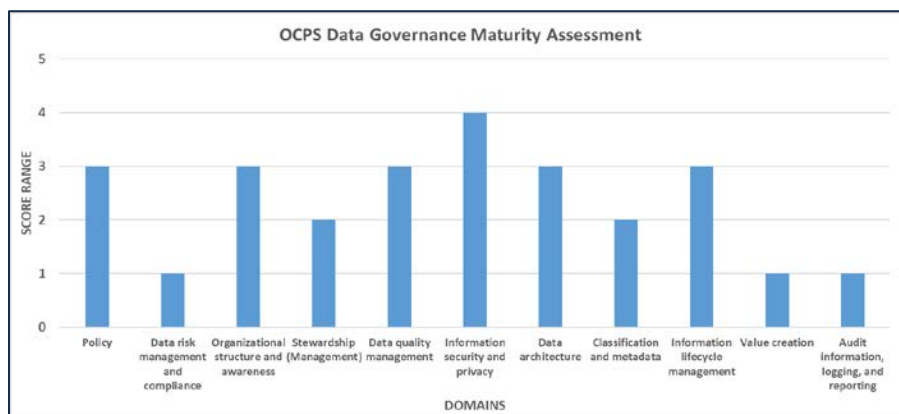
Definitions of Domains:

- <u>Policy</u> – a description of the desired organizational behavior(s)
- <u>Data risk management and compliance</u> – the methodology by which risks are identified, qualified, and quantified, avoided, accepted, mitigated or transferred
- <u>Organizational structure and awareness</u> – description of the level of mutual responsibility between the organization and IT, and the recognition of the fiduciary responsibility to govern data at different levels of management
- <u>Stewardship (Management)</u> – a quality control discipline designed to ensure custodial care of data for asset enhancement, risk management, and organizational control

Data maturity models help organizations understand various technological aspects and also helps them compare their progress among their peers.

We used the IBM Data Governance Maturity Model.

We assessed 11 domains of data governance.

- <u>Data quality management</u> – methods to measure, improve and certify the quality and integrity of production, test, and archival data
- <u>Information security and privacy</u> – the policies, practices and controls used by the organization to mitigate risk and protect data assets
- <u>Data architecture</u> – the architectural design of structured and unstructured data systems and applications that enables data availability and distribution to appropriate users
- <u>Classification and metadata</u> – the methods and tools used to create common definitions for business and IT terms, data models, data types, and repositories (Metadata that bridge human and computer understanding)
- <u>Information lifecycle management</u> – a systematic policy-based approach to information collection, use, retention, and deletion
- <u>Value creation</u> – the process by which data assets are qualified and quantified to enable the business to maximize the value created by data assets
- <u>Audit information, logging, and reporting</u> – the organizational processes for monitoring and measuring the data value, risks, and efficacy of governance

Definitions of Levels of Maturity[1]:

- <u>Level 1: Initial</u> – there is little to no awareness of the importance of data and there are no set standards for managing data
- <u>Level 2: Managed</u> – the importance of data in the organization is realized
- <u>Level 3: Defined</u> – data regulation and management guidelines are defined better and are integrated with the organization's processes
- <u>Level 4: Quantitatively Managed</u> – measurable quality goals are set for each project, data process, and maintenance
- <u>Level 5: Optimizing</u> – data governance becomes an enterprise-wide effort that improves productivity and efficacy

The scores for each domain are as follows:

Domain	Score
Policy	*3*
Data Risk Management & Compliance	*1*
Organizational Structure & Awareness	*3*
Stewardship (Management)	*2*
Data Quality Management	*3*
Information Security & Privacy	*4*
Data Architecture	*3*
Classification & Metadata	*2*
Information Lifecycle Management	*3*
Value Creation	*1*
Audit Information, Logging & Reporting	*1*

---

[1] Our evaluation of each domain's maturity level was based on this 1 to 5 scale, according to the ITS Department's responses to our audit inquiries.

1) The Business Impact Analysis (BIA) and Risk Assessment (RA) are not yet complete and School Board Policy EHB - Data and Records Retention – does not reflect how the District manages non-student electronic files and records. *Moderate risk*

Best Practice:
Having an up-to-date BIA helps organizations arrange their information and data sets according to criticality and business needs. Also, an organization's data and records retention policy should address how electronic files and electronic records are being managed, handled, and disposed.

Audit Result:
According to the ITS Senior Director of Information Security, they have classified data according to National Institute of Standards and Technology (NIST) and the Federal Information Processing Standards (FIPS), but that data is not addressed in a BIA because it hasn't yet been developed. It is important for the ITS department to have a BIA to provide a much clearer and prioritized view of what information is critical to the District.

As a result, they haven't produced a report after the inventory is completed. Instead, they plan to conduct a RA and the BIA by the end of 2020 to reflect not only an inventory count of mission critical systems and assets, but the data each of these hosts manages, stores, or transmits. In addition, School Board Policy EHB should include a statement[2] that says which Florida statute or law the District uses to manage, handle and dispose of non-student electronic files and records.

Recommendation:
Complete development of a BIA to include all data that is critical and add a statement on the School Board Policy EHB indicating which Florida statute or law the District follows to manage, handle and dispose of non-student electronic files and records.

By completing the Business Impact Analysis, along with the Risk Assessment, the ITS Department will have a much clearer view of what information is critical to the District and will have an inventory count of mission critical systems and assets, and the data each of these hosts, manages, stores, or transmits.

School Board policy should address electronic records.

---

[2] Mention the statute for reference only (a link to the statute can be added too).

Department / School Name	Information Technology Services
Administrator / Department Head	Russell Holmes
Cabinet Official / Area Superintendent	Robert Curran

Audit Result / Recommendation	Management Response Acknowledgement/ Agreement of Condition	Responsible Person (Name & Title) And Target Completion Date (MM/YYYY)	Management's Action Plan
Complete development of the Business Impact Analysis (BIA) and Risk Assessment (RA) to include an inventory of all mission critical systems, and assets of the District, as well as other significant information and add wording to the School Board Policy EHB Data and Records Retention to reflect how the District manages non-student electronic files and records.	ITS agrees that a Risk Assessment and Business Impact Analysis should be completed and finding reported and documented.	Russell Holmes, Sr. Director of Information Security (08/2021)	A Risk Assessment was planned for in 2019 and kicked off/initiated in July of 2020. Once the Risk Assessment is completed, the Business Impact Analysis will be conducted on the results as well as recommended procedures/security controls to reduce the Districts risk profile.