

Office of Inspector General
Information Technology Governance

Report #C-1415-010

August 2016

Executive Summary

In response to a request by Department of Education (department) management, the Office of Inspector General (OIG) conducted a consulting engagement of the department's information technology (IT) governance program. The purpose of this engagement was to review the department's IT governance program and make recommendations for improvement. During the review, we noted that the department should continue to strengthen its IT governance plan. For example, the department should ensure that policies are cohesive and are subject to a unified framework.

Scope, Objectives, and Methodology

The objective of the engagement was to review the department's processes and procedures to determine if the department has adequate IT governance policies. The scope of the engagement included policies, procedures, and processes in place through the end of engagement fieldwork. To accomplish our objectives we reviewed applicable laws, rules and regulations; interviewed appropriate department staff; reviewed policies and procedures; and reviewed standards and best practices.

Background

IT governance is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.¹ The purpose of IT governance is to align IT strategy with department strategy and ensure that the department is successfully implementing its strategies and achieving its goals.²

The OIG conducted a department *IT Application Development and Procurement Audit* in 2011. The audit noted that the department did not follow a documented project management methodology and the overall effectiveness of project governance needed to improve. The OIG conducted a follow up on the corrective actions resulting from the audit for 34 months. After 34 months, three deficiencies identified in the original report had not been resolved through corrective action. In consultation with department management, the OIG closed out the former audit and initiated a consulting engagement to assist the department in implementing and enhancing its governance processes.

¹ <http://www.gartner.com/it-glossary/it-governance/>

² <http://www.cio.com/article/2438931/governance/it-governance-definition-and-solutions.html>

During the consulting engagement, the Division of Accountability, Research and Measurement (ARM), hired an outside consulting firm to help the department develop and implement a data governance process. The department is currently implementing the recommendations for establishing the data governance procedures. Once data governance is established, implementation of IT project governance will follow.

With the implementation of data governance in the final stages, the primary focus of this engagement was to assist the department with the development of project governance. The department requested that the OIG assist them by ensuring they complied with their project governance implementation schedule. The department originally intended to complete all tasks on the schedule in six months, however; due to delays and workload issues, many of those tasks were not completed as scheduled. The department did develop data and project governance policies. During this engagement, we met with the department on several occasions, provided feedback, and made recommendations on presented documentation.

Current Conditions

During our review of the department's project governance policy, (03-02-02) we determined the policy addresses many principles outlined by COBIT 5 such as responsibility, strategy, acquisition, performance, and conformance. The department adequately addresses many of these areas.

Steering Committee

Project governance allows the department to align projects with organizational objectives to ensure they support the fulfillment of overall educational goals and achieve intended outcomes. Effective project governance ensures projects yield the expected benefits. The department has developed a working draft of its project governance plan. According to the governance plan, the project governance structure includes:

- Governance Steering Committee (GSC)
- Governance Internal Support Subcommittee
- Application (Supporting Subcommittee as required)
- Security (Supporting Subcommittee as required)
- Business Operations (Supporting Subcommittee as required)

The project governance plan states that there will be one GSC, one governance internal subcommittee, and several supporting subcommittees as needed. The GSC will be the department's centralized decision-making body, comprised of executive level decision makers responsible for reviewing, approving, and monitoring projects that fit the organization's ongoing needs; influences the progress of all projects; and ensures the optimal balance of current projects. The GSC will have overall responsibility for governance of project management, and the department's chief of staff will chair the governance steering committee.

Currently, the department has not identified project governance steering committee members, however; a data governance council has begun holding meetings. This council currently meets

monthly. In order to provide guidance and make recommendations, representatives from the OIG have attended and participated in the council meetings.

Strategic Planning

The department's project governance plan addresses strategic planning. According to the plan, the department's project governance will be a continuous process of tracking and prioritizing the optimum set of project-oriented initiatives to deliver maximum value to the department. In the decision making process, department senior leaders can efficiently use resources to focus on projects that are achievable and strategically aligned with organizational goals. The department's GSC will be responsible for strategic planning. GSC duties will include analyzing and ranking project proposals; making decisions on department project proposals; providing overall project guidance and direction; authorizing project funding; approving contract negotiations; approving major change requests; and monitoring overall project status and strategic alignment. The plan also states that the GSC will be the final decision making body.

Performance

According to COBIT 5, a performance measurement process is required to ensure the department monitors performance consistently and reliably. The department should have clear definition of performance goals and effective metrics to monitor the achievement of goals. Performance measurements will allow the department to determine if projects are successfully achieving the department's objectives and identify areas for improvement. Two critical governance success factors are the approval of goals by stakeholders and the acceptance of accountability for achievement of goals by directors and managers.

During our review, we determined the department's governance plan does not address performance measures. However, the data governance policy states the data governance council will define a set of metrics and key performance indicators to measure the effectiveness of data management activities. The policy does not define the performance indicators. According to department staff, performance measures have not been developed.

Future Projects

The department plans to develop and start implementation of project governance at the completion of data governance. The department also plans to merge project and data governance into a unified governance structure and implement a device standard, password policy, and data suppression policy. A draft of the department's password policy is currently awaiting approval.

Recommendations

The department has made great strides in developing and implementing data governance. The department has created working draft policies for both data and project governance. We recommend that the department formalize these policies while continuing to strengthen them. Formalized policies and procedures will allow efficient and productive governance. We also

recommend that the department merge the data governance and project governance processes to increase efficiency and avoid duplication of efforts. Additionally, top down support for the data and project governance processes is critical to the ongoing success of those processes.

As processes mature, we recommend the department create performance measures. Performance measures will enable management and other stakeholders to determine if IT is meeting its objectives. The department should ensure that the ownership and accountability for achieving targets are clear. Once ownership and accountability are established, the department will be able to decide which measurements are important. For example, stakeholders may want to measure business and IT alignment, whereas IT may want to measure database validation consistency.

The department plans to develop and implement project governance after the implementation of data governance. To assist in activating an effective project governance program, we recommend that the department develop implementation procedures. The procedures should establish clear goals and objectives in order to align efforts. ISACA suggests that the procedures consist of activities to get started, followed by key implementation tasks with suggested roles and responsibilities. The procedures should also indicate relative scheduling for implementing the project.

We recommend the department use a framework such as COBIT 5 to assist in developing project governance and for the continued improvement of data governance. COBIT 5 integrates different widely accepted standards such as Information Technology Infrastructure Library and the International Organization for Standardization. The COBIT framework incorporates different subsets of information management and control in which the department may find value. COBIT provides guidance in areas such as information security, regulatory compliance, risk management, and governance of enterprise IT.

Department staff indicated that IT standards would become a focus. The department plans to implement a device standard, password policy, and data suppression policy. To assist with the development of device standards, the National Institute of Standards and Technology has (NIST) issued the following publications:

- NIST 800-164 (draft) offers insight on the security risk associated with the use of mobile devices .The publication also introduces baseline security technologies that can be implemented across a wide range of mobile devices to help secure both department issued and personally owned devices, and
- NIST 800-122 offers a guide for protecting personally identifiable information.

The National Center for Education Statistics also released a publication, *SLDS Technical Brief Guidance for Statewide Longitudinal Data Systems*, which provides best practices for the data stewardship of educational records.

Closing Comments

The Office of the Inspector General would like to recognize and acknowledge the Division of Technology and Innovation and the Division of Accountability, Research and Measurement and staff for their time and assistance during the course of this review. Our review was facilitated by the cooperation and assistance extended by all staff involved.

To promote accountability, integrity, and efficiency in state government, the OIG completes audits and reviews of department programs, activities, and functions. Our audit was conducted under the authority of section 20.055, F.S., and in accordance with the International Standards for the Professional Practice of Internal Auditing, published by the Institute of Internal Auditors, and Principles and Standards for Offices of Inspector General, published by the Association of Inspectors General. The audit was conducted by Jeremy Anderson and supervised by Janet Snyder, CIA, CGAP, Audit Director.

Please address inquiries regarding this report to the OIG's Audit Director by telephone at 850-245-0403. Copies of final reports may be viewed and downloaded via the internet at <http://www.fldoe.org/ig/auditreports.asp#F>. Copies may also be requested by telephone at 850-245-0403, by fax at 850-245-9419, and in person or by mail at the Department of Education, Office of the Inspector General, 325 West Gaines Street, Suite 1201, Tallahassee, FL 32399.