FLORIDA DEPARTMENT OF EDUCATION

Office of Inspector General

January 2012 Report No. A-10/11-14

Information Technology Application Development and Procurement

Overview

An evaluation of management techniques for designing, building, and maintaining custom information technology (IT) software applications was the initial focus of this audit. We intended to assess whether management controls such as project planning, project management, and change management processes were followed.

Finding negligible approved policies and procedures in place, we utilized other criteria in our assessment. We decided to focus our efforts more broadly on general project management practices (which include tasks related to information technology application development). Most of these practices were still under development from a governance perspective. Department staff agreed that enterprise-wide governance is early in its maturity. They indicated their awareness of the steps needed to be taken and their intent to incrementally build more structure into the process.

We found the Department can improve activities to more effectively oversee practices involving resource investment, use and allocation. Adoption and use of a formal methodology of organizing and accomplishing project tasks can mitigate inherent risks to better ensure project success.

This report identifies opportunities for improvements in strengthening management controls in administering both the IT application development function as well as overarching governance for Department projects.

We recommend the Department:

- Develop formal written policies and procedures for administering the enterprise-wide project management function, as well as IT application development, and have them adopted for use by the Department;
- Increase its efforts to further develop, strengthen, and formalize its governance structure and activities;
- Develop a formal documented project management methodology for managing projects;
- Ensure that application support projects are performed in accordance with requirements of the Department's ISDM; and
- Ensure that segregation of duties is strengthened with regards to data security administration.

Background

This audit was identified in the Office of Inspector General's (OIG) annual risk assessment and included in the approved annual audit plan. It was performed in support of the Department's goal of quality efficient services with the purpose of promoting the strategic imperative of aligning resources with performance.

The Department's Office of Technology and Information Systems, headed by the Chief Information Officer (CIO), is responsible for Technology Planning and Management; Educational Technology; Data Center Operations; Applications Development and Support; and End User Support.

Staff in the *Technology Planning and Management Section* are involved in implementation of enterprise-wide governance activities that help ensure decisions and resource allocations related to new projects undertaken by the Department are made in support of the Department's strategic plan. Workgroups and an oversight governing committee are being developed to address the needs of prioritizing the many project ideas and plans under consideration for acceptance, improving project management practices, and focusing on critical project issues and risks.

The Department's project management office is placing emphasis on processes to control the approval of new projects and programs, many of which involve IT components (hardware and software elements). These practices are intended to ensure decisions on resource investment, use, and allocation align with and support the Department's strategic plan.

The *Applications Development and Support Section* responds to service requests for existing software programs which could range from minor fixes to major enhancements and new system developments. Applications development staff are required to follow the Department's Information System Development Methodology (ISDM) which outlines a common framework of lifecycle phases that may include planning, analysis, design, development, testing, implementation, and maintenance.

Results of Previous Assessment

We identified a technical assistance report prepared by the Center for Educational Leadership and Technology (CELT), an information technology architect and systems integrator for educational entities. The firm performed a review that included an assessment of the Department's overall IT structure and governance processes.

The CELT final report, issued in June 2011, indicates that Department leadership has strongly embraced project management as an essential mechanism for overseeing the implementation of Department grants. They reported areas of continued focus which included recommendations that the Department:

- Support the move toward agency-wide implementation of project management;
- Develop an agency-wide data governance structure and process; and
- Implement an IT governance process to continuously monitor and improve IT organizational alignment, resource allocation, efficiency and responsiveness to internal and external stakeholder needs.

The results of this assessment parallel the first three findings and recommendations included in this audit report.

Findings and Recommendations

1. Formal written policies and procedures are needed.

Department policies and procedures related to information technology (IT) application development as well as enterprise-wide project management are limited. Documents were limited to a draft development methodology, a document regarding minimal security standards for software development, a brief document on technical standards, and draft flowcharts on proposed governance processes.

Written policies and procedures are used to communicate and control the activities and processes to achieve established goals and objectives. They should be comprehensive, current, and effectively communicated to the responsible staff.

A review of two Florida state agencies found extensive guidance related to IT application development and governance structure. Published documents addressed such areas as application development and requirements, information technology acquisition, data policies, testing standards, information security, and project management.

In the absence of policies and procedures, Department staff have relied on instructions provided from other sources (e.g., knowledgeable staff members, industry practices, etc.).

Without written policies and procedures, administration of the enterprise-wide project management process as well as IT application development may not be consistent and accountability may be difficult to maintain. Established policies and procedures are a crucial internal control; their absence can decrease the probability that management's directives will be followed and objectives achieved.

Recommendation:

The Department should develop formal written policies and procedures for administering the enterprise-wide project management function, as well as IT application development and have them approved by executive management. Approved policies and procedures should be implemented and staff trained on their application. Once established, written policies and procedures should be reviewed at least annually and updated as necessary. Policies and procedures should cover the areas listed below in addition to other areas as determined necessary.

Project Management

- Project governance (including oversight committee charters)
- Project management methodology

Application Development and Support

- Approved Information Systems Development Methodology
- Securing software applications
- Change management

Management Response:

Project Management

The establishment of a Project Management system was initiated in large part as a mechanism for implementing the challenging reforms required by two very large federal grants: Race to the Top and the Partnership for Assessment of Readiness for College and Careers. The timelines for both of these grants required the Department to very quickly put into place processes and procedures for managing an extensive number of complex projects. Under the leadership of the Commissioner Smith, the Project Management function was established as a way of work for the Department. Shortly thereafter, the Department went through a transition period under the leadership of an Interim Commissioner, and on July 31, 2011, Commissioner Robinson was appointed Commissioner by the State Board of Education.

Throughout this period, the Project Management Oversight Committee (PMOC) has continued to evolve. Policies, procedures, and methodologies have been developed and are being used to guide the ongoing implementation, while continuing to be refined to reflect the changes in Department leadership as well as the differing types and stages of the identified projects. The written documents, including for example, the charter template, are being revised and refined concurrently to reflect the direction of the PMOC. The anticipated completion date for finalizing policies and procedures for the areas listed in the audit report is June 30, 2012.

It is anticipated that this Project Management function, like those of other agencies, will continue to mature and thus the policies, procedures, and methodologies will likewise need to be continuously examined and enhanced. While the PMOC will formally adopt these written documents related to management and governance, it will be necessary to make periodic revisions to ensure that these enhancements are communicated effectively. Training of personnel has been ongoing throughout the process of establishing the system and will continue to be provided as new information is available or as additional staff become involved in the process.

Application Development and Support

The Information Systems Development Methodology has been developed and implemented for almost a year. Although the ISDM has not yet been formally adopted, it is in use and is guiding the development methodology used by the Department. A written procedure related to the security of software applications has been developed and added as an Addendum to the ISDM. A change management system, the Service Request System, has also been established. The ISDM will be examined to determine whether any revisions are necessary prior to presenting it for formal adoption (anticipated completion date of June 30, 2012). All of these are documents are written and are being used by relevant staff. Training for affected staff will be provided as needed (when changes are made or when additional staff need to use these policies, procedures, and methodologies).

2. Effectiveness of project governance should continue to be improved.

Governance processes were under development during the audit. For example, responsibilities of a project oversight committee were still being formulated. Governance can be established by finalizing a governing oversight committee, developing policies and procedures, defining job roles, executing good human resource practices, and performing risk assessments.

A project management function is in place at the Department to establish enterprise-wide project governance. It facilitates activities of a governing body, the Project Management Oversight Committee (PMOC). Comprised of Department senior managers (including the CIO), the PMOC considers concept papers, feasibility studies and business cases for new project ideas or solutions and monitors progress on certain significant projects approved for delivery.

Neither of these function's roles and responsibilities had been formally defined and documented. Staff of the project management function were drafting a policy and procedures document along with charter documents. At the time of the audit, Department staff members were working to re-establish the PMOC's structure and processes to include a meeting schedule and a focus of addressing critical project issues and risks, while also providing a forum for program and project managers and executive leadership.

This lack of formalized governance may have resulted from project managers being wary of activities that could slow down a project, especially during a time when the Department is operating under pressure to implement new projects and keep ongoing projects on track.

Not having a clearly defined process gives clear warning that practices involving resource investment, use, and allocation may not align with and support the Department's strategic plan. Potential impacts of not having an effective steering committee in place may include, for example, reduced uniformity in managing and reporting on project activities, reactive rather than proactive decision making on projects, disparities in the project selection and approval process, and inconsistencies in project monitoring and oversight practices.

Recommendation:

As project governance is critical to support the management of limited resources, the Department should continue on the path to further develop, strengthen, and formalize its governance structure and activities. This includes creating governance committee charters and policies to implement governance activities and empowering a strategy or steering committee to ensure adequate control over project decisions, directions, and performance to ensure project activities support the Department's strategic plan.

Management Response:

See response to Finding 1.

3. The Department is not following a formal documented project management methodology.

We found that important planning steps and related deliverables of selected ongoing projects were not evidenced. These include:

- Concept paper, feasibility study or business case;
- Documentation of project approval at the Division level and by the PMOC;
- Spending plan documentation;
- Project level communications plan; and
- Project charter documents were written at a high level, incomplete and not approved (signed) by project sponsors and project team members.

A project management methodology should establish a documented process which guides project activities. The typical process begins when the idea for a new project is first conceived. The methodology would give the project team a road map to help ensure all needed components are addressed.

One goal of the methodology would be to improve the quality and efficiency of projects undertaken. The methodology can evolve as the needs of the Department change and as improved methods, techniques, standards and technology become available.

The Department has not established a formal project management methodology, possibly because project managers are wary of activities that could slow down projects.

Not having in place a formal means of organizing and accomplishing project tasks while documenting approvals could lead to inadequate project management, scope variations, time and cost over-runs, and performance criteria not being met.

Establishing formal project approval steps, for example, will better ensure that evaluations such as project feasibility studies and concept papers are prepared up front before projects are initiated.

Recommendation:

The Department should develop a formal project management methodology for managing projects. A one-size-fits-all methodology is not likely to work given the different types of projects and management styles involved.

The methodology would likely include templates that can guide project teams in obtaining an appropriate level of documentation, while streamlining preparation time and effort involved.

Management Response:

See response to Finding 1.

4. Documentation of ISDM deliverable activities for application support projects should be improved.

Based on a review of selected application support projects, we found that documentation of ISDM deliverable activities should be improved. Incomplete or insufficient documentation was noted for the following areas:

- Risk analysis
- System architecture
- Business requirements definition
- Data requirements
- Programming specifications
- Security plan and design
- Compliance with Americans with Disabilities Act
- System test plan and results
- User acceptance test plan

The Department's ISDM provides a standard set of tasks and products to be used in application systems development. It outlines a common framework of lifecycle phases, and provides instructions to staff on completion of required deliverables that evidence execution of steps that will help ensure all needed components are addressed.

The ISDM addresses required documents and formats and defines staff roles and responsibilities with respect to the development process. ISDM steps are applied based on project size and complexity.

In several instances, it was indicated that required ISDM analyses had been performed, though not formally documented, due to the lack of staffing. One project reviewed had begun before the adoption of the ISDM (June 2010), thus some of the requirements were not completed.

If steps in the ISDM are not sufficiently documented, evidence of their performance becomes questionable. Failing to perform required steps in the methodology could lead to inadequate project management, scope variations, time and cost over-runs, and performance criteria not being met.

Recommendation:

The Department should ensure that application support projects be performed in accordance with requirements of the Department's ISDM. Staff performing deliverable tasks should be sufficiently trained on use of the development methodology and effectively supervised to ensure quality. Opportunities to streamline the documentation of ISDM deliverables could potentially be achieved by expanding the use of templates.

Management Response:

As noted above, the ISDM is being implemented throughout the Department; however, there are varying levels of implementation among staff based on the type of system being worked on. The Office of Application Development and Support (OAS) will continue to supervise and monitor the levels of implementation of the ISDM, specifically the documentation of ISDM deliverables. Additional training will be provided as needed and as indicated by the results of internal monitoring. Training will include guidance and best practices related to the use of templates for documentation of deliverables. OAS will also update the ISDM to address deliverable activities documentation in the areas mentioned in the report (risk analysis, system architecture, business requirements definition, data requirements, programming specifications, security plan and design, compliance with Americans with Disability Act, system test plan and results, and user acceptance test plan).

5. Segregation of duties should be strengthened.

Certain programmer employees in the Department's internal applications support section are allowed to implement development tasks (coded software) into the production environment. This lack of separation results in a potentially significant control weakness.

Strict control of software and data changes requires that programmers not be allowed to move software into production. Typically, a software change manager implements changes into production, after testing for readiness. For appropriate segregation of duties, programmers should not be able to execute any jobs in a production mode, perform database administration functions, perform application security functions, or have access to production databases.

Department staff agreed that this situation represents a control weakness, but indicated limited staff resources have led to certain senior level programmers performing dual (conflicting) roles.

Not establishing appropriate segregation of duties among IT functions increases the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented and not be detected, and that computer resources could be damaged.

Recommendation:

Existing security administration and application programming functions should be reviewed. Effective segregation of duties should be implemented where practicable. Programmers should not have access to the production environment. Where an appropriate segregation of duties is not possible, careful monitoring of the activities of affected individuals should be performed. The approach to separation of duties should be defined in the Department's security policies.

Management Response:

The Department has made every effort to segregate duties; however, in a small number of instances, select senior staff have been given the authority to perform functions in multiple areas. OAS carefully monitors updates to code and databases to ensure the integrity of the data and to prevent any breach of security. As noted earlier, the Department has established the Services Request system process and the change management process, specifically with respect to moving code into production. Use of this system by all staff, and most specifically the staff who perform functions in multiple areas, will ensure that any programmer is not the same person who updates the production environment.

These enhancements to the existing procedures, along with constant internal monitoring, will strengthen the segregation of duties to compensate for the need for staff to handle multiple functions in certain situations. These procedures will also be updated in the Department's security policies as needed.

Objectives and Scope

The objectives of this audit were to: 1) identify current practices regarding IT application development and procurement; 2) measure compliance with applicable guidance, and 3) consider best practices used by other agencies.

The scope of the audit included activity during the period July 1, 2010, to November 30, 2011.

Methodology

This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors. To achieve audit objectives, the audit team:

- Researched and reviewed applicable statutes, rules, manuals, procedures, related reports, and supporting documentation;
- Interviewed appropriate staff;
- Reviewed documentation for selected ongoing projects and for completed support projects;
- Reviewed procurement documentation where appropriate; and

- Evaluated internal controls

Closing Comments

The OIG would like to recognize and acknowledge the Office of Technology and Information Systems management and staff for their assistance during the course of this audit. Our fieldwork was facilitated by the cooperation and assistance provided by all personnel involved.