FLORIDA DEPARTMENT OF EDUCATION
fldoe.org

Office of Inspector General
Applications Development

Report #A-1516-024 **August 2017**

Executive Summary

In accordance with the Department of Education's fiscal year (FY) 2015-16 audit plan, the Office of Inspector General (OIG) conducted an audit of the Office of Application Development and Support (OADS) within the Division of Technology and Innovation. This audit reviewed the applications development and support policies, procedures, and methodologies to ensure that information technology (IT) development projects are planned, approved, and executed consistently in accordance with applicable laws and rules.

During this audit, we noted that the department has developed a draft IT governance plan but has not formally adopted the plan or implemented a governance framework; the department has not developed agency wide application development policies; the department did not follow the project management security standard; and the department's application development cost estimation process resulted in unreliable cost estimates. The Audit Results section below provides details of the instances noted during our audit.

Scope, Objectives, and Methodology

The scope of this audit included the period of July 1, 2014, through the end of fieldwork. We established the following objectives for our audit:

1. Determine if the department's Information Systems Development Methodology (ISDM) aligns with national standards;
2. Determine if the ISDM is being followed during the systems development cycle;
3. Determine if proper change management processes are being followed;
4. Ensure proper application security practices are being implemented; and
5. Determine if criteria exist to ensure efficient estimation and use of department resources during system development.

To accomplish our objectives we reviewed applicable laws, rules, and regulations; interviewed appropriate department staff; reviewed the department's ISDM and supporting documents; reviewed policies and procedures; reviewed cost estimates; and reviewed a sample of developed applications.

Background

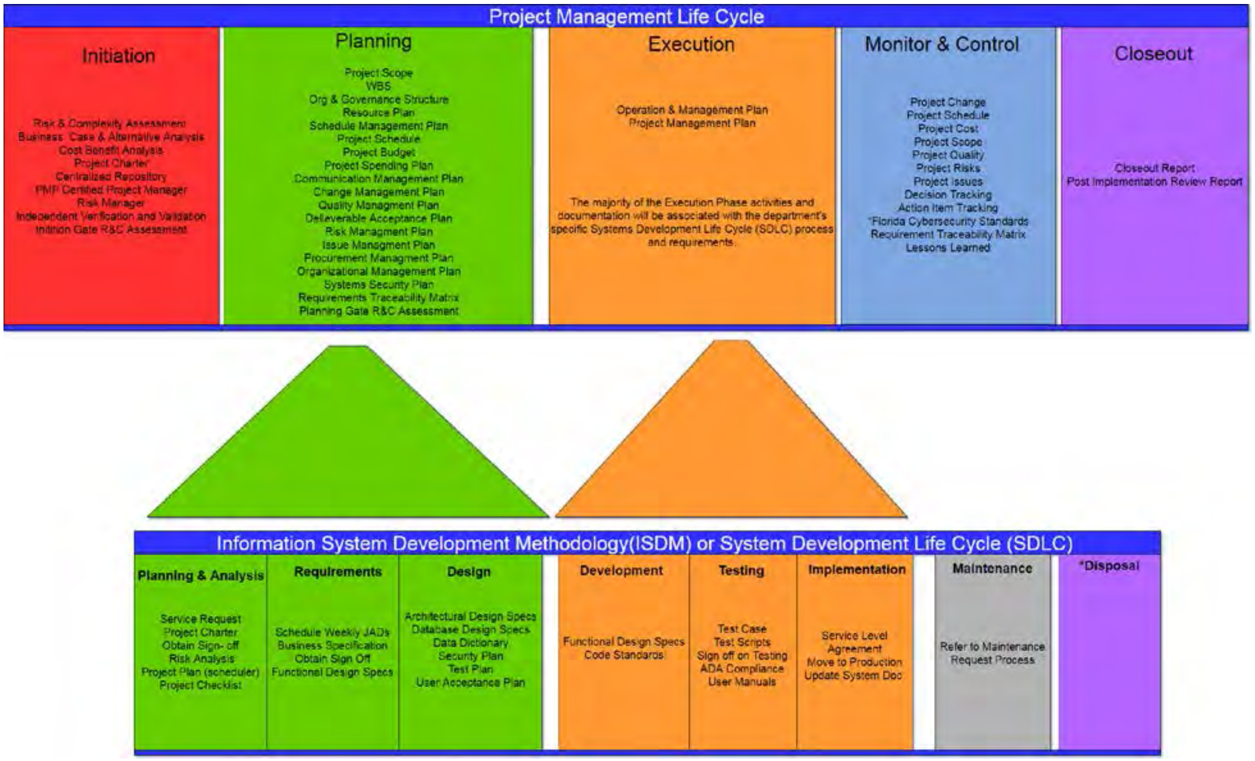
The Office of Application Development and Support (OADS) within the Division of Technology and Innovation provide internal information technology (IT) consulting services to department offices. OADS is responsible for systems development, systems support, data administration, and web development. OADS also establishes enterprise wide standards relative to these services.

OADS works in partnership with its customers to identify needs and develop applications that support their business functions. OADS currently manages 362 applications. On March 14, 2013, the Chief Information Officer approved the Information Systems Development Methodology (ISDM). The ISDM or System Development Life Cycle (SDLC) provides a set of processes, standards, and best practices to be used in the development of software applications. These processes include project initiation, planning, design, development, testing, and implementation. The methodology ensures that all projects are developed with consistent standards and ensures system continuity.

The purpose of the IT Project Management Standard is to specify requirements for compliance with the department's information technology policies, other department policies, and applicable laws and regulations. The standard describes the project management methodology that guides all IT projects. The Project Management Standard includes an initiation phase, planning phase, execution phase, monitoring and controlling phase, and closeout phase. Per the standard, the majority of the execution phase activities and documentation will be associated with the department's SDLC process and requirements. See Table 1[1] for the Project Management Life Cycle and ISDM activities.

[1] The department performs risk and complexity assessments for the IT projects to determine the minimum level of project control necessary. Most of the project management steps are optional unless the project is deemed to have higher risk and complexity.

Table 1[2]



Project Management Life Cycle				
Initiation	Planning	Execution	Monitor & Control	Closeout
Risk & Complexity Assessment Business Case & Alternative Analysis Cost Benefit Analysis Project Charter Centralized Repository PMP Certified Project Manager Risk Manager Independent Verification and Validation Inition Gate R&C Assessment	Project Scope WBS Org & Governance Structure Resource Plan Schedule Management Plan Project Schedule Project Budget Project Spending Plan Communication Management Plan Change Management Plan Quality Managment Plan Delleverable Acceptance Plan Risk Managment Plan Issue Managment Plan Procurement Managment Plan Organizational Management Plan Systems Security Plan Requirements Traceability Matrix Planning Gate R&C Assessment	Operation & Management Plan Project Management Plan The majority of the Execution Phase activities and documentation will be associated with the department's specific Systems Development Life Cycle (SDLC) process and requirements.	Project Change Project Schedule Project Cost Project Scope Project Quality Project Risks Project Issues Decision Tracking Action Item Tracking *Florida Cybersecurity Standards Requirement Traceability Matrix Lessons Learned	Closeout Report Post Implementation Review Report

Information System Development Methodology(ISDM) or System Development Life Cycle (SDLC)							
Planning & Analysis	Requirements	Design	Development	Testing	Implementation	Maintenance	*Disposal
Service Request Project Charter Obtain Sign- off Risk Analysis Project Plan (scheduler) Project Checklist	Schedule Weekly JADs Business Specification Obtain Sign Off Functional Design Specs	Architectural Design Specs Database Design Specs Data Dictionary Security Plan Test Plan User Acceptance Plan	Functional Design Specs Code Standards	Test Case Test Scripts Sign off on Testing ADA Compliance User Manuals	Service Level Agreement Move to Production Update System Doc	Refer to Maintenance Request Process	

While the Systems Development Methodology and Project Management Methodology are similar, they are not the same. The two methodologies should never compete against each other during the development of an IT project, nor should you attempt to execute a development project using just one of the methodologies. In fact, the two methodologies should complement each other during system development projects to ensure successful development of IT projects. [3] Currently there is no department policy requiring the use of either the Project Management Standard or the ISDM.

We requested all applications developed and all IT projects overseen by OADS from July 1, 2014, through May 1, 2017. The department identified the Bureau of Educator Certification (BEC) Enterprise Licensing Project and the Statewide Course Numbering System (SCNS). Per the BEC Project Charter, "The original BEC Project, began in 2013, adopted an in-house development effort to try to refresh hardware and operating systems to current standard and then recode applications to current supportable software." Absent IT governance oversight, the contractors spent excessive time stabilizing and documenting the old system. After two years in development, the project stalled due to the complexity and challenge of trying to upgrade the current system. As a result, department management assigned the maintenance for the current BEC Enterprise Licensing Project to OADS and assigned a new project manager to assess the

[2] Items with asterisks (*) were not included in the department's Project Management Life Cycle or the System Development Life Cycle.

[3] http://www.thinkforachange.com/blog/sdlcisnotapmmethodology/

development project and get it back on track. The project team and business sponsors unanimously agreed that a wholesale replacement of the system was needed. Through additional assessment, the project team identified a customizable off-the-shelf solution that met BEC's business requirements. Subsequently, the department purchased an off-the-shelf software solution for the BEC Enterprise Licensing Project and is customizing the software based on its specific needs. The project oversight team followed the department's Project Management Standard, but the project did not follow the department's ISDM. We determined that the project oversight team completed all requirements in the department's Project Management Standard with the exception of the security requirements identified in the Florida Cybersecurity Standards.

SCNS is a uniform system for numbering courses across public higher education institutions. The assigned numbers describe course content to improve research, assist program planning, and facilitate the transfer of students. The system was developed in 2003 using technology that is no longer supported by the department. The purpose of the SCNS project is to transition the current legacy system from its existing Java/Oracle technology to a new system that uses Microsoft's Structured Query Language database and .Net programming technologies. SCNS was initially considered a maintenance task; however, due to the complexity, timeframe, age of the system, and inexperience of the staff in JAVA, OADS converted the task to a project in May 2016. The project oversight team followed the department's Project Management Standard. We determined that the project oversight team completed most requirements in the department's Project Management Standard but failed to complete the security requirements identified in the Florida Cybersecurity Standards, a Business Case and Alternative Analysis, a Cost Benefit Analysis Plan, a Resource Plan, a Project Spending Plan, or an Operation & Management Plan. The SCNS project is currently over budget. A cost estimate was completed in April 2016 with an estimated cost of $126,336.00. On April 25, 2017, OADS submitted an Application Development Request (ADR) form to request a true up of hours for the SCNS project and request additional hours. The new projected cost totals $379,497.80, exceeding the original estimated cost by $253,161.80. The Audit Results section below provides details of the identified deficiencies.

Findings

1: The department lacks an overall IT governance framework.

Gartner defines IT governance as, "the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals." Project governance provides business and project managers, the project team, project sponsors and all stakeholders with the structure, processes, decision-making models, and tools to ensure the successful management of the project and delivery of the end product. Governance provides a framework for making project decisions and defining roles, responsibilities, and accountabilities to ensure the success of the project.

The OIG completed a consulting engagement to assist with the development of the department's IT governance plan in August 2016. That review noted that prior efforts to establish IT governance were largely unsuccessful. The engagement concluded with the department developing an Enterprise Project Management Governance Plan. According to the department's draft Project Management Governance Plan, the project governance structure would include a governance steering committee comprised of executive level decision makers. The governance steering committee, when established, would be the department's decision-making body responsible for reviewing, approving, and monitoring IT projects to ensure new projects fit the organization's strategic objectives; remain within budgeted timeframes and costs; and utilize IT resources based on assigned priority.

As of May 16, 2017, the Division of Technology and Innovation's Enterprise Project Management Governance Plan remains in draft form and has not been formally adopted or implemented, and no formal IT governance structure is currently in place. Absent an agency-wide IT governance program and steering committee, stakeholders have no formal process for sharing project ideas, assignments, and tasks; approving and monitoring IT development projects; setting priorities for IT projects; and participating in strategic IT decisions. This could lead to duplicate IT development projects and projects that do not align with organizational strategic objectives. Since the department has a current data governance committee in place, project governance could be combined into the data governance meetings for time management and scheduling purposes. The data governance committee could vet the proposed projects and make recommendations to the executive level for approval and prioritization.

As described earlier in the report, the absence of agency-wide governance leads to divisions within the department not following a consistent development methodology and projects with no clear direction and oversight. This results in cost and hour overruns, which we observed in both the BEC Enterprise Licensing project and SCNS.

Recommendation

We recommend that the department approve and implement a project management governance plan. We recommend the approved plan establish a project governance structure, including a project steering committee, to enable department senior management to approve and monitor IT development projects, set priorities for IT projects, and participate in strategic IT decisions in a controlled and consistent manner.

Management Response

FDOE-IT concurs with the development of IT Governance. Therefore, we will work with the business units and the Data Governance Council to establish a project management plan for review and approval by leadership.

2: The department does not have enterprise Application Development policies.

Florida Administrative Code (F.A.C) Rule 74-2.003 requires agencies to, "Establish a System Development Life Cycle (SDLC) to manage system implementation and maintenance (PR.IP-2)". The ISDM or SDLC provides a consistent set of processes, standards, and best practices to be used in the development of software applications. These processes include project initiation, planning, design, development, testing, and implementation. The methodology ensures that all projects are developed with consistent standards and ensures system continuity. The department's last revision of the ISDM occurred on September 23, 2015.

We reviewed the OADS' ISDM and compared it to the National Institute of Standards and Technology (NIST) publication 800-64r2, F.A.C Rule 74, and ISACA's Control Objectives for Information and Related Technology (COBIT) to ensure alignment with national standards. We determined the ISDM generally aligned with national standards, but some improvements could be made. The ISDM did not include the detailed security activities identified through NIST. NIST also includes a disposal phase, which is not included in the department's ISDM. The disposal phase is the final phase of the SDLC and provides for the disposal of a system and closeout of contracts. We additionally noted the OADS ISDM is based on the Information Technology Infrastructure Library (ITIL) standard; however, OADS was not able to provide the ITIL documentation.

During our review, we evaluated whether all agency divisions followed the OADS ISDM. We interviewed staff from various divisions and offices within the department to determine the methodologies utilized. We determined systems development at the department is a decentralized process managed by individual divisions and offices that create and develop their own data systems with little or no oversight from OADS. Various divisions have their own developers who build applications for specific offices. These decentralized divisions included the Division of Blind Services (DBS), the Division of Vocational Rehabilitation (DVR), and the Commission for Independent Education (CIE). We determined DBS and CIE do not utilize the department's ISDM. DVR utilizes the ISDM but includes a section called "ISDM Exemptions." We noted that additional offices have contracted developers who report to the IT division but office management was unaware of the ISDM.

As part of our evaluation, we determined OADS has established internal procedures such as the Applications Development Request (ADR) form and the ISDM, but has not developed agency wide policies to govern and mandate the use of the ISDM and Project Management Standard. Absent application development policies, department management and staff lack consistent direction and development parameters and tend to adopt what appears to be the best approach to serve their purpose. This lack of policies and consistent methodologies leads to cost and hour overruns in application development projects and increases the likelihood that critical steps, such as the security requirements analysis, can be omitted.

Recommendation

We recommend the department develop and implement application development policies. These policies should include, but not be limited to:

- A requirement that the department's ISDM and Project Management Standard be followed for new application development projects and major modifications to existing applications;
- Definitions for projects, application modifications, and maintenance tasks, including criteria for differentiating major application modifications from routine application maintenance tasks (ex: risk, hours, complexity);
- Direction for establishing which projects must go through the governance process;
- A requirement that all new projects or major application modifications be assigned an applications development manager who has knowledge over the subject matter;
- A requirement that an ADR form be used to initiate new projects or application modifications; and
- Cost estimation guidelines.

We further recommend OADS consult with the other divisions and offices to update the current SDLC methodology and implement it department-wide. The revised SDLC should consider the various approaches to system implementation (build from scratch, purchase commercial software (COTS), modify commercial software, maintenance, etc.). Finally, we recommend the department include a closeout phase in the SDLC in order to align with national standards.

Management Response

- FDOE-IT will work to update the ISDM and create a policy that requires all IT staff to follow the same methodologies;
- FDOE-IT will create project definitions vs maintenance task;
- FDOE-IT will develop guidelines that identify which projects will require governance process;
- FDOE-IT will establish a standard requiring that new projects and major application modifications be assigned to application knowledgeable subject matter;
- FDOE-IT will establish an internal policy governing the initiation of new projects and application modifications and the use of ADR forms;
- FDOE-IT will develop specific guidelines for applying cost estimates; and
- FDOE-IT will work to update the ISDM and create a policy that requires all IT staff to follow the same methodologies.

3. The department did not follow the Project Management Security Standard.

F.A.C. Rule 74-2.003 requires agencies to, “Establish a System Development Life Cycle (SDLC) to manage system implementation and maintenance (PR.IP-2).” The rule further requires agencies to review security requirements and controls for new technologies, ensure security reviews are approved before new applications are moved to production, and ensure the applications development team implements appropriate security controls to minimize risks to development projects. F.A.C. 74-2.002 states, “Each agency shall establish policies, procedures, and processes to manage and monitor the agency’s regulatory, legal, risk, environmental, and operational IT requirements. Procedures shall address providing timely notification to management of cybersecurity risks.”

According to NIST Special Publication 800-64, “Security planning should begin in the initiation phase by:

- Identifying key security roles for the system development;
- Identifying sources of security requirements, such as relevant laws, regulations, and standards;
- Ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements; and
- Outlining initial thoughts on key security milestones including time frames or the development triggers that signal a security step is approaching.”

We requested all applications developed and projects overseen by OADS from July 1, 2014, through May 1, 2017, to determine if the project oversight team completed all application development requirements. The department identified the BEC Enterprise Licensing Project and

SCNS. According to the project manager of the BEC Enterprise Licensing Project, the project was in the execution phase of its SDLC at the time of our review. The project oversight team followed the department's Project Management Standard but did not follow the ISDM. We determined that the project oversight team completed all requirements in the Project Management Standard with the exception of the security requirement.

We requested the BEC security plan; however, as of April 28, 2017, the plan remained in draft form and had not been approved by department management. Management indicated they were unaware of the security plan requirement due to the omission of the Florida Cybersecurity Standards from the department Project Management Standard. We interviewed staff and requested additional documentation to determine if the project oversight team identified security risks and requirements in the initiation phase of the project. Per staff, the team identified security requirements in January 2016, and the department required the vendor to ensure security was built into the new BEC licensing product. The project oversight team held an Executive Leadership briefing on January 28, 2016, and listed "identify core business and security requirements" as a standard activity. We found no additional documentation or description of the requirements discussed.

The SCNS project also followed the department's Project Management Standard. We requested the SCNS security plan; however, as of May 5, 2017, the plan was in draft form pending review. SCNS was developed in 2003. The purpose of the SCNS project is to transition the current legacy system from its existing Java/Oracle technology to a new system that uses an SQL database and .Net programming technologies. SCNS was initially considered a maintenance task; however, due to the complexity, timeframe, age of the system, and inexperience of the staff in JAVA, OADS converted the task to a project in May 2016. The conversion was to ensure the project followed the Project Management Standard and ISDM.

We compared the department's project management standard to F.A.C. Rule 74-1 to ensure alignment. We determined the department's Project Management Standard aligned with F.A.C. Rule 74-1 with the exception of the omitted Security Planning Requirement related to the Florida Cybersecurity Standards. The Florida Cybersecurity Standards includes a requirement to monitor and control projects in compliance with F.A.C. Rule 74-2, and is reflected in the monitoring and controlling phase of F.A.C. Rule 74-1. The Florida Cybersecurity Standards require each application with a categorization of a moderate impact or higher to have a documented system security plan.

In addition, we noted the department's minimum-security standards for software development were not up to date with the F.A.C. Rule 74. In the absence of integrated security, IT management are not fully aware of current risks and weaknesses, and cannot appropriately identify and prioritize security activities or initiatives, and rationalize budget considerations that would normally flow from planning discussions. Security should be planned well in advance as the implementation tools may take time and considerable resources to implement. Failure to implement adequate controls increases risk and other sensitive resources and the data it contains and exposes the projects to excessive change orders and can lead to increased cost and time.

Recommendation

We recommend the department update the Project Management Standard to include the Security Planning Requirement related to the Florida Cyber Security Standard and ensure the system security plan is documented for all applicable projects. We further recommend the department update the minimum-security standard to reflect the current F.A.C. Rule 74-2.

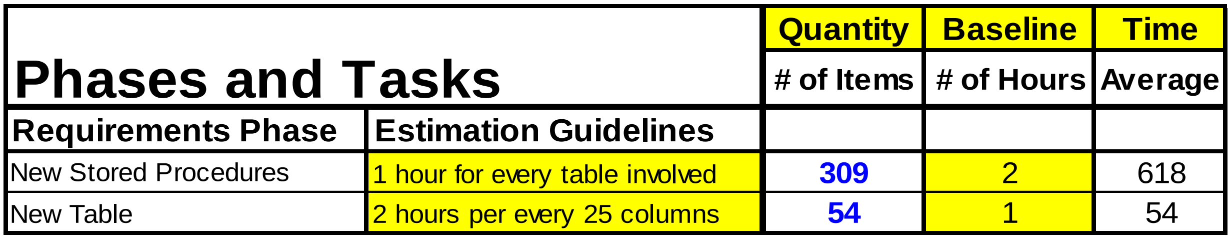
Management Response

FDOE-IT will resubmit the Enterprise Governance plan to leadership for approval ensuring that it includes the Security Planning Requirements related to the Florida Cyber Security Standard and ensure the system security plan is documented for all applicable projects and meets minimum security standard.

4. Application Development Cost Estimates are not reliable.

It is very important to accurately estimate the cost and duration of IT application development projects. If the potential costs and hours are underestimated, the resulting overruns could lead to forgoing key system functions due to a lack of funds or a complete project failure. Conversely, greatly overestimating costs could cause business owners to eliminate key functions unnecessarily or decline to build the needed system at all. Inaccurate estimates can harm the credibility of the information systems development group and jeopardize relationships with the business owners.

We reviewed a sample of cost estimates from July 1, 2014, through the end of fieldwork to determine if estimates were accurate. We determined that OADS completed a cost estimate for SCNS in April 2016. The project was a technology upgrade and originally considered a maintenance task. Due to the complexity, timeframe, age of the system, and inexperience of the staff in JAVA, OADS converted the task to a project in May 2016. The estimation work sheet from April 2016 estimated 3,948 hours with a projected cost of $126,336.00. We noted two baseline hours changed on the estimation without justifications.



Phases and Tasks		Quantity # of Items	Baseline # of Hours	Time Average
Requirements Phase	**Estimation Guidelines**			
New Stored Procedures	1 hour for every table involved	**309**	2	618
New Table	2 hours per every 25 columns	**54**	1	54

The original estimate multiplied the estimated hours of 3,948 by $32.00 to reach a total cost of $126,336.00. The rate was calculated incorrectly, as the department used the hourly rate of a developer instead of the department's blended rate. The blended rate is the average hourly rate of application development employees. These rates are adjusted throughout the year based on number of applications development employees and number of applications being supported.

The original estimation was conducted without a Business Analyst (BA) or technical documents. After conducting additional research, OADS created a new in-depth cost estimate and estimated the project would take 3,079 hours. OADS informed the project owner of the change in rate and hours and provided a Service Level Agreement (SLA) for FY 16-17, which included the new blended rate and allocated 3,040 hours to the project. With the new blended rate, the estimated cost of the project totaled $201,794.20 (500 hours of contracted service at $90 per hour and 2,540 hours for application support at $61.73 per hour). The new cost exceeded the original estimate by $75,458.20. On April 25, 2017, OADS submitted an ADR form to request a true up of hours for the SCNS project and request additional hours for the project. The project currently has used 379 more hours than originally budgeted. The ADR is requesting an additional 2,679 hours (379 hours to cover the current negative balance, 1,380 additional hours for FY 16/17 and 920 for FY 17/18). The additional requested hours, (2,000 hours for Development, 439 for contracted services, and 240 for a Database Analyst) will cost the division $177,703.60. The new projected cost totals $379,497.80, exceeding the original estimated cost by $253,161.80. Per the Project Management Plan, the SCNS budget is currently $349,344.00.

We also reviewed the projected recovery costs for FY 14-15, 15-16, and 16-17. We determined OADS had not calculated end of year costs during the scope of the audit. OADS completed a mid-year reconciliation for FY 15-16, which was the first activity of this kind. Per staff, performing actual end of year cost calculations is a planned activity for the end of FY 16-17. Calculating end of year costs would assist OADS in planning for the next year’s activities and provide reliable future projections.

We determined the department does not have policies and procedures that govern cost estimates. The estimates for new development are contingent upon staff experience. Estimating costs early in the process without detailed research, lacking justification for deviations from the estimations, and completing estimations without a knowledgeable BA leads to inaccurate estimates, costs exceeding original estimates, and reputational harm. Previous year costs can assist with cost estimate and provide more reliable future projections.

Recommendation

We recommend OADS establish documented policies for conducting cost estimates. These policies should include, but not be limited to:

- Conducting detailed research with the business owner prior to estimating the costs of projects, applications, and maintenance activities;
- Having a knowledgeable BA participate in all cost estimates and document justifications for deviations from the estimates;
- Conducting periodic budget to actual comparisons to evaluate the accuracy of the cost estimates;
- Reviewing the cost estimates at the end of each project to evaluate the accuracy of the estimate and determine if adjustments to the methodology are warranted;
- Considering whether cost and hour estimates were met when evaluating project team members; and
- Completing end of fiscal year actual cost calculations to enable more reliable future projections.

Management Response

FDOE-IT will develop specific guidelines for applying cost estimates. The guidelines will incorporate conducting detail research with business owners, periodic budget comparisons, and other reviews including requirements for BA participation in cost estimated and documentation.

Closing Comments

The Office of the Inspector General would like to recognize and acknowledge the OADS and staff for their assistance during the course of this audit. Our fieldwork was facilitated by the cooperation and assistance extended by all personnel involved.

To promote accountability, integrity, and efficiency in state government, the OIG completes audits and reviews of agency 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 Keisha Conyers and supervised by Tiffany Hurst, 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.