Idaho Legislative Audits
P.O. Box 83720
Boise, ID 83720-0054
208-334-2475

Office of the State Controller
Special Report on IT System

Management Report on Financial Procedures

Issued: April 21, 2004
Fiscal Year: 2003

LEGISLATIVE AUDITS' MANAGEMENT LETTER

OFFICE OF THE STATE CONTROLLER

PURPOSE AND SCOPE. We completed certain audit procedures on the Office of the State Controller's (Office) information technology (IT) systems during the period ending June 30, 2003. In planning and performing the scope of our audit procedures, we considered the internal controls pertaining to the Office's financial-related IT systems and compared them to the Control Objectives for Information and Related Technology (COBIT) guidelines. These guidelines are published by the IT Governance Institute, that was formed by the Information Systems Audit and Control Association. Based on this evaluation, we determined appropriate procedures and tests that would allow us to state our recommendations and not to provide assurance on the agency's overall internal control.

CONCLUSION. This management letter contains six findings and recommendations to improve the Office's IT related internal controls. Although we include six findings and recommendations, we believe that the Office's overall IT functions adequately meet current industry standards and that the Office substantially complies with laws, regulations, rules, and contracts related to information technology for which we tested compliance.

FINDINGS AND RECOMMENDATIONS. The six findings and recommendations summarized below apply specifically to the Office's financial-related IT systems:

FINDING #1 <u>The Office has no formal IT Planning/Steering Committee, nor does it have well-defined long- and short-range information technology plans</u>.

Information technology industry standards, as referenced in COBIT, call for detailed long- and short-range IT plans, typically produced by an IT planning/steering committee (committee). The committee should include executive level representation, senior IT and non-IT management representation, and representation from major users both internal and external to the Office. This committee should study and provide guidance for long-range IT needs of all users, understanding that the committee will not only have an internal influence but also a statewide influence on the State's ability to accomplish its goals in an efficient and effective manner.

The Office holds weekly executive management meetings and other periodic meetings in which staff discuss various issues, including limited IT discussions. However, the Office does not have a separate IT planning/ steering committee solely dedicated to aligning IT activities with the vision, mission, goals, and objectives of the Office. In addition, the IT steering committee should be responsible for producing the Office's long-range IT plan and ensuring that IT decisions make progress toward the goals stated in the long-range plan. As a result of having no IT steering committee, the Office also has no well-defined long-range IT plan.

The Office provides many mission critical services to the State of Idaho including most, if not all, State agencies. These services include maintaining and administering the State's Employee Information System (payroll accounting) (EIS), fixed asset accounting system (FAS), and the Statewide Accounting and Reporting System (STARS), as well as other services. Each of these services is IT dependent and therefore IT factors highly into determining whether the Office and the State's agencies can each accomplish its mission, vision, long-term goals and objectives.

While acknowledging that the Office does not wish to convey that IT is more important than any other office or State business function, IT certainly is more pervasive and has the potential of halting or holding back the other business functions and, therefore, requires focused, office-wide attention to planning efforts. Since IT factors so highly into whether the Office and the State's agencies can each meet its goals and objectives, it is evident that there are logical consequences of not having an adequate long-range IT plan. The Office risks making short-term IT decisions that fail to meet the State's long-term IT needs. The possibility of philosophical and political change in the Office also contributes to this risk. A long-range plan can help provide continuity to the IT process, thereby reducing the associated risk.

We recommend that the Office establish a formal IT planning/steering committee dedicated specifically, but not solely, to strategic IT planning. We also recommend that the IT steering committee be charged with producing a long-range IT plan and overseeing the production of short-range IT plans, ensuring the plans align with the long-range plan.

CORRECTIVE ACTION PLAN

Where IT planning has taken place at the management team level, the State Controller's Office (SCO) recognizes the value of broadening the group of IT planners to include customers, agencies, and other stakeholders and partners. To this end, an invitation will be extended to appropriate potential IT planning committee members and a committee will be formed. The charge of this committee will be the creation of a long-range IT plan and to oversee the production of short-range IT plans to ensure alignment. This committee will

also address the multi-party service level agreements, practical cross training, and business continuity recommendations contained in the management letter.

FINDING #2

The Office has no service-level agreements with its business partners to ensure the continuity of critical business services.

The Division of Computer Services does not have or maintain service-level agreements with any of its internal or external customers. The Division is responsible for the principal mainframe computer and other servers operated by the State, that are used to run applications and house data needed by other organizations including, State agencies and other non-State business partners. The most notable mainframe applications include STARS, EIS, and several Health and Welfare applications. In addition to this responsibility, the Division also provides programming and development services to other internal divisions and State agencies. Clearly, many parties depend on the Office to provide these critical business services.

It is important to note that the Office also depends on other parties to provide critical business services to the Office. These services are critical to the Office's ability to provide continuous critical business services to others. As noted, the Office receives and provides critical business services, thereby establishing the need for agreements between all related parties.

Good business practices and industry standards cited through COBIT recommend that organizations establish service-level agreements with all business partners who are considered key links to the organization's ability to provide continuous service in any of its critical business functions. Service-level agreements ensure that all parties, both users *and* service providers, know what is required of them and what will be provided to them by their business partners, as well as any penalties, which may be non-monetary, for failing to perform at the agreed upon level. Penalties may not be practical between State agencies, but they can and should be incorporated into agreements with non-State service providers.

Service-level agreements can be flexible, allowing shifts in resources when workloads are low and computer resources are not in use, so others can gain efficiencies. Service-level agreements are even more critical during unexpected down times or when resources are limited due to disaster. The agreements will serve to remind all parties of the previously agreed upon level of service they can expect or are expected to provide under the circumstances. If disaster strikes, or some other debilitating event occurs that requires the Office to use its alternate site, these agreements will be

critical in determining what resources can be made available, and when. Equally important, the Office can use these agreements prior to a debilitating or disastrous event to prepare and plan the steps necessary to respond responsibly if an event of this nature occurs.

Another benefit of service-level agreements is that they bring the parties together so each party knows what the other is planning. This in turn will assist the Office with its overall IT planning efforts by helping it understand its clients' future needs.

We recommend the Office work with its major service suppliers and customers, both internal and external, to implement service-level agreements. These agreements can be either two-party agreements or three or more party agreements, as long as the objective of ensuring continuous critical business services is met.

CORRECTIVE ACTION PLAN

Through the IT planning committee, the SCO will work with its major service suppliers and customers to implement multi-party service level agreements. In this way the service objective will be aligned to the strategic IT plans.

FINDING #3

The Office's Employee Information Handbook does not contain effective up-to-date policies regarding computer, Internet, or e-mail usage.

Good business practice and IT standards cited through COBIT call for current, detailed office policies specifically related to general use of computers, the Internet, and e-mail.

The Office has not updated its employee handbook since 1999. This is because the Office lacks a process for periodically reviewing the handbook. A lack of communication and understanding between management and employees regarding IT policies creates a control weakness, which allows the possibility for employees to make costly errors and then reason that they had no direction from the organization regarding the action in question. For instance, an employee could misuse the Internet by passing confidential or questionable materials into or out of the agency, while claiming that they did not know these actions were forbidden. With no policy in place, any resulting losses would likely be directed against the State.

We recommend that the Office initiate a process to ensure that the employee handbook, as well as other IT policies are updated on a periodic basis. At a minimum, the policies should reference existing statewide executive level policies regarding these subjects, stating that it is the policy of the Office to follow these executive level policies. Each employee should then be required to acknowledge, in writing on an annual basis, that they have read and understand the Office policy.

CORRECTIVE ACTION PLAN An in depth review of the employee handbook began in the summer of 2003 which was fine tuned at a management team meeting in the fall. Currently, the employee handbook is in the edit/refine stage. Significant changes have been put in place and the policies regarding Internet and email usage will follow closely the Governor's executive order 2001-12. The targeted completion date will correspond with SCO employee evaluations done in the spring of 2004. Each employee will review this handbook and attest that they have done so at that time. Attestation will be required of each employee at the time of employment and yearly thereafter.

FINDING #4 The Office does not routinely cross-train its IT staff.

Industry best practices recommend cross-training IT workers. While it is assumed that some workers could perform many of the tasks of other workers, we found no established plan for cross-training IT personnel. If workers are not sufficiently cross-trained, disruptions in service can occur, as well as the loss of institutional knowledge when workers leave the agency.

Cross-training provides an important function and helps maintain a competent staff. This training is crucial when back-up personnel are needed to cover critical IT functions, especially during disasters or when workflow bottlenecks occur, requiring additional personnel in specific areas.

There are several ways to cross-train employees. A well-planned periodic rotation of staff between positions is one excellent way to achieve cross-training. Staff rotation helps provide employees with a better understanding of the needs and demands specific to other jobs. An additional benefit of staff rotation is that it helps prevent certain types of fraud that require an individual remain in his/her position to go undetected. Other cross-training methods, such as periodically working with a coworker, can also be used effectively.

We recommend that the Office initiate an office-wide policy requiring some form of practical cross-training between IT functions.

CORRECTIVE ACTION PLAN The IT planning committee will address the creation of an office-wide policy for practical cross-training between IT functions.

FINDING #5 The Office has no alternate power source to sustain the State's central computer systems for an extended period of time in case of a power outage.

Industry standards and best business practices recommend that organizations provide a backup power supply capable of sustaining critical

operations in the event of a power failure until power is restored. The Office's computer system, especially its mainframe system, is critical to the State's daily business operations. Without the ability for the computers to operate during a period of prolonged power outages or disruptions, the Office would be faced with two disruptive options. These options are:

1. Relocate to the alternate site contracted by the Office.
2. Shut down operations and wait for the power to be restored.

Since no other options are available, the Office would be forced to choose one of these options. Either choice would cost the Office, State agencies, other organizations, and individuals time and money.

We recommend that the Office acquire an alternate power source capable of sustaining its critical business operations for extended periods, thereby substantially reducing the risk of financial loss and liability associated with a shutdown of critical business functions. In addition, we also recommend that the Office coordinate with other capitol mall agencies to determine whether it would be practical and more efficient to combine efforts to obtain an alternate power source capable of restoring lost power to all critical systems in the area.

CORRECTIVE ACTION PLAN

The SCO is implementing its plan for an alternative power source to be completed in May 2004. This alternate power source will be capable of sustaining critical business operations for extended periods and is being done in cooperation with the Division of Public Works.

FINDING #6

The Office's Business Continuity Plan does not address all key internal and external concerns.

Industry standards and good business practices recommend creating thorough, comprehensive business continuity plans that are published and tested for workability. Currently, the Office's Division of Computer Services has a detailed plan to restore computer operations in the event of an in-house mainframe system failure. The plan is designed to limit the impact on State operations if the Office were to lose access to its mainframe resources locally. Although the plan allows for limited computer resources to be established at a remote site in a different geographical area, the plan does not fully consider the possible overall impact on the operations of the Office and other State agencies. The possible areas of impact include, but are not limited to, STARS, EIS, and computer services for employees not working at the alternate site, both inside and outside of the Office.

If an incident required the Office to switch computer operations to its alternate site, there is a strong probability that the remaining office space in the J.R. Williams Building would not be available for use. This could

mean that STARS and EIS may be out of service, and the remaining computer services employees would not be able to perform their duties that require system access. In addition, there is no plan in place to inform employees when a debilitating event has occurred or where they are to report to work should an event of this nature occur.

Outside of internal operations, the Office must coordinate with other State agencies should an emergency occur. These agencies need to know how to contact key Office personnel and how to reestablish system connections to STARS, EIS, several Health and Welfare applications, and any other office system necessary for each to carry out their responsibilities

We recommend that the Office review its overall operations and adjust its business continuity plan to address the needs and requirements of all affected parties. In addition, agreements to provide office space and communication services should also be formalized. These agreements and the business continuity plan should include provisions for distributing key personnel rosters and contact information to all responsible parties in the case of a debilitating event. We also encourage statewide policymakers, such as the Information Technology Resource Management Council (ITRMC), to ensure agencies adequately address disaster recovery/business continuity needs by issuing policy statements and recommending that financial resources be provided to agencies as necessary.

CORRECTIVE ACTION PLAN

The IT planning committee will be charged with reviewing and adjusting business continuity efforts to address the needs of all affected parties. Currently, a business continuity planning committee headed by Robert Sox is working out agreements to provide office space and communication services and will soon be formalized. This committee is also creating detailed provisions for distributing key personnel rosters and contact information to all responsible parties in the case of a debilitating event.

The SCO has a tested, workable plan for the recovery of computerized operations in place. We have offered our expertise in this area to other state mainframe operations and would allow them to piggyback on our current plans. Other agencies could use the SCO as a hot site for their own disaster recover planning and the offer has been made to expand SCO's existing hot site for their use. This recommendation would be better served being directed to the statewide policymakers where funding decisions could be addressed. Backing by policymakers including funding and widespread cooperation between agencies is necessary for the successful implementation of business continuity. Disaster recovery and business continuity planning require significant resources, and a funding commitment is paramount to their success.

AGENCY RESPONSE. The Office has reviewed this information and is in general agreement with its contents. The Office of the State Controller's full response to each finding and recommendation has been included in this report.

OTHER ISSUES. In addition to the findings and recommendations, we discussed other, less important issues which, if changed, would improve internal control, ensure compliance, or improve efficiency.

This letter is intended solely for the information and use of the Office of the State Controller and the Idaho Legislature, and is not intended to be, and should not be, used by anyone other than these specified parties.

We appreciate the cooperation and assistance given to us by the Idaho State Controller, Keith Johnson, and his staff.

QUESTIONS CONCERNING THIS DOCUMENT SHOULD BE DIRECTED TO:
Ray Ineck, CGFM, Supervisor, Legislative Audits
Scott Thornton, CISA, IS Audit Coordinator

Report SP14002