Volume 13 • 2007 Annual

ILLINOIS Audit ADVISORY

Emerging and Potential Audit Issues

William G. Holland
AUDITOR GENERAL

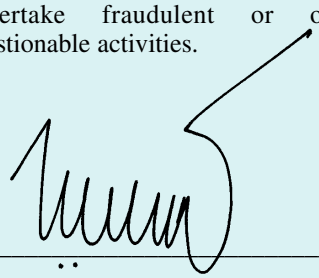
AUDITOR GENERAL'S MESSAGE

My Office routinely reports on findings in agency operations. While all findings are important, there are clearly those which – for various reasons – pose a higher risk to the operation of State government than others.

Beginning this year, in a manner similar to that utilized by the federal Government Accountability Office, the Auditor General's Office has compiled a list of high risk areas. These are areas where: 1) the State is exposed to a high level of risk; and 2) the deficiency occurs in multiple State agencies.

This issue of the Audit Advisory examines this year's list. In subsequent issues of the Advisory, this list will be updated. If significant progress has been made by State agencies to resolve these high risk areas, the issue will be removed. As new high risk areas are identified, they will be added.

This Advisory also examines an important change made in auditing standards, specifically the changes imposed by Statement on Auditing Standards No. 112 "Communicating Internal Control Related Matters Identified in an Audit." Finally, the Advisory examines actions that management can take to lessen the likelihood that employees will undertake fraudulent or other questionable activities.



WILLIAM G. HOLLAND
August 2007

HIGH RISK AREAS

There are certain activities that State government undertakes that, if not done correctly, expose the State to an unacceptable level of risk. The Office of the Auditor General has compiled a listing of high risk areas, based on findings in recent audit reports. These areas are high risk because they are susceptible to abuse, fraud, mismanagement, or noncompliance. These deficiencies occur in multiple State agencies.

The five high risk areas on our initial list are:

1. Contracting Processes
2. Subrecipient Monitoring
3. Financial Reporting
4. Safeguarding Confidential Information
5. Noncompliance with State Laws

The following sections of the Advisory provide an overview of each of these high risk areas.

1. CONTRACTING PROCESSES

The contracting process poses unique and significant risks for State agencies and is susceptible to fraud and abuse. There are a myriad of ways the contracting process can be manipulated or abused. Contracts can be directed to favored firms by altering the evaluation process or using the emergency or sole source procurement method. Contractors can be paid for work not performed or for expenses not incurred if the agency's payment review process is ineffective. Consequently, an agency's system of internal controls related to contracting needs to be strong, monitored, and enforced.

Contracting deficiencies have been routine findings in OAG audits, with some of the more significant findings occurring in recent years. Examples of contracting deficiencies cited in recent audits of State agencies included: untimely execution of contracts; lack of documentation for the evaluation, selection, and contracting processes; use of evaluation criteria that were not stated in the RFP; failure to include information on subcontractors in the contracts; allowing vendors to begin work without a formal written agreement in place; failure to publish the required notice of awards in the Procurement Bulletin; failure to submit emergency purchase affidavits to the Office of the Auditor General; and inadequate documentation to support items billed and inadequate agency review of such billings.

Noncompliance with contracting laws, agency policies and procedures, and good business practices leaves State agencies vulnerable to contracting abuses. As agency managers, we have the responsibility to monitor our contracting processes, and routinely review our internal controls to ensure that State laws, rules, and agency policies are being followed.

2. SUBRECIPIENT MONITORING

State agencies' failure to adequately monitor subrecipients has been a central finding in the State's Single Audit for years. The FY 2005 Single Audit included 24 findings and the FY 2006 Single Audit had 21 findings related to agencies' deficiencies in monitoring subrecipients. Agencies covered by the Single Audit received $15.5 billion in federal funding in FY06.

It is not sufficient for agencies to simply pass funding on to third parties. Rather, a system must be established to monitor how those funds are being spent and ensure these monies are being spent for the specified purpose.

See HIGH RISK on Page 2

HIGH RISK

Continued from page 1

Subrecipient monitoring includes many aspects, such as reviewing and receiving grant reports, as well as some level of on-site reviews or inspections. Some of the subrecipient monitoring issues reported in recent Single Audits include:

- Failure to use a risk assessment approach in monitoring.
- Failure to monitor subrecipient cash management.
- Failure to receive or timely review required reports.
- Failure to follow-up on deficiencies identified in monitoring reports.
- Failure to conduct programmatic and fiscal reviews (including on-site visits).

Failure to adequately monitor subrecipients may result in federal funds being expended for unallowable purposes and subrecipients not properly administering federal programs in accordance with laws, regulations, and the grant agreement.

3. FINANCIAL REPORTING

Deficiencies in financial reporting by State agencies have been an issue for a number of years and the subject of articles in prior Audit Advisories.

Financial reporting errors have several important effects, including increased audit testing, delays in the completion of audits, and delays in the preparation of the Comptroller's Comprehensive Annual Financial Report (CAFR). These reporting errors may be caused by inadequate internal controls over the financial reporting process. If internal controls are weak over financial reporting, they may also be weak over the receipt and disbursement of funds, which can lead to even greater problems at the agency.

Deficiencies in financial reporting include:

- Late preparation of financial statements and other financial reporting forms (GAAP forms).
- Improper recording or misclassification of transactions, requiring significant revisions to financial statements.
- Lack of appropriate reconciliations of cash balances to bank accounts.
- Failure to reconcile account detail to the records used to prepare financial statements.
- Inadequate controls over the calculation and submission of capital asset information for financial reporting purposes.
- Lack of control over the accounts receivable reporting process.
- Inappropriate application of generally accepted accounting principles (GAAP).

Some improvement was observed in the fiscal year 2006 financial reporting by State agencies, which enabled the completion of the State's CAFR in February 2007; in the two previous years, the CAFR was issued in May and June, respectively, primarily because of the amount of time needed to work with State agencies to fix financial reporting deficiencies.

4. SAFEGUARDING CONFIDENTIAL INFORMATION

The theft or loss of personal information is an increasing problem in the State of Illinois. Recent news stories have detailed accounts of hackers accessing State systems to obtain personal information and State agencies not properly disposing of confidential or sensitive documents.

Audits have identified two areas of concern. The first deals with inadequate controls over the disposal of hard copy confidential information. Auditors found confidential, personal, and sensitive information in trash and recycle bins located both inside and outside the State office buildings. Information included:

- Recipient names, social security numbers, and case numbers.
- Payroll reports, including names and social security numbers.
- Employee timesheets, benefit statements, and bond statements that contained employee names, dependent names, social security numbers, and home addresses.
- Sensitive computer security information.

The second area of concern is a failure to ensure adequate security over computer systems and resources. Our audits reported the following:

- Servers were not updated with the current vendor patch levels.
- An excessive number of users having powerful security administration authorization.
- Accounts with no password requirements.
- Accounts for terminated employees remained active from 2 to 14 months after termination.
- Access to the agency's data center and network wiring closets was not adequately restricted.

At one agency, a security breach led to the unauthorized access and potential compromise of personal and confidential information, including social security numbers and credit card numbers of anywhere from 200,000 to 240,000 individuals. The agency had failed to implement solutions to correct security administration and firewall weaknesses identified in the prior audit.

The Personal Information Protection Act requires State agencies to properly dispose of information. The Act states, *"Any State agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material."*

(815 ILCS 530/30)

The Act defines personal information as the individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social Security number.
- Driver's license number or State identification card number.
- Account number or credit or debit card number.

State agencies should perform a detailed assessment of the retention, storage, security, disposal, and control over confidential and personal information. One of the best approaches to protect such information is to eliminate its retention and storage, unless it is absolutely necessary. If personal information must be retained, it should be encrypted (rendering the contents of a message or file unintelligible to anyone not authorized to read it) or redacted (removing all or portions of personal data).

The Act contains specific requirements for State agencies to notify individuals at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach.

See HIGH RISK on Page 4

WORKPLACE ENVIRONMENT AND FRAUD

As agency managers, one of the most unpleasant possible occurrences is to find out that one or more of your employees have been involved in fraudulent activity. Agency management is ultimately responsible for instituting a set of internal controls to minimize the possibility that fraud could occur undetected.

One of the most important actions management can take is to create a culture of honesty and high ethics. Part of such an effort is for management to communicate, to each employee, what behavior is acceptable and what management's expectations are of that employee.

Much has been written about management setting the "tone at the top." Employees often take their cues on what is acceptable behavior from their managers.

If managers act in a highly ethical manner and demonstrate that behavior to their employees, it is likely that employees will behave similarly. However, if employees observe management acting in a questionable manner, there is a greater possibility they will do likewise. Consequently, it is critical that management establish a culture of high ethical and moral behavior.

A positive workplace environment can also be an effective tool against fraud. If employee morale suffers, the employee may have less reservation about acting contrary to the well-being of the organization and creating a fraud.

Other important actions management should take include:

- Hiring and promoting employees who demonstrate high levels of honesty and competence.
- Training employees on the agency's values and code of conduct.
- Letting employees know they will be held accountable for their actions.
- Disciplining employees who have taken inappropriate or unacceptable actions.

NEW AUDITING STANDARDS

Auditing standards promulgated by the American Institute of Certified Public Accountants (AICPA) and the Government Accountability Office have been revised this past year and will impact audits conducted by the Office of the Auditor General. One of the more significant changes which will impact financial audits is contained in Statement on Auditing Standards (SAS) No. 112 — "Communicating Internal Control Related Matters Identified in an Audit."

SAS No. 112 requires auditors to evaluate identified control deficiencies and then determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses. SAS No. 112 states that a *control deficiency* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

A deficiency in *design* exists when (a) a control necessary to meet the control objectives is missing or (b) an existing control is not properly designed, so that even if the control operates as designed, the control objective is not always met. A deficiency in *operation* exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

A *significant deficiency* is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles, such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control. See inset for examples of indicators of significant deficiencies.

A *material weakness* is a significant deficiency, or combination of significant deficiencies, that results in **more** than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control. See inset on page 4 for examples of indicators of material weaknesses.

SAS No. 112 states that auditors must communicate, in writing, significant deficiencies and material weaknesses identified during an audit. Consequently, given the revised definitions of significant deficiencies and material weaknesses and the requirement that they now be reported in the audit report, matters that previously may have been included in an agency's immaterial findings letter, may now be reported as report findings in the regular financial audit. The Appendix to SAS No. 112 provides examples of circumstances that may be control deficiencies, significant deficiencies, or material weaknesses.

SAS 112: INDICATORS OF SIGNIFICANT DEFICIENCIES

Control deficiencies in the following areas usually are considered to be at least significant deficiencies:

- Antifraud programs and controls.
- Controls over nonroutine and nonsystematic transactions.
- Controls over selection and application of accounting principles that are in conformity with GAAP, including having sufficient expertise in the selection and application of GAAP.
- Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; initiate, authorize, record, and process journal entries into the general ledger; and record recurring and nonrecurring adjustments to the financial statements.

HIGH RISK

Continued from page 2

5. NONCOMPLIANCE WITH STATE LAWS

The primary responsibility of State agencies is to implement and administer programs and functions given to them by the General Assembly. Audits routinely find that agencies are not complying with these programmatic mandates.

In some instances, agencies are carrying out the required activities but are not fully accomplishing them, such as not meeting required time parameters. In other instances, the required activity has not occurred.

In addition to programmatic requirements, agencies are also required to follow administrative requirements prescribed by statute. Audits routinely contain findings on noncompliance with these administrative requirements (e.g., failure to comply with the timekeeping requirement of the State Officials and Employees Ethics Act).

Agencies need to take the necessary action to comply with statutory requirements. If agencies are not complying with a law because they believe it is outdated or duplicative, they should seek legislation to have the law revised. ■

SAS 112: INDICATORS OF MATERIAL WEAKNESSES

The following conditions are considered to be at least significant deficiencies and strongly indicate material weaknesses:

- The auditor has identified a material misstatement in the financial statements that was not identified by the entity's internal control. This includes misstatements involving estimates and judgment for which the auditor has identified likely material adjustments and corrections of recorded amounts. (Even if management subsequently corrects the misstatement, this is a strong indicator of a material weakness.)
- Previously issued financial statements are restated to correct a material misstatement.
- Fraud by senior management is identified, regardless of the magnitude of the fraud.
- Oversight of financial reporting and internal control by those charged with governance is ineffective.
- Management or those charged with governance fail to assess the effect of a previously communicated significant deficiency and correct it or communicate that it will not be corrected.
- An internal audit or risk assessment function is ineffective and such functions are important to the entity's monitoring or risk assessment of internal control.
- Because of deficiencies in various components of internal control, the auditor concludes that the control environment is ineffective.

Office of the Auditor General
• Iles Park Plaza, 740 East Ash Street
Springfield, Illinois 62703-3154
• Michael A. Bilandic Building,
160 N. LaSalle Street, Suite S-900
Chicago, Illinois 60601-3109

Phone: 217-782-6046
Fax: 217-785-8222
TTY: 1-888-261-2887
E-mail: auditor@mail.state.il.us
Website: www.auditor.illinois.gov