

**SWIAF/SEIAF Intergovernmental Audit Forums Joint Conference**  
**Panel Session: Process to Implement the New Yellow Book**  
**September 17, 2008**  
**8:00 – 9:45 A.M.**

**Office of the City Auditor, Austin, Texas**  
**Summary of Major Changes Made to Implement July 2007 Yellow Book Revisions**  
**By Stephen L. Morgan, City Auditor**

- We updated our policy on auditor independence to reflect more detailed descriptions of types of impairments and more explicitly require that audit managers review prior projects for the last five years when attesting to the team's independence. We also added a sign-off on the competency of assigned staff and a sign-off that the team's representations of their independence seem appropriate.
- We updated our office Code of Ethics, signed by all employees, to incorporate the ethical principles in Chapter 2 of the Yellow Book. Our previous code of ethics was adapted from the IIA's code of ethics, so now our Code incorporates both IIA and Yellow Book language.
- We created a new Quality Control and Assurance System policy to institute an internal Quality Control Assessment process to be performed annually. This assessment will be completed by a team appointed by the City Auditor. The results of the assessment will be reported to the City Auditor and any recommendations for improvement are implemented through a Management Team action plan.
- We conducted internal training and made revisions and clarifications to several policies to reflect the "musts and shoulds" contained in the 2007 Yellow Book. This included detailed analysis of the "musts and shoulds" and subsequent revisions to planning, fieldwork and evidence, and reporting policies to provide more explicit guidance to ensure compliance with the Yellow Book. For example, we expanded our planning policy to specify all of the elements that should be considered during planning (e.g. internal/IS controls, legal requirements, fraud or abuse, data reliability, prior work). We also expanded our fieldwork and evidence policy to explicitly address data reliability and fraud testing in fieldwork and include an overall assessment of evidence prepared by the team and properly signed off.
- We are in the process of updating our policy on non-audit services to more broadly define non-audit services and eliminate language regarding "routine activities". Our prior policy for non-audit services primarily applied to assistance or consulting work. Now, based on the expanded requirements and an inability to claim that we only followed the general standards, we categorize other types of work as non-audit including fraud investigations and requests for information from Council.
- Congruent with our policy changes we are also updating our "audit guide" to ensure it provides guidance in sync with our revised and new policies based on the Yellow Book revisions. We are also creating and updating our audit templates and examples for key documents (e.g. audit communication and planning documents). The templates and examples are designed to facilitate compliance with policies and supervisory review.
- Finally, we engaged in continuous improvement by:
  - ◆ participating as a "pilot" in the IIA's research project on the capability maturity model for government auditing;
  - ◆ evolving our integrity audit model which includes prevention, detection, investigation, and follow through; and
  - ◆ engaging in dialogue with City Council and management to strengthen the City's audit governance structure.

## Processes to Implement the New Yellow Book

**Note:** The following are process areas that individual panel participants can address in their presentations and/or questions can be asked of participants regarding their processes.

### Internal Audit Standards

3.16 Internal Audit functions are encouraged to use the IIA “International Standards for the Professional Practice of Internal Auditing” in conjunction with GAGAS.

*Does your audit organization follow Red Book standards?*

No

*What processes have you instituted to integrate the Red Book and Yellow Book standards and document compliance with both?*

N/A

### Overall Assessment

7.68 Auditors should perform and document an overall assessment on the collective evidence used to support findings and conclusions.

*What processes have you established for your organization to perform and document the overall assessment?*

We now explicitly require that the audit team conduct an overall assessment of evidence reviewed by the audit manager (typically once the audit findings are fully developed) where the team presents their support for each finding. Some teams are piloting using a form to document this assessment for each finding statement that speaks to the type of evidence used to support the finding, sources of evidence used to support the finding, steps taken to corroborate evidence used (including data reliability steps), and the team’s assertion about why the evidence is sufficient and appropriate. Other teams are summarizing the steps they took to assess the sufficiency and appropriateness of their evidence in a workpaper.

*How do you evaluate whether there is sufficient appropriate evidence to support the audit findings?*

See above, after the team completes the overall assessment the supervisor reviews it, asks questions, and signs off on the assessment.

### Quality Control and Assurance

3.53 An audit organization should include policies and procedures in its system of quality control that collectively address: a) leadership responsibilities for quality control; b)

independence, legal and ethical requirements; c) initiation, acceptance and continuance of audit and attestation engagements; d) human resources; e) audit and attestation engagement performance, documentation, and reporting; and f) monitoring of quality.

- 3.54 The audit organization should analyze and summarize the results of monitoring procedures at least annually.

*How has your audit organization enhanced its quality control system to comply with the Yellow Book?*

We created a new policy that institutes an internal Quality Control Assessment process to be performed annually by a Quality Control and Assurance Team (QCAT) appointed by the City Auditor.

*What are the processes for summarizing the results of your monitoring procedures at least annually? How and to whom are these results communicated?*

The Quality Control and Assurance Team (QCAT) provides a written summary of their results to the City Auditor, who then directs the OCA Management Team to prepare an action plan to address any recommendations made by the QCAT.

#### Auditors' Electronic Documentation

- 7.82 For audit documentation that is retained electronically, the audit organization should establish information systems controls concerning accessing and updating the audit documentation.

*What are your processes for establishing controls over your electronic data?*

For each audit project in our office, we establish permission rights when the project is started that give read/write access to team members and read-only access to the rest of our office. For particularly sensitive projects we may restrict access to only the team (no read-only access). This helps ensure that the audit documentation (during the audit) is only modified by the team assigned to the project. Once the project is completed, we burn a copy of the electronic documents to a CD, which becomes the permanent electronic record and is read-only. This needs to be codified in policy.

#### Independence/Non-Audit Services

- 1.34 Audit organizations that provide non-audit services must evaluate whether providing non-audit services creates an independence impairment either in fact or appearance.

*What processes are in place to evaluate potential impairments to independence? [related to non-audits]*

The policy currently in place was developed after the 2003 revisions and requires that OCA should consider whether providing non-audit services creates an impairment by applying the overarching principles (not performing management functions or making management decisions and not auditing our own work). It also requires that we document our consideration of independence as related to the non-audit service and develop an agreement with management when performing non-audit services that are not routine services.

We are currently revising our non-audit services policy to expand on the types of projects considered to be non-audits and ensure that the 2007 revisions are reflected in our policy. For the one assistance project since the revisions, we modified the agreement with management to reflect the revised standards language.

*What policies have been established to accept non-audit engagements?*

See above.

### Internal Control

7.16 For internal control that is significant within the context of the audit objectives, auditors should assess whether internal control has been properly designed and implemented.

*What processes do you use to obtain an understanding of internal control and how do you determine if it is significant to your audit objectives?*

Our planning policy requires that our audit planning includes steps designed to gain an understanding of the internal controls that are significant to the audit objectives. We also use our risk/vulnerability assessment process to evaluate risks relevant to the audit objectives and assess controls in place to mitigate risk.

We also are also in the process of developing templates for our planning documents that include generic steps that serve as placeholders to ensure that internal controls are reviewed and tested as needed.

*How do you determine that your evidence is sufficient and appropriate to support your assessment of the effectiveness of internal control?*

Insofar as an audit finding relates to ineffective internal controls, the team presents their assertion about the sufficiency and appropriateness of evidence and the audit manager reviews and signs off on those assertions as part of the overall assessment of evidence. (See overall assessment description above.)

7.24 When information systems controls are determined to be significant to the audit objectives, auditors should evaluate the design and operating effectiveness of such controls.

*What processes do you have in place to determine the significance of information systems control to the audit objectives?*

Our planning policy requires that our audit planning includes steps designed to gain an understanding of the information systems controls which are significant to the audit objectives or to data needed to complete the audit objectives.

We also are also in the process of developing templates for our planning documents that include generic steps that serve as placeholders to ensure that information system controls are reviewed and data reliability tests are performed as needed.

### Fraud

7.30 Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect findings and conclusions.

*What processes have you designed to accept this higher level of responsibility to “assess risk of fraud, rather than consider risks due to fraud (2003 Yellow Book)” in evaluating whether fraud could or has occurred?*

The process we have in place for considering risks due to fraud will also facilitate assessing the risk of fraud. Our planning policy requires that our audit planning includes steps designed to gain an understanding of the risks and sources or opportunities for potential fraud that could be significant within the context of the audit objectives. We also are also in the process of developing templates for our planning documents that include generic steps that serve as placeholders for planning to assess fraud risk and planning to detect fraud.

In practice, we assess the risk of fraud by administering questionnaires about fraud during audit interviews and conducting a brainstorming meeting with our fraud investigators as part of the planning (survey) phase to identify areas where fraud could be occurring in the audit area and to develop steps to provide reasonable assurance of detecting such fraud. As part of our fieldwork phase, we met with the fraud investigators again to discuss testing results and identify any further testing needed related to fraud.