

## **Internal Audit Department Peer Review**

The Internal Audit Department (IAD) last had a Peer Review completed on February 21, 2001. The US Governmental Accounting Office (Yellow Book) requires the next peer review to be complete within three years of the last review. The Yellow Book has an extension provision; however, IAD wanted to have the peer review finished by the AOC meeting today.

IAD selected and contracted with Jefferson Wells International to perform the review. However upon reflection and several communications, IAD asked Jefferson Wells to stop work until after direction by the AOC. IAD wishes to allow the existing governance and oversight of the AOC to actively select and direct the peer reviewer.

IAD seeks clarification and direction by the AOC of their intent to actively participate in the solicitation and evaluation of future vendors or rather to simply ensure that a peer review is performed tri-annually. As always, Internal Audit remains transparent and supports whatever direction the AOC would pursue.

**Item 4**

AOC Meeting 2/26/04



their areas of specialization but are not required to meet the CPE requirements described here. However, auditors who use the work of external and internal specialists should ensure that such specialists are qualified in their areas of specialization and should document such assurance.

### Quality Control and Assurance

**3.49** The general standard related to quality control and assurance is:

**Each audit organization performing audits and/or attestation engagements in accordance with GAGAS should have an appropriate internal quality control system in place and should undergo an external peer review.**

**3.50** An audit organization's system of quality control encompasses the audit organization's structure and the policies adopted and procedures established to provide the organization with reasonable assurance of complying with applicable standards governing audits and attestation engagements. An audit organization's internal quality control system should include procedures for monitoring, on an ongoing basis, whether the policies and procedures related to the standards are suitably designed and are being effectively applied.

**3.51** The nature and extent of an audit organization's internal quality control system depends on a number of factors, such as its size, the degree of operating autonomy allowed its personnel and its audit offices, the nature of its work, its organizational structure, and appropriate cost-benefit considerations. Thus, the systems established by individual audit organizations will vary as will the need for, and extent of, their documentation of the systems. However, each audit organization should prepare appropriate documentation for its system of quality control to demonstrate compliance with its policies and procedures. The form and content of such documentation is a matter of judgment. Documentation of compliance should be retained for a period of time sufficient to enable those performing monitoring procedures and peer reviews to evaluate the extent of the audit organization's compliance with the quality control policies and procedures.

**3.52** Audit organizations performing audits and attestation engagements in accordance with GAGAS should have an external peer review of their auditing and attestation engagement practices at least once every 3 years by reviewers independent of the audit organization being reviewed.<sup>38</sup> The external peer review should determine whether, during the period under review, the reviewed audit organization's internal quality control system was adequate and whether quality

---

<sup>38</sup> Audit organizations should have an external peer review conducted within 3 years from the date they start (that is, start of field work) their first assignment in accordance with GAGAS. Subsequent external peer reviews should be conducted every 3 years. Extensions of these time frames beyond 3 months to meet the external peer review requirements can only be granted by GAO and should only be requested for extraordinary circumstances.



**BYLAWS OF THE  
ORANGE COUNTY AUDIT OVERSIGHT COMMITTEE**

**December 17, 2002**

**I. GENERAL PROVISIONS**

**Rule 1:** The rules contained in these Bylaws shall govern the Orange County Audit Oversight Committee (hereinafter referred to as "Committee"). This Committee has been established as an advisory committee to the Board of Supervisors (hereinafter referred to as "Board").

**II. MEMBERSHIP OF COMMITTEE, RIGHTS AND DUTIES OF MEMBERS**

**Rule 2:** The membership of the Committee shall consist of the following: the Chairman and Vice-Chairman of the Board, the Auditor-Controller, the County Executive Officer (CEO), the Treasurer-Tax Collector as Ex-Officio (non-voting) Member, and one member-from the private sector appointed by the Board.

**Rule 3:** All Committee members will have an equal voice in the decision-making process. Due to the scope of the Committee's assignment, and the value of each member's input, consistent attendance by all members is expected, however, with the approval of the Chairman, a substitute may attend the meeting with the member's proxy.

**Rule 4:** In the event that a member chooses to resign from the Committee, such member should notify the Chairman, in writing. The Chairman will then immediately notify the Board and the Committee of any such resignations. Upon notification, the Chair of the Board will then solicit for a new member until the vacancy is filled.

**III. APPOINTMENTS, POWERS AND DUTIES OF THE CHAIRMAN**

**Rule 5:** The Chairman and Vice-Chairman shall initially be elected for a one year term, which may be extended for one additional year by a favorable vote of a majority of the Committee members.

**Rule 6:** The Chairman's duties include presiding over all Committee meetings, establishing subcommittees, responding to members' requests for information, signing communications on behalf of the Committee and representing the Committee before the Board and other governmental and quasi-governmental bodies, subject to the approval of the other Committee members.

**Rule 7:** In the absence or inability of the Chairman to preside over the meetings, the Vice-Chairman will perform such duties. If neither the Chairman nor Vice-Chairman is able to preside, the Committee shall select one of the members to act as Chairman pro-tem. The Chairman pro-tem shall have all the powers and duties of the Chairman during the absence of the Chairman.

**Rule 8:** The Chairman shall preserve order and decorum. The presence of a majority of the members will constitute a quorum, which will be necessary to conduct a meeting. The Committee shall operate under Roberts' Rules ("Rules") and the Chairman shall decide all questions of order (unless overridden by a majority of the Committee members present) consistent with such Rules.

#### **IV. ORDER AND SCHEDULING OF MEETINGS**

**Rule 9:** At a minimum, the Committee will meet on a quarterly basis. All meetings will be subject to the Ralph M. Brown Act. Whenever possible, quarterly meetings will be prescheduled at the beginning of each year to ensure attendance.

**Rule 10:** County staff will keep minutes of each meeting and offer them for Committee approval as the first item on the subsequent meeting agenda. Whenever possible, such minutes will be distributed to Committee members in draft form within a reasonable time after the meeting and in advance of the subsequent meeting.

#### **V. PUBLIC PARTICIPATION**

**Rule 11:** Every person addressing the Committee shall be limited in his remarks to three minutes, unless an extension is granted by the Chairman.

#### **VI. SCOPE OF COMMITTEE'S AUTHORITY AND OBJECTIVES**

**Rule 12:** The scope of Committee's authority will be determined based on the Board Resolution No. 95-271, dated April 25, 1995 as amended by any future Board action. The general authority is summarized as follows:

- a. To oversee the establishment and maintenance of the County's internal control structure primarily through oversight of the activities of the Internal Audit Department.
- b. To oversee the quality of financial reporting activities which portray the County's financial condition, results of operations, and plans and long-term commitments, primarily through oversight of the public accounting firm providing the external audit coverage of the County's consolidated financial statements. In addition, the Committee shall review audit results of County programs for which the Board has responsibility.

- c. To oversee and monitor County compliance with pertinent laws and regulations, applicable ethical standards, and conflicts of interest and fraud policies through review of the results of activities of the Internal Audit Department.
- d. To ensure that an external quality control review of the Internal Audit Department be conducted every three years by an organization not affiliated with the internal audit department in accordance with the United States General Accounting Office's Government Auditing Standards.
- e. To immediately notify the Board in writing should the Committee determine any significant or material irregularity exists in County operations.
- f. To present a summary of Committee activities and significant audit results to the Board through the distribution of the quarterly meeting material distributions packages. If the minutes were corrected or amended upon the regular order of business (see Rule 10), the minutes of each Committee meeting will be sent to the Board members once approved by the Committee.
- g. Such other duties as the Board shall prescribe from time to time.

**VII. STAFF SUPPORT FOR COMMITTEE**

**Rule 13:** To the extent available, County staff will provide technical and administrative support to the Committee, when requested.

**VIII. INDEMNIFICATION OF COMMITTEE MEMBERS BY COUNTY OF ORANGE**

**Rule 14:** The County of Orange will indemnify Committee members for their participation, decisions, or actions taken on behalf of the Audit Oversight Committee. Each Committee member should also familiarize him/herself with County of Orange Conflict of Interest Code and Gift Ban Ordinance requirements and file the appropriate annual certifications.

**IX. MISCELLANEOUS PROVISIONS**

**Rule 15:** These bylaws are subject to change by the Committee, with subsequent approval by the Board.

**Rule 16:** Copies of these bylaws may be obtained from the County of Orange free of charge.

References:

Board of Supervisors Minute Order S102B, 12/17/02  
 Board of Supervisors Resolution No. 95-271.  
 Board of Supervisors Minute Order 18444

IIA Article – Learning  
to Love the Scrutiny

Initiating a quality assessment can help an  
internal audit group come out on top.

**BY MICHAEL P. FABRIZIUS, CIA, CPA**  
VICE PRESIDENT OF INTERNAL AUDIT, BON SECOURS HEALTH SYSTEM

**RICHARD M. SERAFINI, CIA, CFE, CRP, CFSA**  
PARTNER, ENTERPRISE RISK SERVICES, DELOITTE

**M**ANY INTERNAL AUDIT DIRECTORS HAVE MIXED EMOTIONS ABOUT conducting an independent quality assessment (QA) (formerly known as a quality assurance review) once every five years, as mandated by The IIA's *International Standards for the Professional Practice of Internal Auditing (Standards)*. Although they love the idea of raising the bar on quality — especially since the U.S. Sarbanes-Oxley Act of 2002 upped the stakes — they often loathe the idea of inflicting a QA upon themselves. ■ So, why did the internal audit department at Bon Secours Health System, based in Marriottsville, Md., welcome the scrutiny of a QA even before it was a requirement of the *Standards*? No one had been questioning the department's practices. There were no burning issues or concerns regarding quality. Still, the internal auditors were determined to take

*Learning to*  
**LOVE** *the*  
**S**



# CRUTINY

ILLUSTRATIONS BY ED FOTHERINGHAM

a proactive approach and complete an independent review of the department. The QA became a catalyst to reinforce and strengthen the department's position within the organization. It also offered access to professional best practices that would help ensure that the department was state-of-the-art.

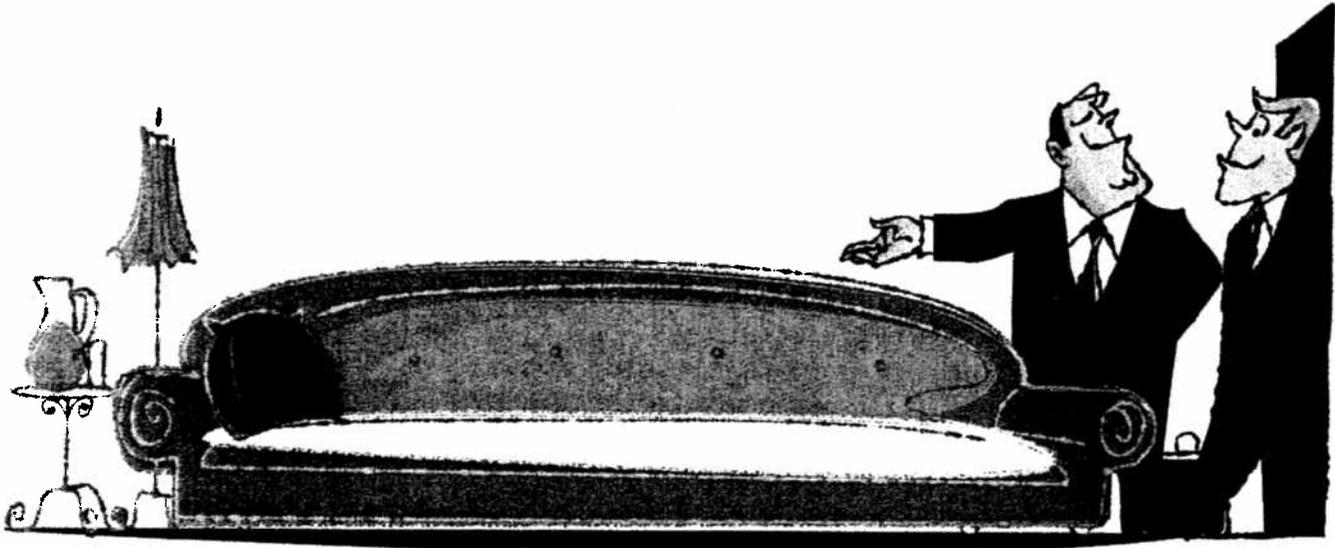
The QA process turned out to be empowering and surprisingly painless. The experience has strengthened the

time and effort involved with conducting an internal review and the expense of doing an external review. Additionally, three managers from the internal audit department attended The IIA's QA training courses to obtain the necessary skills and resources to optimize process effectiveness.

The internal review helped clarify the nuances of a QA and the multiple objectives that could be achieved. It revealed

company planning a QA should universally apply the concept.

The oversight committee helped develop the objectives for the review, the request for proposal (RFP), and the project timeline (see "Internal Audit Services QA Objectives and Schedule, page 41), and also assisted with selecting the service provider. The committee's involvement and oversight continued during the QA process and



internal audit program and helped raise the department's profile throughout the entire organization.

#### STARTING FROM WITHIN

Preparation, communication, and a positive attitude are the secrets of an enriching QA. At Bon Secours, preparations began with the decision to first include an *internally* conducted QA of the departmental objectives. The self-assessment helped prepare for and ultimately get the most value from an externally conducted QA.

A formal internal review is not always necessary before undergoing an external QA. In some cases, the results of the external review are needed to provide the framework for an ongoing quality control program that gets implemented internally. The key is doing what it takes to be prepared and to make the process as effective as possible.

Bon Secours' preparation included educating senior management and the audit committee on the concept of a QA, which in turn helped justify the

that, in addition to assessing technical compliance with the *Standards*, a QA would provide important information on benchmarking and best practices.

When the time came for the external review, the internal audit department, management, and the board knew exactly what to expect. Perhaps more importantly, the internal audit team faced the process with confidence. Everyone was hungry for a fresh perspective, rather than fearing what the QA might reveal.

#### INVOLVING SENIOR MANAGEMENT

Upon launching the external review, Bon Secours formed a QA oversight committee that included the chief financial officer, chief legal officer, and a member of the audit committee. Having total buy-in and direct involvement from these players was critical to the project's success. The appropriate people to involve in an oversight committee will vary from company to company, depending on the culture and the way management is organized. However, any

through the final report to the audit committee.

The oversight committee provided much more than a "rubber stamp." The committee's advice and counsel during the QA was invaluable. Its interactions with the service provider also gave executives increased respect for the internal audit function.

#### SELECTING A PROVIDER

Bon Secours issued formal RFPs to four providers. Based on a model provided by The IIA, the RFP was a critical document in communicating expectations to potential service providers (see "Sample Request for Proposal," page 42).

Each provider had an opportunity to learn as much as possible about the company and the internal audit function through the Bon Secours annual internal audit plan, which was an attachment to the RFP. The plan is a comprehensive document that includes internal auditing's scheduled audits, charter, organizational chart, annual budget, and staff background and credentials. Providing

this level of detail ensured that all proposals were well-founded.

From the proposals the oversight committee received, it narrowed the field and interviewed two firms. One outlier was eliminated based on price. Another firm seemed more interested in promoting its marketing concept for a review rather than providing the fundamentals of what was needed. The committee ultimately selected Deloitte

Bon Secours collaborated extensively on the specific elements of the assessment. They discussed in detail the areas of the internal audit process that would be reviewed and the Bon Secours executives who would be interviewed. Both sides also worked together to develop a detailed schedule for the interviews and delivery of the final reports so that the timing would be carefully coordinated. Very little was left uncovered.

interviews with nearly 30 managers, executives, and audit committee members.

Initially, the number of interviews planned seemed high. However, the decentralized nature of the Bon Secours organization made it important to involve all levels, up through the audit committee chairs and the chairman of the board. The purview of the review was important to help understand the organization's structure and culture.

In addition to the interviews, the review included an assessment of:

- The scope of the internal audit plan.
- Individual audits.
- Policies and procedures.
- Governance support.
- Documentation of meetings and audit results.
- Ongoing communication and reporting.
- The internal audit department charter.
- The audit committee charter.
- Human resource management.
- Staff turnover.
- Training.

Throughout the assessment, the QA team reported its progress weekly, which was vital to ensuring a smooth process. Ongoing communications helped everyone stay on top of the progress and carefully manage any developments. In addition, having a detailed plan with clear deliverables, clearly defined roles

### The QA provided a new comfort level to executive management and the audit committee about the audit approach and the way the function is managed.

to conduct the QA, based on the firm's qualities and experience.

#### LEAVING NOTHING TO CHANCE

The Deloitte proposal communicated the scope and objectives of the QA. However, before beginning the process, Deloitte and

With the number of people at Bon Secours involved in the QA, it was critical to keep the process carefully orchestrated. Detailed communications were sent to all involved so they would know what to expect and the process could unfold smoothly. The QA ultimately included

## Internal Audit Services QA Objectives and Schedule

**OBJECTIVE:** Obtain an independent, external review of the Internal Audit Service Department to evaluate compliance with The IIA's *International Standards for the Professional Practice of Internal Auditing* and to provide benchmarking and best practice information.

DATE	ACTIVITY
1. January 2, 200x	Send request for proposal (RFP) to group of independent providers.
2. January 20, 200x	Responses to RFP due.
3. February 1, 200x	QA oversight committee selects provider.
4. March 1, 200x	Independent provider commences review.
5. March 28, 200x	Independent provider completes review.
6. April 3, 200x	Closing meeting of independent provider with QA oversight committee.
7. April 28, 200x	Draft report completed and reviewed with chief executive officer and QA oversight committee.
8. May 15, 200x	Final written report received.
9. June 10, 200x	Report presented to audit committee by independent service provider.
10. June 11, 200x	Summary report presented to board of directors by the audit committee chair.
11. June 12, 200x	Internal auditing communicates summarized QA results to internal participants in the process.

# Sample Request for Proposal

Ms. XXX  
c/o XYZ Assurance Firm  
353 Royal Canal Boulevard  
Jacksonville, UT XXXXX

January 2, 200x

Dear Ms. XXX:

Request for Proposal (RFP): Quality Assessment (QA), Amalgamated Manufacturing Inc. Internal Audit Services

**BACKGROUND** Amalgamated, a public company, manufactures and markets specialty medical surgical devices. Manufacturing facilities are located in three mid-Atlantic states. Distribution facilities are located in Pennsylvania, Indiana, Louisiana, and Nevada, and sales are made through an outsourced sales organization. In the fiscal year ended Aug. 31, 200x, net revenues were approximately \$2.2 billion, and assets exceeded \$2.5 billion. Further Amalgamated information is available on our Web site.

Our Internal Audit Services Department consists of 12 professionals, including the vice president who reports to the president/chief executive officer (CEO). The vice president has access to the chairman of the board and the audit committee.

The audit function provides an independent appraisal of key financial and operational controls. The audit department also shares best practices that promote operational efficiencies and cost saving opportunities. Our audit plan is the result of an annual risk assessment. A copy of the approved FY200x Audit Plan is enclosed for your reference.

**REVIEW SERVICES TO BE PROVIDED** This RFP is for a QA of Internal Audit Services. The selected independent party will:

- Assess the efficiency and effectiveness of the internal audit department based on standards and benchmark information.
- Review the Amalgamated audit universe and the method followed for annual risk assessment leading to the audit plan.
- Evaluate the internal audit organizational structure, staffing, and internal audit approach.
- Determine how internal auditing is perceived through interviews and surveys with customers, including governance personnel.
- Examine internal audit techniques and methodology for testing controls.
- Identify ways to enhance internal audit policies and practices.
- Evaluate whether the department conforms to The IIA's *International Standards for the Professional Practice of Internal Auditing*.

The response to this RFP should identify the membership and credentials of the review team, including an organizational chart and the primary contact. The review team will include manufacturing internal audit experience.

The review will be confidential, with the results only provided to designated Amalgamated representatives. The independent party shall prepare a written report upon completion of the QA that is addressed to the CEO and the audit committee. A presentation on the QA results will be made to the audit committee.

**FEE ESTIMATE ASSUMPTIONS** Your fee estimate should incorporate the following assumptions:

- The project will be performed in March, with a preliminary report submitted by April 28, 200x, and the final report issued by May 15, 200x.
- Fees should include the cost, plus any estimated expenses. Please indicate the hourly rates for this review and the hourly rates for any additional services that might be contracted in CY200x.

**SUBMISSION AND SELECTION** Proposals for the QA must be submitted by Jan. 20, 200x. Internal auditing and our QA oversight committee, which is composed of our chief financial officer, chief legal officer, and a member of our audit committee, will review each proposal. Selection of the provider vendor is tentatively set for Feb. 1, 200x, after interviews of finalists. Additional information requests should be coordinated through my office at +1-410-555-3234.

**OTHER MATTERS** Please provide references. Also, limit the material provided in response to this RFP to 12 pages.

We are looking forward to working with you, and please do not hesitate to contact me if you have any additional questions.

Sincerely,

David P. Auditor  
Vice President, Internal Audit

Attachment  
cc: President/CEO  
QA Oversight Committee

and responsibilities, and well understood expectations by all stakeholders was key to the success of the QA.

#### RECOMMENDATIONS AND RESULTS

Within a month, Deloitte prepared a summary of the QA findings to discuss

support to increase the scope of auditing where needed.

- *Use presentation formats more for reporting.* Interviews with internal audit customers revealed a preference for more concise reporting, rather than a narrative format. Making this change also reduced the

audit QA program. Six months after issuing the formal report, a follow-up report was done on the progress made in implementing the recommendations. The internal audit plan now also includes yearly improvement goals. The internal auditors regularly survey the audit committee and senior manage-



**Company executives deal with internal auditing on a regular basis for legal and compliance issues, but sometimes fail to understand its role in the organization.**

with the oversight committee. The preparation had paid off, as there were few surprises — but a lot of value — in the results.

The QA helped address a few resource issues and gain support for more information technology auditing. It also revealed several best practices to adopt moving forward, such as how to improve communications and the management of audit committee meetings.

The final report, which was presented to the audit committee and other selected executives, included a few key recommendations:

- *Balance financial and operational audits in the annual audit plan.* The internal audit department had already begun to shift its focus to achieve a good balance between financial and operational audits. The QA confirmed the need to continue moving in this direction, with a recommendation to more consciously align audits with the company's strategic and operational needs.
- *Communicate gaps — as well as coverage — in audit plan.* By presenting the universe of potential audit areas in a matrix, the internal audit plan now illustrates the areas that are not audited, in addition to those that are. This approach gives a clearer picture of risk and has provided the

time spent drafting and redrafting reports that were presented in a narrative, rather than an executive summary, format.

The QA report also provided benchmarking on staffing and resource allocation, which revealed that the Bon Secours plan was largely on target. The report also confirmed that the internal audit department was in compliance with The IIA's *Standards*. Again, the internal QA conducted before the external review helped make the minor adjustments needed to make the external review most productive.

Another benefit of the QA was the level of education that it provided to key players at Bon Secours. For example, it had not been apparent how little the company's acting chief information officer understood about the internal audit process. He had been working with internal auditing, but only in a limited capacity. Company executives deal with internal auditing on a regular basis for legal and compliance issues, but sometimes fail to understand its role in the organization. The QA provided an excellent way to market internal auditing through the independent voice of the QA service provider.

#### AN ONGOING PROCESS

The external QA was a beginning — not an end — to the Bon Secours internal

audit QA program. Six months after issuing the formal report, a follow-up report was done on the progress made in implementing the recommendations. The internal audit plan now also includes yearly improvement goals. The internal auditors regularly survey the audit committee and senior manage-

#### BEING PROACTIVE

The QA provided a new comfort level to executive management and the audit committee about the audit approach and the way the internal audit function is managed. Through the discussions facilitated as part of the QA, executives now have new insights into the internal audit process and more respect for the entire function.

Taking a proactive approach can yield many benefits. If an internal audit function is operating efficiently and effectively, a QA serves as a valuable endorsement of the quality of those operations. Where improvements can be made, the QA aims to present practical, comprehensive solutions that can help the internal audit department increase its value to the organization, enhance its efficiency and effectiveness in meeting the needs of its key customers, and improve its planning for the future.

To comment on this article, e-mail the authors at [mfabrizius@theiia.org](mailto:mfabrizius@theiia.org).

**List of Suggested  
Peer Review  
Companies**

## **List of Possible Vendors**

Jefferson Wells, International (contract on hold pending AOC approval)  
Mr. James P. Jimenez, Director of Internal Audit Services  
(949) 885-1596

Price Waterhouse/Coopers  
Ms. Nancy Shelman, Peer Review Services  
(213) 217-3146

Deloitte & Touche  
(800) 871-2586

KPMG  
Orange County  
(714) 850 4300

### List of Vendors Selection from Publications:

National Association of Local Government Auditors  
(859) 276-0686

Audit Chiefs Association  
Monterey County, (831) 755-5441

Institute of Internal Auditors  
(407) 937-1100

American Institute of Certified Public Accountants  
(888) 777-7077

Compliance  
Evaluation Standards

**ATTRIBUTE STANDARDS**

**1000 – Purpose, Authority, and Responsibility**

The purpose, authority, and responsibility of the internal audit activity should be formally defined in a charter, consistent with the *Standards*, and approved by the board.

<b>Practice</b>	<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<p><b>1000.A1</b> - The nature of assurance services provided to the organization should be defined in the audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances should also be defined in the charter.</p>	X		<p>There is a current Audit Charter detailing the Nature, Objective and Scope, Responsibility and Authority, and Independence requirements of the Internal Audit Department. The BOS reviewed and approved this Charter on December 17, 2002.</p> <p>Also, Board Resolution 95-271 details the requirements of setting up and running the audit department. The Board Resolution covers the purpose, authority, and responsibility of the IAD.</p>
<p><b>1000.C1</b> - The nature of consulting services should be defined in the audit charter.</p>			<p>The Audit Charter states Internal Audit provides business and financial consulting services to the Board of Supervisors and County management to assist in the realization of their business goals and objectives. However, IAD accomplishes this by performing audits, and does not provide consulting engagements.</p>

**ATTRIBUTE STANDARDS**

**1100 – Independence and Objectivity**

The internal audit activity should be independent, and internal auditors should be objective in performing their work.

<b>Practice</b>	<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<p><b>1110 – Organizational Independence</b></p> <p>The chief audit executive should report to a level within the organization that allows the internal audit activity to fulfill its responsibilities.</p>	X		<p>IAD reports to the Board of Supervisors (BOS). In addition, the County has a Audit Oversight Committee (AOC) which provides oversight of IAD.</p>
<p><b>1110.A1</b> - The internal audit activity should be free from interference in determining the scope of internal auditing, performing work, and communicating results.</p>	X		<p>See 1110 above.</p>
<p><b>1120 – Individual Objectivity</b></p> <p>Internal auditors should have an impartial, unbiased attitude and avoid conflicts of interest.</p>	X		<p>There is an Independence Policy that all auditors signed upon the beginning of employment. In addition, all auditors are now required to sign annually an Independence Policy Statement.</p>
<p><b>1130 – Impairments to Independence or Objectivity</b></p> <p>If independence or objectivity is impaired in fact or appearance, the details of the impairment should be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.</p>	X		<p>An Independence Analysis was prepared in February 2003 in response to an effort by the Auditor-Controller to “reunify” Internal Audit with Auditor-Controller Office. A staff meeting was held to discuss various independence issues and all audit staff participated in preparing the analysis.</p>

<p><b>1130.A1</b> – Internal auditors should refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an <i>internal</i> auditor provides assurance services for an activity for which the <i>internal</i> auditor had responsibility within the previous year.</p>	<p>X</p>	<p>IAD staff does not participate in any operating responsibilities through rotation or on a temporary basis, nor does IAD allow operating staff to participate on audits on a rotation.</p> <p>Audit staff is required to disclose any potential conflicts or anything that might impair their objectivity on an audit.</p>
<p><b>1130.A2</b> – Assurance engagements for functions over which the chief audit executive has responsibility should be overseen by a party outside the internal audit activity.</p>	<p>X</p>	<p>The Director of IAD does not have responsibility for any other functions. Peer reviews of IAD are done by an external firm. In addition, the County external audit firm, performs procedures to evaluate the quality and effectiveness of the Internal Audit Department's work that significantly affects the nature, timing, and extent of their audit procedures.</p>
<p><b>1130.C1</b> - Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.</p>		<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>
<p><b>1130.C2</b> - If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure should be made to the engagement client prior to accepting the engagement.</p>		<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>

**ATTRIBUTE STANDARDS**

**1200 – Proficiency and Due Professional Care**

Engagements should be performed with proficiency and due professional care.

<b>Practice</b>	<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<p><b>1210 – Proficiency</b></p> <p>Internal auditors should possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.</p>	X		<p>Eleven of the 11 staff auditors have a college degree, 10 of the 11 have at least one professional designation, and with 6 having two or more. Two of the three managers have two designations; and one manager, the Deputy Director and the Director have four designations. Responsibilities are detailed in the Matrix of Responsibilities.</p> <p>Each staff member is a participant in at least one professional organization.</p>
<p><b>1210.A1</b> - The chief audit executive should obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills, or other competencies needed to perform all or part of the engagement.</p>	X		<p>The IAD obtains outside expertise when necessary to perform reviews when needed. Consultants were obtained to provide expertise in the following audits: Human Resources/Reclassification Review; CAPS Upgrade – Readiness Assessment; and A-C/CAPS – Payroll Risk Assessment.</p>
<p><b>1210.A2</b> – The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.</p>	X		<p>Four auditors (including Director and Deputy Director) are either a Certified Fraud Examiner (CFE) or Certified Fraud Specialist (CFS).</p> <p>IAD allows each auditor to obtain 60 hours of Continuing Professional Education (CPE) a year. The IAD has an annual budget of \$1,800 per staff member for training. This includes travel costs. In addition, the</p>

			County has an annual budget of \$2,000 per employee for training. The auditors each year take various CPE courses on fraud related subjects.
			SAS 82 – Fraud Auditing Standard is used in financial attestation audits (Annual Treasury Funds Audit - see
	X	1210.A3 – Internal auditors should have knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.	In 2002, all auditors studied and sat for the CISA exam. All auditors were allocated 200 hrs. for study and preparation for the CISA exam. Six out of the 10 auditors who sat for the exam passed on the first time. Currently, three auditors have the CISA Certification.
		1210.C1 - The chief audit executive should decline the consulting engagement or obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills, or other competencies needed to perform all or part of the engagement.	Not applicable – IAD does not perform consulting engagements. (See 1000.C1)
		<b>1220 – Due Professional Care</b>	
	X	Internal auditors should apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.	
		1220.A1 - The internal auditor should exercise due professional care by considering the: <ul style="list-style-type: none"> <li>• Extent of work needed to achieve the engagement's objectives.</li> <li>• Relative complexity, materiality, or significance of matters to which assurance procedures are applied.</li> </ul>	<ul style="list-style-type: none"> <li>• Auditors with the appropriate skills are assigned to each audit.</li> <li>• Planning meetings are held with audit staff to discuss engagement's objectives and entity's risks.</li> <li>• Utilize standardized audit programs.</li> <li>• Audit Managers approve scope of work and testing approaches before work is performed.</li> </ul>

<ul style="list-style-type: none"> <li>• Adequacy and effectiveness of risk management, control, and governance processes.</li> <li>• Probability of significant errors, irregularities, or noncompliance.</li> <li>• Cost of assurance in relation to potential benefits.</li> </ul>		<ul style="list-style-type: none"> <li>• In-charge auditors have periodic meetings with Audit Managers to discuss job status, findings, achievement of objectives, and any obstacles in achieving the objectives.</li> <li>• Time budgets are established and monitored. Time budgets provide audit staff with a perspective on the amount of time and emphasis that should be spent in reviewing a particular area (cost vs. benefit).</li> </ul>
<p><b>1220.A2</b> - In exercising due professional care the internal auditor should consider the use of computer-assisted audit tools and other data analysis techniques.</p>	X	<p>Auditors consider and use when appropriate computer-assisted audit tools and other analysis techniques.  Examples: ACL was used in the Treasury Quarterly Compliance Agreed Upon Procedures, H/CD DCR, and Purchasing Card DCR.</p> <p>Prepare a monthly report on Computer Assisted Audit Techniques for identifying duplicate payments, employee vendors, employee vendor address match, direct deposits, and deleted vendors.</p> <p>Auditors in the planning stage of the audit, apply significant effort into identifying all potential risks associated with the audited area. This is documented in various ways, e.g., planning memo, scope memo, understanding and assessment of internal controls, etc.  Example provided for Child Support Services DCR.</p> <p>See other examples provided under <b>1220.A1 and 1220.A2</b> above.</p>
<p><b>1220.A3</b> – The internal auditor should be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.</p>	X	

<p><b>1220.C1</b> - The internal auditor should exercise due professional care during a consulting engagement by considering the:</p> <ul style="list-style-type: none"> <li>• Needs and expectations of clients, including the nature, timing, and communication of engagement results.</li> <li>• Relative complexity and extent of work needed to achieve the engagement's objectives.</li> <li>• Cost of the consulting engagement in relation to potential benefits.</li> </ul>			<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>
<p><b>1230 – Continuing Professional Development</b></p> <p>Internal auditors should enhance their knowledge, skills, and other competencies through continuing professional development.</p>	<p>X</p>		<p>IAD allows each auditor to obtain 60 hours of Continuing Professional Education (CPE) a year. The IAD has an annual budget of \$1,800 per staff member for training. This includes travel costs. In addition, the County has an annual budget of \$2,000 per employee for training.</p> <p>CPE hours is tracked by each staff member.</p>

**ATTRIBUTE STANDARDS**

**1300 – Quality Assurance and Improvement Program**

The chief audit executive should develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity and continuously monitors its effectiveness. *This program includes periodic internal and external quality assessments and ongoing internal monitoring. Each part of the program* should be designed to help the internal auditing activity add value and improve the organization’s operations and to provide assurance that the internal audit activity is in conformity with the *Standards* and the *Code of Ethics*.

<b>Practice</b>		<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<b>1310 – Quality Program Assessments</b>				
<p>The internal audit activity should adopt a process to monitor and assess the overall effectiveness of the quality program. The process should include both internal and external assessments.</p> <p><b>1311 – Internal Assessments</b></p> <p>Internal assessments should include:</p> <ul style="list-style-type: none"> <li>• Ongoing reviews of the performance of the internal audit activity; and</li> <li>• Periodic reviews performed through self-assessment or by other persons within the organization, with knowledge of internal audit practices and the Standards.</li> </ul>		X		<p>An Audit Manager is assigned to oversee every audit.</p> <p>The Audit Manager prior to commencement of work approves audit program and audit scope. An Audit Checklist is prepared for each audit engagement and is reviewed by the Manager (checklist recently revised to reflect changes to IIA standards.) The Audit Manager reviews and initials the work papers.</p> <p>Starting in 2003, <i>Customer Survey of Audit Services</i> are sent out at the completion of assignments to obtain the client’s perspective of the audit. In 2004, we plan on formalizing this process and tabulating results to help identify where improvements can be made. CSA has a built-in evaluation and feedback process.</p>

<p><b>1312 – External Assessments</b></p> <p>External assessments, such as quality assurance reviews, should be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization.</p>	<p>X</p>	<p>Peer reviews of IAD are done by an external firm every three years. The last peer review was performed February 21, 2001 and covered audit work performed during 1999 and 2000. In addition, the County external audit firm performs procedures to evaluate the quality and effectiveness of the Internal Audit Department's work that significantly affects the nature, timing, and extent of their audit procedures.</p> <p>The external firm is copied as part of our audit report distribution. They periodically attend AOC meetings and receive a copy of our annual Audit Plan.</p>
<p><b>1320 – Reporting on the Quality Program</b></p> <p>The chief audit executive should communicate the results of external assessments to the board.</p>	<p>X</p>	<p>This is done during the Quarterly AOC meetings, and within our annual Business Plan, and by individual meeting between the IAD Director and BOS members. The results of the last peer review were communicated to the AOC, as will be the results of the current Peer Review upon completion.</p>
<p><b>1330 – Use of "Conducted in Accordance with the Standards"</b></p> <p>Internal auditors are encouraged to report that their activities are "conducted in accordance with the <i>International Standards for the Professional Practice of Internal Auditing</i>." However, internal auditors may use the statement only if assessments of the quality improvement program demonstrate that the internal audit activity is in compliance with the <i>Standards</i>.</p>		<p>Department Control Reviews (and certain other audits) state in the audit reports that "our review was made in accordance with professional standards by the Institute of Internal Auditors for the purpose of evaluating the adequacy of internal controls in the areas noted above."</p>
<p><b>1340 – Disclosure of Noncompliance</b></p> <p>Although the internal audit activity should achieve full compliance with the <i>Standards</i> and internal auditors with the <i>Code of Ethics</i>, there may be instances in which full compliance is not</p>	<p>X</p>	<p>Signed copies of the IIA Code of Ethics are retained in each employee's file. Additionally, a County of Orange Code of Ethics and Commitment to County Public Service is provided and each employee must make an oral Oath of Allegiance to comply with this</p>

<p>achieved. When noncompliance impacts the overall scope or operation of the internal audit activity, disclosure should be made to senior management and the board.</p>			<p>code. Also, each employee has signed an Information Technology Usage Policy. Reviewed copies of the signed Code of Ethics and Information Technology Usage Policy for each employee compiled in the self-review performed by IAD.</p>

## PERFORMANCE STANDARDS

### 2000 – Managing the Internal Audit Activity

The chief audit executive should effectively manage the internal audit activity to ensure it adds value to the organization.

Practice	Yes	No	Comments (note source of info., etc.)
<p><b>2010 – Planning</b></p> <p>The chief audit executive should establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.</p> <p><b>2010.A1</b> - The internal audit activity's plan of engagements should be based on a risk assessment, undertaken at least annually. The input of senior management and the board should be considered in this process.</p>	X		<p>In 2003, IAD significantly enhanced the annual risk assessment process for the 2004 Audit Plan by meeting with Executive Management in the departments to discuss their operating environments and areas of importance and concern. In addition, we expanded the risk assessment to include an inventory and assessment of key information systems used by the departments.</p>
<p><b>2010.C1</b> - The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Those engagements that have been accepted should be included in the plan.</p>			<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>

<p><b>2020 – Communication and Approval</b></p> <p>The chief audit executive should communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and to the board for review and approval. The chief audit executive should also communicate the impact of resource limitations.</p>	<p>X</p>	<p>The Director of IAD reports to the BOS and holds monthly meetings with each Board member. Also, the Board Chairman and Vice Chairman are members of the AOC. (See 1110)</p> <p>The Director of IAD is present at the quarterly AOC meetings. Also, all final audit reports are provided to all members of the BOS and AOC. Per the AOC Administrative Procedure memo dated May 22, 1996 and revised March 1, 2000.</p>
<p><b>2030 – Resource Management</b></p> <p>The chief audit executive should ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.</p>	<p>X</p>	<p>There is a comprehensive annual Audit Plan document prepared each year detailing the planned activities for the year. In addition, there is an annual Business Plan document detailing the staffing, budget and financial needs of IAD. Each of these items is provided to the AOC for review and the BOS for review and approval. Also, at each AOC meeting a quarterly Status Report of audit activity is provided to the AOC members.</p>
<p><b>2040 – Policies and Procedures</b></p> <p>The chief audit executive should establish policies and procedures to guide the internal audit activity.</p>	<p>X</p>	<p>Policies and procedures (P&amp;P) in substance exist for conducting audits and managing the department. P&amp;P for conducting the audit include: the professional standards, e.g., AICPA, IIA, GAO, etc., work paper standards, e.g., audit programs, and reporting standards. P&amp;P for Administrative management of the department is in various places on the IAD server.</p>
<p><b>2050 – Coordination</b></p> <p>The chief audit executive should share information and coordinate activities with other internal and external providers of relevant assurance and consulting services to ensure proper coverage and minimize duplication of efforts.</p>	<p>X</p>	<p>IAD provides a copy of their Audit Plan to the external auditors. In addition, IAD monitors for the County all external audit activity and prepares a quarterly status report of External Audit Activity, which is presented at each quarterly AOC meeting.</p>

<p><b>2060 – Reporting to the Board and Senior Management</b></p> <p>The chief audit executive should report periodically to the board and senior management on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting should also include significant risk exposures and control issues, corporate governance issues, and other matters needed or requested by the board and senior management.</p>	<p>X</p>		<p>See 2020 above.</p>
---	----------	--	------------------------

**PERFORMANCE STANDARDS**

**2100 – Nature of Work**

The internal audit activity should evaluate and contribute to the improvement of risk management, control, and governance *processes using a systematic and disciplined approach.*

<b>Practice</b>		<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<b>2110 – Risk Management</b>				
The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.				
<p><b>2110.A1</b> - The internal audit activity should monitor and evaluate the effectiveness of the organization's risk management system.</p>		X		Depending upon the type and scope of audit, e.g., Attestation Services & Mandates, IT, DCRs, CSA and Compliance risks are identified along with determining whether adequate controls are in place to address the risks.
<p><b>2110.A2</b> - The internal audit activity should evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the</p> <ul style="list-style-type: none"> <li>• Reliability and integrity of financial and operational information.</li> <li>• Effectiveness and efficiency of operations.</li> <li>• Safeguarding of assets.</li> <li>• Compliance with laws, regulations, and contracts.</li> </ul>		X		Depending upon the type and scope of audit, e.g., Attestation Services & Mandates, IT, DCRs, CSA and Compliance risks are identified along with determining whether adequate controls are in place to address the risks. Effectiveness and efficiency of County operations are addressed by conducting Control Self Assessment (CSA) workshops.

<p><b>2110.C1</b> - During consulting engagements, internal auditors should address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.</p>			<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>
<p><b>2110.C2</b> – Internal auditors should incorporate knowledge of risks gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization.</p>			<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>
<p><b>2120 – Control</b></p> <p>The internal audit activity should assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.</p>			
<p><b>2120.A1</b> - Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization's governance, operations, and information systems. This should include:</p> <ul style="list-style-type: none"> <li>• Reliability and integrity of financial and operational information.</li> <li>• Effectiveness and efficiency of operations.</li> <li>• Safeguarding of assets.</li> <li>• Compliance with laws, regulations, and contracts</li> </ul>	<p>X</p>		<p>Depending upon the type and scope of audit, e.g., Attestation Services &amp; Mandates, IT, DCRs, CSA and Compliance risks are identified along with determining whether adequate controls are in place to address the risks. Effectiveness and efficiency of County operations are addressed by conducting Control Self Assessment (CSA) workshops.</p>
<p><b>2120.A2</b> - Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization.</p>	<p>X</p>		<p>Effectiveness and efficiency of County operations are addressed by conducting Control Self Assessment (CSA) workshops.</p>

<p><b>2120.A3</b> - Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.</p>	<p>X</p>	<p>Effectiveness and efficiency of County operations are addressed by conducting Control Self Assessment (CSA) workshops.</p>
<p><b>2120.A4</b> - Adequate criteria are needed to evaluate controls. Internal auditors should ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors should use such criteria in their evaluation. If inadequate, internal auditors should work with management to develop appropriate evaluation criteria.</p>	<p>X</p>	<p>Auditors use the professional standards (AICPA, GAO, etc.), Internal Control Questionnaires (ICQs), and audit experience to establish criteria to evaluate controls. In addition, when conducting CSA workshops, IAD facilitates discussions with the participants regarding Setting Team Objectives, Planning &amp; Risk Assessment, Control Activities, and Monitoring.</p>
<p><b>2120.C1</b> - During consulting engagements, internal auditors should address controls consistent with the engagement's objectives and be alert to the existence of any significant control weaknesses.</p>		<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>
<p><b>2120.C2</b> – Internal auditors should incorporate knowledge of controls gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization.</p>		<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>

<p><b>2130 – Governance</b></p> <p>The internal audit activity should assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:</p> <ul style="list-style-type: none"> <li>• Promoting appropriate ethics and values within the organization.</li> <li>• Ensuring effective organizational performance management and accountability.</li> <li>• Effectively communicating risk and control information to appropriate areas of the organization.</li> <li>• Effectively coordinating the activities of and communicating information among the board, external and internal auditors and management.</li> </ul>	<p>X</p>	<p>Depending upon the type and scope of audit, e.g., Attestation Services &amp; Mandates, IT, DCRs, CSA and Compliance risks are identified along with determining whether adequate controls are in place to address the risks. Effectiveness and efficiency of County operations are addressed by conducting Control Self Assessment (CSA) workshops. Also, IAD in conducting CSA workshops facilitates discussions regarding planning and risk assessment, and values and ethics.</p>
<p><b>2130.A1</b> – The internal audit activity should evaluate the design, implementation, and effectiveness of the organization’s ethics-related objectives, programs and activities.</p>	<p>X</p>	<p>See 2130 above.</p>
<p><b>2130.C1</b> – Consulting engagement objectives should be consistent with the overall values and goals of the organization.</p>		<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>

**PERFORMANCE STANDARDS**

**2200 – Engagement Planning**

Internal auditors should develop and record a plan for each engagement, including the scope, objectives, timing and resource allocations.

<b>Practice</b>	<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<p><b>2201 - Planning Considerations</b></p> <p>In planning the engagement, internal auditors should consider:</p> <ul style="list-style-type: none"> <li>• The objectives of the activity being reviewed and the means by which the activity controls its performance.</li> <li>• The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.</li> <li>• The adequacy and effectiveness of the activity's risk management and control systems compared to a relevant control framework or model.</li> <li>• The opportunities for making significant improvements to the activity's risk management and control systems.</li> </ul>	<p>X</p>		<p>An audit program is prepared for each audit, which is approved by the Manager. Any changes to the audit program are reviewed and approved.</p> <p>Within the planning phase of the audit, an Estimated Budget, Planning Meeting with Manager, Pre-Audit Meeting, Engagement Letter, Entrance Letter, Entrance Conference Memo, Request for Information, Listing of Contacts, Request for Special Access (if necessary) and a Management Representation Letter are completed. Depending on the complexity of the audit, several of these items may be combined into one document. Additionally, there are checklists for audit planning and program development.</p> <p>Detailed timekeeping records are completed weekly for each audit.</p> <p>Final Scope document documents that all areas of risks were discussed.</p> <p>During the planning stage of the audit, risks associated with the audited area are identified.</p>

<p><b>2201.A1</b> – When planning an engagement for parties outside the organization, internal auditors should establish a written understanding with them about objectives, scope, respective responsibilities and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.</p>		X	See 2201 above.
<p><b>2201.C1</b> - Internal auditors should establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding should be documented.</p>			Not applicable – IAD does not perform consulting engagements. (See 1000.C1)
<p><b>2210 – Engagement Objectives</b></p> <p>Objectives should be established for each engagement.</p>			
<p><b>2210.A1</b> – Internal auditors should conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives should reflect the results of this assessment.</p>		X	See 2201 above.
<p><b>2210.A2</b> - The internal auditor should consider the probability of significant errors, irregularities, noncompliance, and other exposures when developing the engagement objectives.</p>		X	See 2201 above.
<p><b>2210.C1</b> – Consulting engagement objectives should address risks, controls, and governance processes to the extent agreed upon with the client.</p>			Not applicable – IAD does not perform consulting engagements. (See 1000.C1)
<p><b>2220 – Engagement Scope</b></p> <p>The established scope should be sufficient to satisfy the objectives of</p>			

the engagement.				
<b>2220.A1</b> - The scope of the engagement should include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.	X			See 2201 above.
<b>2220.A2</b> - If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.				Not applicable – IAD does not perform consulting engagements. (See 1000.C1)
<b>2220.C1</b> – In performing consulting engagements, internal auditors should ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations should be discussed with the client to determine whether to continue with the engagement.				Not applicable – IAD does not perform consulting engagements. (See 1000.C1)
<b>2230 – Engagement Resource Allocation</b>				
Internal auditors should determine appropriate resources to achieve engagement objectives. Staffing should be based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.	X			See 2201 above.
<b>2240 – Engagement Work Program</b>				
Internal auditors should develop work programs that achieve the engagement objectives. These work programs should be recorded.	X			See 2201 above.

<p><b>2240.A1</b> - Work programs should establish the procedures for identifying, analyzing, evaluating, and recording information during the engagement. The work program should be approved prior to <i>its implementation</i>, and any adjustments approved promptly.</p>	<p>X</p>	<p>See 2201 above.</p>
<p><b>2240.C1</b> - Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.</p>		<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>

**PERFORMANCE STANDARDS**

**2300 – Performing the Engagement**

Internal auditors should identify, analyze, evaluate, and record sufficient information to achieve the engagement's objectives.

<b>Practice</b>	<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<p><b>2310 – Identifying Information</b></p> <p>Internal auditors should identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.</p>	<p>X</p>		<p>Audit programs and working papers are cross-referenced to support results indicated.</p> <p>Audit programs and working papers are reviewed which is evidenced by initials and dates.</p> <p>The AIC prepares detailed review notes for the audit staff. Also, the Audit Manager reviews the AIC work papers and provides review notes.</p> <p>Findings are documented on Finding Abstracts and cross-referenced to the work papers.</p> <p>Audit work papers indicate what was reviewed/tested: systems, risks, internal controls, documents, etc.</p> <p>Auditors obtain the necessary information to achieve the audit objectives.</p> <p>Auditors have the necessary skills to prepare work papers that clearly support conclusions and the audit</p>

			<p>testing.</p> <p>The scope stated in the audit program is effective in achieving the audit objectives and in reaching a concise audit opinion.</p> <p>Auditors are skilled in utilizing techniques such as interviews, questionnaires, flowcharts, and sampling.</p> <p>Auditors perform the tests needed to meet the object objectives, and the sample size and methodology is appropriate to achieve an audit opinion.</p>
<b>2320 – Analysis and Evaluation</b>			See 2310 above.
Internal auditors should base conclusions and engagement results on appropriate analyses and evaluations.	X		
<b>2330 – Recording Information</b>			See 2310 above.
Internal auditors should record relevant information to support the conclusions and engagement results.	X		
<b>2330.A1</b> - The chief audit executive should control access to engagement records. The chief audit executive should obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.	X		IAD maintains all audit work paper files. Access to files is granted by IAD, however, all audit work paper files are public documents and can be obtained. IAD allows the work paper files to be reviewed in IAD's office, and will make copies of work papers for a fee.
<b>2330.A2</b> - The chief audit executive should develop retention requirements for engagement records. These retention requirements should be consistent with the organization's guidelines and any pertinent regulatory or other requirements.	X		IAD Audit Manual Chapter 7 – Work paper Standards and Audit Evidence, Section 7.12 discusses the retention of work papers. The policy states that once a subsequent audit has been completed, auditors should make a determination, approved by the Director, as to whether the work papers should be retained or

			<p>destroyed. As a practice, IAD has been maintaining work papers for 10 years.</p>
<p><b>2330.C1</b> - The chief audit executive should develop policies governing the custody and retention of engagement records, as well as their release to internal and external parties. These policies should be consistent with the organization's guidelines and any pertinent regulatory or other requirements.</p>			<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>
<p><b>2340 – Engagement Supervision</b> Engagements should be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.</p>	<p>X</p>		<p>Audit programs and working papers are reviewed which is evidenced by initials and dates.  The AIC prepares detailed review notes for the audit staff. Also, the Audit Manager reviews the AIC work papers and provides review notes. The Deputy Director on a case-by-case basis will also review work papers.  The Audit Manager and Deputy Director of IAD reviews the audit report drafts and final reports.</p>

**PERFORMANCE STANDARDS**

**2400 – Communicating Results**

Internal auditors should communicate the engagement results.

<b>Practice</b>	<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<p><b>2410 – Criteria for Communicating</b></p> <p>Communications should include the engagement’s objectives and scope as well as applicable conclusions, recommendations, and action plans.</p>	X		<p>Final audit reports for the audits use a standard format that ensures background; objective, scope and conclusions are discussed in the Overview section of the report. Findings, Recommendations and Management Responses are included in their own section of the report.</p>
<p><b>2410.A1</b> – Final communication of engagement results should, where appropriate, contain the internal auditor’s overall opinion and or conclusions.</p>	X		<p>See 2410 above.</p>
<p><b>2410.A2</b> – Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.</p>		X	<p>The Conclusion section discusses the overall performance of the auditee. IAD as a matter of practice does not make “positive findings,” however, IAD does acknowledge assistance received and satisfactory performance.</p>
<p><b>2410.A3</b> – When releasing engagement results to parties outside the organization, the communication should include limitations on distribution and use of the results.</p>	X		<p>IAD states on their reports as needed the limitations on distribution. Example: Audit of the District Attorney Spousal Abuser Prosecution Program for the year ended June 30, 2003 (Audit No. 2311) contains the following statement: “This report is intended for the information of the management of the County of Orange District Attorney and the California Department of Justice and should not be used for any</p>

			other purpose. However, this report is a matter of public record and its distribution is not limited.” Not applicable – IAD does not perform consulting engagements. (See 1000.C1)
<b>2410.C1</b> – Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.			
<b>2420 – Quality of Communications</b> Communications should be accurate, objective, clear, concise, constructive, complete, and timely.	X		The AIC cross-references the draft audit report to the audit work papers. The Audit Manager reviews the draft audit report and compares the findings to the Finding Abstracts and work papers. The Deputy Director reviews and approves the draft and final audit report. A copy of the draft audit report is also provided to the auditee for their review of accuracy and tone.
<b>2421 – Errors and Omissions</b> If a final communication contains a significant error or omission, the chief audit executive should communicate corrected information to all <i>parties</i> who received the original communication.	X		IAD has not issued any audit reports that contain any significant errors. However, if this were to occur, IAD would communicate the corrected information to all parties who received the original audit report.
<b>2430 – Engagement Disclosure of Noncompliance with the Standards</b> When noncompliance with the <i>Standards</i> impacts a specific engagement, communication of the results should disclose the: <ul style="list-style-type: none"> <li>• <i>Standard(s)</i> with which full compliance was not achieved,</li> <li>• Reason(s) for noncompliance, and</li> <li>• Impact of noncompliance on the engagement.</li> </ul>	X		IAD only states in their audit reports compliance with Standards, e.g., AICPA, IIA, GAO, when those standards have been followed. However, if a Standard was not followed this would be stated. Example: Report of Review of the Statement of Assets Held by the County Treasury as of September 30, 2003 (File No. 2307) we state that “Based on our review, with the exception of the matter described in the following paragraph, we are not aware of any material modifications that should be made to the accompanying financial statement prepared on the cash basis, as modified, which is a comprehensive basis of

		<p>accounting other than United States generally accepted accounting principles. “</p> <p>“Management has elected to omit all disclosures ordinarily included in a financial statement prepared on the cash basis, as modified. If the omitted disclosures were included in the financial statement, they might influence the user’s conclusions about the Treasurer’s assets. Accordingly, this financial statement is not designed for those who are not informed about such matters.”</p>
<p><b>2440 – Disseminating Results</b></p> <p>The chief audit executive should communicate results to the appropriate <i>parties</i>.</p>	<p>X</p>	<p>IAD has established a standard distribution list which includes: Members, Board of Supervisors, Members, Audit Oversight Committee, James Ruth, County Executive Officer, David Sundstrom, Auditor-Controller. In addition, the department head of the department being audited receives a copy of the report along with applicable management within the department.</p>
<p><b>2440.A1</b> - The chief audit executive is responsible for communicating the final results to <i>parties</i> who can ensure that the results are given due consideration.</p> <p><b>2440.A2</b> - If not otherwise mandated by legal, statutory or regulatory requirements, prior to releasing results to parties outside the organization, the chief audit executive should:</p> <ul style="list-style-type: none"> <li>• Assess the potential risk to the organization.</li> <li>• Consult with senior management and/or legal counsel as appropriate</li> <li>• Control dissemination by restricting the use</li> </ul>	<p>X</p>	<p>The Audit Manager, Deputy Director, Director, and Executive Secretary reviews the reports for proper distribution.</p>

<p>of the results.</p>		
<p><b>2440.C1</b> - The chief audit executive is responsible for communicating the final results of consulting engagements to clients.</p>		<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>
<p><b>2440.C2</b> – During consulting engagements, risk management, control, and governance issues may be identified. Whenever these issues are significant to the organization, they should be communicated to senior management and the board.</p>		<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>

**PERFORMANCE STANDARDS**

**2500 – Monitoring Progress**

The chief audit executive should establish and maintain a system to monitor the disposition of results communicated to management.

<b>Practice</b>	<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
<p><b>2500.A1</b> - The chief audit executive should establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.</p>	<p>X</p>		<p>IAD reviews all previously issued Findings and Recommendations during the subsequent audit. Additionally, if Findings and Recommendations are cleared while the audit is still being performed, IAD documents that corrective action was taken while on-site.</p> <p>If IAD and the auditee agree to disagree on a finding and recommendation, this will be documented in the audit report and brought to the attention of the Audit Oversight Committee for resolution.</p>
<p><b>2500.C1</b> – The internal audit activity should monitor the disposition of results of consulting engagements to the extent agreed upon with the client.</p>			<p>Not applicable – IAD does not perform consulting engagements. (See 1000.C1)</p>

**PERFORMANCE STANDARDS**

**2600 – Resolution of Management’s Acceptance of Risks**

<b>Practice</b>	<b>Yes</b>	<b>No</b>	<b>Comments (note source of info., etc.)</b>
When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive should discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive and senior management should report the matter to the board for resolution.	X		If IAD and the auditee agree to disagree on a finding and recommendation, this will be documented in the audit report and brought to the attention of the Audit Oversight Committee for resolution.



February 21, 2001

Peter Hughes, PhD  
Director, Internal Audit  
County of Orange  
400 Civic Center Drive West  
Building 12, Room 232  
Santa Ana, CA 92701

Dear Dr. Hughes,

At your request, we have conducted a quality assurance review of the work of your internal audit department. We reviewed for compliance with The Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing*, and based our review on the Association of College and University Auditor's *Quality Assurance Review Handbook*. Additionally, we ensured the Quality Assurance Review addressed all aspects of the *Government Auditing Standards* discussed in *The Yellow Book*.

Persons independent of your internal audit department performed the review and covered audit work performed during 1999 and 2000. The scope of the review was restricted to reviewing selected documents, reviewing the workpapers of a sample of audit projects, interviewing key personnel and reviewing the documents compiled during the Self Review completed by the internal audit department.

Based on the scope of our review, we determined that, the work of the internal audit department did comply with IIA *Standards* during the period under review. Additional information is provided in the attached report.

We appreciate the cooperation and assistance provided to us throughout the course of our review. All individuals interviewed offered candid and constructive comments. We will be pleased to review any of the information in the attached report with you at your convenience.

Sincerely,



Nancy Johnson  
Director Of Audit  
Jefferson Wells International

Attachment

## INTRODUCTION

The *Standards for the Professional Practice of Internal Auditing (Standards)*, issued by The Institute of Internal Auditors (IIA), require internal audit departments to develop and maintain a quality assurance program to ensure the quality and credibility of their work. According to the IIA, a comprehensive quality assurance program includes the following elements:

- Ongoing supervision of internal audits
- Periodic internal reviews of the work of the internal audit department.
- Periodic external reviews or peer reviews of the work of the internal audit department.

This report presents the results of a peer review conducted February 9 through February 16, 2001. Nancy Johnson and R. Matthew Byers of Jefferson Wells International performed the review.

## OBJECTIVES

The primary objective of this review was to determine whether the internal audit department was in compliance with the *Standards* established by the IIA. A secondary objective was to foster the sharing of experiences, ideas, and approaches with directors of other internal audit departments, in order to provide additional recommendations for improving the internal audit function.

## SCOPE

The scope included:

- Reviewing the general information and documents gathered by the internal audit department during the performance of their self-review.
- Reviewing selected audits and control self-assessments performed during the 2000 audit year.
- Interviewing key management and personnel of the internal audit department.

<sup>1</sup> Taken from the *Standards for the Professional Practice of Internal Auditing* as published by the Institute of Internal Auditors.

## CONCLUSIONS

Our overall evaluation of the internal audit department is that it did comply with the IIA *Standards* for the period under review. This overall evaluation was derived from separate evaluations for each of the five general and 25 specific standards that comprise the IIA *Standards*, and was limited to the scope of our review.

## OBSERVATIONS AND RECOMMENDATIONS

Following are the observations of the review team as they relate to the five general IIA *Standards: Independence, Professional Proficiency, Scope of Work, Performance of Audit Work, and Management of the Internal Auditing Department*. For each standard, the review team identified the conditions observed and, where appropriate, made recommendations for enhancing the efficiency and effectiveness of operations.

### 100 **INDEPENDENCE** – INTERNAL AUDITORS SHOULD BE INDEPENDENT OF THE ACTIVITIES THEY AUDIT<sup>1</sup>.

**Observations:** The internal audit department demonstrates independence from the activities that they audit. Their reporting relationship to the Board of Supervisors enables them to carry out their work responsibilities freely and objectively and enables them to render impartial and unbiased judgements and conclusions.

However, the Audit Charter of the internal audit department has not been reviewed and approved by the Board of Supervisors or the Audit Oversight Committee. The internal audit department was formed based upon the Board Resolution 95-271, which addresses the requirements of the *Standards*.

Also, internal audit department management does not discuss independence and objectivity on a regular basis with the staff auditors. Reliance is placed on the initial independence and objectivity statement that all new auditors sign upon accepting employment and on the auditor's judgment to disclose any potential conflicts of interest.

**Recommendations:** We are recommending that the Audit Charter from 1997 in the Audit Manual be updated to include the new definition of internal audit provided by the IIA and the current goals and objectives of the internal audit department and presented to the Board of Supervisors and/or the Audit Oversight Committee for approval. This would assist in presenting the current goals and objectives of the internal audit department and document that the Board of Supervisors and the Audit Oversight Committee has agreed to the goals and objectives presented.

<sup>1</sup> Taken from the *Standards for the Professional Practice of Internal Auditing* as published by the Institute of Internal Auditors.

**Internal Audit Department's Response:** *We concur with this recommendation and will pursue updating our Audit Charter and having it approved by the Board of Supervisors and the Audit Oversight Committee. The deputy director of the department has taken the initiative of updating the Audit Charter to conform it to the new definitions provided by the IIA and have it approved by the Board of Supervisors and the Audit Oversight Committee by December 31, 2001. He will also include a section in next year's audit plan and will present and discuss the current goals and objectives of the internal audit department. We feel that keeping the Audit Charter in conformance with IIA guidelines and general in nature, while at the same time presenting and discussing goals and objectives annually in the audit plan will appropriately address the points raised in the above recommendation.*

We are recommending that the internal audit department add an item to the Staff section of the Audit Planning Checklist discussing potential conflicts of interest and/or bias. This would assist in maintaining objectivity in all audits performed.

**Internal Audit Department's Response:** *We concur and the deputy director will immediately implement this recommendation by adding this section to the planning checklist and begin including the revised checklist in all new audit initiatives.*

**200**    **PROFESSIONAL PROFICIENCY – INTERNAL AUDITS SHOULD BE PERFORMED WITH PROFICIENCY AND DUE PROFESSIONAL CARE**<sup>1</sup>.

**Observations:** The internal audit department demonstrates due professional care and audit proficiency in the audits they perform. They possess the necessary knowledge, professional skills, and recognized professional certifications to competently undertake their audit assignments. There are additional tools available that may assist the internal audit department in performing their audits.

**Recommendations:** We are recommending that the internal audit department begin utilizing the Audit Planning and Program Development Checklists on each audit performed. These checklists would assist in guiding the auditors through the planning and development stages of the audit without missing key audit steps.

We are also recommending that should the internal audit department decide to not utilize the Audit Planning checklist that they perform a documented Risk Assessment, detailing the development of the audit plan and program.

**Internal Audit Department's Response:** *We will implement the recommendation above by directing the Audit Managers to use the Audit Planning and Program Development Checklists on each new audit started.*

<sup>1</sup> Taken from the *Standards for the Professional Practice of Internal Auditing* as published by the Institute of Internal Auditors.

**300**    **SCOPE OF WORK** – THE SCOPE OF INTERNAL AUDITING SHOULD ENCOMPASS THE EXAMINATION AND EVALUATION OF THE ADEQUACY AND EFFECTIVENESS OF THE ORGANIZATION’S SYSTEM OF INTERNAL CONTROL AND THE QUALITY OF PERFORMANCE IN CARRYING OUT ASSIGNED RESPONSIBILITIES<sup>1</sup>.

**Observations:** The annual audit plan developed by the internal audit department in conformance with expectations provided by the Board of Supervisors and the Audit Oversight Committee encompasses the examination and evaluation of the adequacy and effectiveness of the County’s systems of internal control. The audit plan systematically addresses the major business functions with the greatest impact and importance to the County. The effectiveness and efficiency of audited entities and accomplishment of goals by audited entities are not included in standard audits, because these types of reviews are conducted by consultants engaged individually by the Departments in coordination with the CEO. This was a decision made by the Board of Supervisors and has been implemented into the standard audit plan of the internal audit department. These areas would be reviewed if requested specifically by management.

**Recommendations:** We are recommending that the Audit Charter and Audit Plan be updated to reflect that the internal audit department does not perform ‘efficiency and effectiveness’ or ‘validation of the measurement and tracking of goals and/or objectives’. This would document that the Board of Supervisors and the Audit Oversight Committee acknowledges and accepts that these areas are not going to be covered. Also, as discussed in section 100 above, this would clarify the current focus of the internal audit department.

We are recommending that the internal audit department begin utilizing the Segregation of Duties Matrix for all audits to provide additional support to their validation of appropriate segregation.

**Internal Audit Department’s Response:** *We concur and the deputy director will update the Audit Charter as previously discussed and he will also present and discuss the annual audit goals and objectives beginning with the next Audit Plan. This way the Audit Oversight Committee has annual visibility and awareness of the audit department’s goals and objectives as well as each audit scheduled.*

*We will also begin using the Segregation of Duties Matrix in all new audits started.*

**400**    **PERFORMANCE OF AUDIT WORK** – AUDIT WORK SHOULD INCLUDE PLANNING THE AUDIT, EXAMINING AND EVALUATING INFORMATION, COMMUNICATING RESULTS, AND FOLLOWING UP<sup>1</sup>.

<sup>1</sup> Taken from the *Standards for the Professional Practice of Internal Auditing* as published by the Institute of Internal Auditors.

**Observations:** The work performed by the internal audit department is clearly documented and includes all aspects discussed in the *Standards*. Their audits are well planned, supervised and properly staffed. Their audit objectives are achieved as evidenced by documentation and other support assembled in the working papers. The audit reports are balanced, objective and clear. The audit recommendations are well developed and would add value to the organization.

**Recommendations:** As discussed in section 200 above, we are recommending the internal audit department begin utilizing the Planning and Program Development Checklists during the planning phase of the audit to ensure all risk areas are covered and documented.

**Internal Audit Department's Response:** *We will immediately incorporate the Planning and Program Development Checklist in new audit initiatives. The audit managers were instructed accordingly.*

500 **MANAGEMENT OF THE INTERNAL AUDIT DEPARTMENT – THE DIRECTOR OF INTERNAL AUDITING SHOULD PROPERLY MANAGE THE INTERNAL AUDITING DEPARTMENT<sup>1</sup>.**

**Observations:** The Director properly manages the internal audit department. The responsibilities approved by the Board of Supervisors and the Audit Oversight Committee are accomplished in the annual audit plan. In addition, the Director manages the resources of the audit department efficiently and effectively demonstrated by completing last year's plan on time and on budget.

**Recommendations:** We are recommending that the internal audit department continue its efforts in compiling policies and procedures in an easy to use, easy to find, standard format for the audit staff.

**Internal Audit Department's Response:** *We will continue our efforts to incorporate and employ the Best Business Practices to the Internal Audit Department.*

## ACKNOWLEDGEMENTS

The team conducting this quality assurance review wishes to thank all internal audit personnel for their cooperation and assistance throughout the course of this review.

<sup>1</sup> Taken from the *Standards for the Professional Practice of Internal Auditing* as published by the Institute of Internal Auditors.

## **Scope of Review, Documents Reviewed and Employee's Interviewed**

The Peer Review performed by Jefferson Wells International during February 9 through February 16, 2001 covered the Internal Audit Departments performance during 1999 and 2000. The Peer Review relied upon workpapers compiled by the Internal Audit Department during their self-review completed in January 2001. The sample utilized during the Self-Review and Peer Review were:

IAD Self Review and Support for Peer Review for IIA Standards Section 100  
IAD Self Review and Support for Peer Review for IIA Standards Section 200  
IAD Self Review and Support for Peer Review for IIA Standards Section 300  
IAD Self Review and Support for Peer Review for IIA Standards Section 400  
IAD Self Review and Support for Peer Review for IIA Standards Section 500  
IAD Self Review Manual  
IAD Audit Manual  
Treasury Fund Audit – Financial Audit #2007 Q/E 09/30/00  
Integrated Waste Management – Departmental Control Review #1299 Y/E 03/31/00  
Tax Redemption Officer – Mandated Audit #0499 Y/E 10/31/99  
Public Administrator/Public Guardian – Control Self Assessment #2066 Y/E 09/30/00  
Orange County Public Library – Control Self Assessment #2002 January-March 2000

The sample utilized only during the Peer Review were:

Registration and Elections Department – Departmental Control Review #2030 Y/E  
05/31/00  
Treasurer SB866 Compliance Audit – Financial Audit #0999 Y/E 12/31/99  
Sheriff-Coroner Department – Control Self Assessment #99-20  
Interviews of: Peter Hughes, Director  
Eli Littner, Deputy Director  
Michael Goodwin, Audit Manager  
Alan Markum, Audit Manager  
Vangie Ortiz, Administrative Staff Analyst II  
Review of Employee Files

**100 INDEPENDENCE**

*“Internal auditors should be independent of the activities they audit.”*

<p><b>110 Organizational Status</b></p> <p><i>“The organizational status of the internal auditing department should be sufficient to permit the accomplishment of its audit responsibilities.”</i></p> <p>The essence of independence centers around the internal audit department having sufficient authority and support from management to be able to carry out its responsibilities.</p> <p>(A minimum of three of the following practices are suggested; especially effective practices are signified by a ★ )</p>			
<p><b>Practice</b></p>	<p><b>Yes</b></p>	<p><b>No</b></p>	<p><b>Comments (note source of info, etc.)</b></p>
<p>★ 1. Does the internal audit director report to an acceptable level -- such as the Board, President, or Chief Financial Officer -- who has sufficient authority to support the audit function and require appropriate action on audit recommendations?</p>	<p>Yes</p>		<p>Reports to the Board of Supervisors (BOS) and to the Audit Oversight Committee (AOC) according to the Organizational Chart.</p>
<p>2. Does the internal audit director have formal access to members of the board?</p>	<p>Yes</p>		<p>The Director of Audit has direct access to the BOS through Supervisor James W. Silva, as the representative to the BOS on the AOC.</p>
<p>★ 3. Does the internal audit director directly communicate with the Board (or Audit Committee) at least annually?</p>	<p>Yes</p>		<p>The Director of Audit is present at the quarterly AOC meetings as noted in the meeting minutes for each quarterly meeting in 2000. Also, all final reports of audit are provided to all members of the BOC, per the AOC Administrative</p>

			<p>4. Does the appointment or removal of the internal audit director require the concurrence of the Board?</p>	<p>Procedure memo dated May 22, 1996 and revised March 1, 2000.</p> <p>Item 5 of the Board Resolution indicates the AOC will select the Director with the final hiring decision made by the BOS. Item 9 of the Director's Contract indicates the BOS has the authority to terminate the Director's contract.</p>	<p>Yes</p>
<p>★</p>			<p>5. Is the purpose, authority, and responsibility of the internal audit department defined in a formal written and approved document (audit charter)?</p>	<p>There is an Audit Charter detailing the Nature, Objective and Scope, Responsibility and Authority, and Independence requirements of the Internal Audit Department. The BOS has not reviewed or approved this Charter; it is used as a guideline only. However, the Board Resolution 95-271 details the requirements of setting up and running the audit department. The Board Resolution covers the purpose, authority, and responsibility of the IAD, however it is not very specific as to the coverage. We are recommending that they update their Charter and obtain Board Approval.</p>	<p>Yes</p>
<p>★</p>			<p>6. Does the internal audit director submit the following items for approval by management and/or the Board on an ongoing regular basis?</p> <ul style="list-style-type: none"> <li>a. Audit Plan</li> <li>b. Staffing levels and needs.</li> <li>c. Budget and financial needs.</li> </ul>	<p>There is a comprehensive Audit Plan 2001 document detailing the planned activities the year, this is maintained on a rolling three year basis. There is a Business Plan 2001 document detailing the staffing, budget and financial needs</p>	<p>Yes</p>

			<p>★ 7. Does the internal audit director submit activity or status reports that highlight significant audit findings, recommendations, audit accomplishments, coverage, and status of the audit plan to management and/or the Board?</p>	<p>for 2001. Each of these items was provided to the BOS prior to final approval.</p>
<p>Yes</p>				<p>The Director provides quarterly status reports to the BOS and the AOC detailing status of audits. All final reports of audit, including all significant issues and resolutions, are provided to each member of the BOS and the AOC.</p>
<p><b>Reviewer's Notes</b></p>				
<p>a. The above practices are typically evidenced by an internal audit charter, organizational charts, board minutes, audit plans, and periodic activity reports, position descriptions, memorandums, and interviews.</p>				
<p><b>Conclusions</b></p>		<p><b>Yes</b></p>	<p><b>No</b></p>	<p><b>Comments</b></p>

THE MASTER AUDIT PROGRAM (MAP) – 100 INDEPENDENCE

<p>Has the internal audit department adopted three or more of the above practices</p>	<p>Yes</p>	<p>We are recommending that the Audit Charter in the Audit Manual from 1997 be reviewed, updated and presented to the BOS for approval. Also, the definition of Internal Auditing has been updated since this charter was written, so this should be considered. And, the Director has indicated that their audits do not consider the 'efficiency and effectiveness' aspect of COSO, this is left to the management team, however, the Charter, as written, indicates that this is one of the IAD functions.</p>
---	------------	---

<p><b>120 Objectivity</b></p> <p><i>“Internal auditors should be objective in performing audits.”</i></p> <p>The essence of this objective centers around the ability of each auditor to maintain an independent mental attitude that eliminates biases and conflicts of interest over operations being audited.</p> <p>(A minimum of two of the following practices are suggested; especially effective practices are signified by a ★.)</p>													
<p><b>Practice</b></p> <p>★ 1. Is the internal audit department free of operating responsibilities, which would thereby impair its ability, either in fact, or appearance, to objectively assess the operations being audited?</p> <p>If internal auditors have assumed operating responsibilities, are they of such a limited or isolated nature so as <b>not to impair</b> ones’ objectivity for the areas that have been or are supposed to be audited?</p>	<table border="1"> <thead> <tr> <th data-bbox="568 735 698 903">Yes</th> <th data-bbox="568 903 698 1071">No</th> <th data-bbox="568 1071 698 1845">Comments (note source of info, etc.)</th> </tr> </thead> <tbody> <tr> <td data-bbox="698 735 828 903">Yes</td> <td data-bbox="698 903 828 1071"></td> <td data-bbox="698 1071 828 1845">There is an Independence Policy that all auditors are required to sign upon beginning employment. Signed copies for each employee were provided for review. The listing of auditor’s primary and secondary responsibilities provided in the Audit Plan 2001 makes it appear that there are no operations management responsibilities within the audit department.</td> </tr> <tr> <td data-bbox="828 735 958 903"></td> <td data-bbox="828 903 958 1071"></td> <td data-bbox="828 1071 958 1845">IAD staff do not participate in any operating responsibilities through rotation or on a temporary basis, nor does the IAD allow operating staff to participate on audits on a rotation.</td> </tr> <tr> <td data-bbox="958 735 1088 903"></td> <td data-bbox="958 903 1088 1071">No</td> <td data-bbox="958 1071 1088 1845">The Director and the Deputy Director indicated that independence and objectivity are discussed during the periodic staff meetings; however, there</td> </tr> </tbody> </table>	Yes	No	Comments (note source of info, etc.)	Yes		There is an Independence Policy that all auditors are required to sign upon beginning employment. Signed copies for each employee were provided for review. The listing of auditor’s primary and secondary responsibilities provided in the Audit Plan 2001 makes it appear that there are no operations management responsibilities within the audit department.			IAD staff do not participate in any operating responsibilities through rotation or on a temporary basis, nor does the IAD allow operating staff to participate on audits on a rotation.		No	The Director and the Deputy Director indicated that independence and objectivity are discussed during the periodic staff meetings; however, there
Yes	No	Comments (note source of info, etc.)											
Yes		There is an Independence Policy that all auditors are required to sign upon beginning employment. Signed copies for each employee were provided for review. The listing of auditor’s primary and secondary responsibilities provided in the Audit Plan 2001 makes it appear that there are no operations management responsibilities within the audit department.											
		IAD staff do not participate in any operating responsibilities through rotation or on a temporary basis, nor does the IAD allow operating staff to participate on audits on a rotation.											
	No	The Director and the Deputy Director indicated that independence and objectivity are discussed during the periodic staff meetings; however, there											
<p>★ 2. Does the internal audit director have periodic discussions with internal audit staff over the importance of maintaining an independent mental attitude when conducting audits?</p>													

			<p>is no documentation to support this. Discussion with Alan Markum and Mike Goodwin revealed they do not normally discuss these issues with staff; they rely upon the audit staff to disclose any potential conflicts or anything that might impair their objectivity on an audit.</p>
<p>3. Does the internal audit director periodically query the internal audit staff about information concerning potential conflicts of interest and bias?</p>	<p>No</p>		<p>During the planning stage of the audit preparation IAD Management relies upon the auditor to disclose any potential conflicts of interest or bias that may exist. They have an Audit Planning Checklist that is not utilized at this time that could be updated to include a verification of no conflicts of interest or bias.</p>
<p><b>Reviewer's Notes</b></p> <p>a. The above practices are typically evidenced by interviews, position descriptions, organizational charts, and memorandums.</p> <p>b. The reviewer administering this section should also consider <i>Standard 240 – Compliance with Standards of Conduct</i>, or actually administer that section as part of this review.</p>			
<p><b>Conclusions</b></p>			
	<p>Yes</p>	<p>No</p>	<p>Comments</p>

Has the internal audit department adopted two or more of the above practices	No	We are recommending that the IAD utilize the Audit Planning Checklist during the planning stage of each audit and that they add an item discussing potential conflicts of interest and/or bias to the staff section of this checklist.
--	----	--

# IAU Control Self Assessment

IAU Control Self Assessment

# **CONTROL SELF-ASSESSMENT**

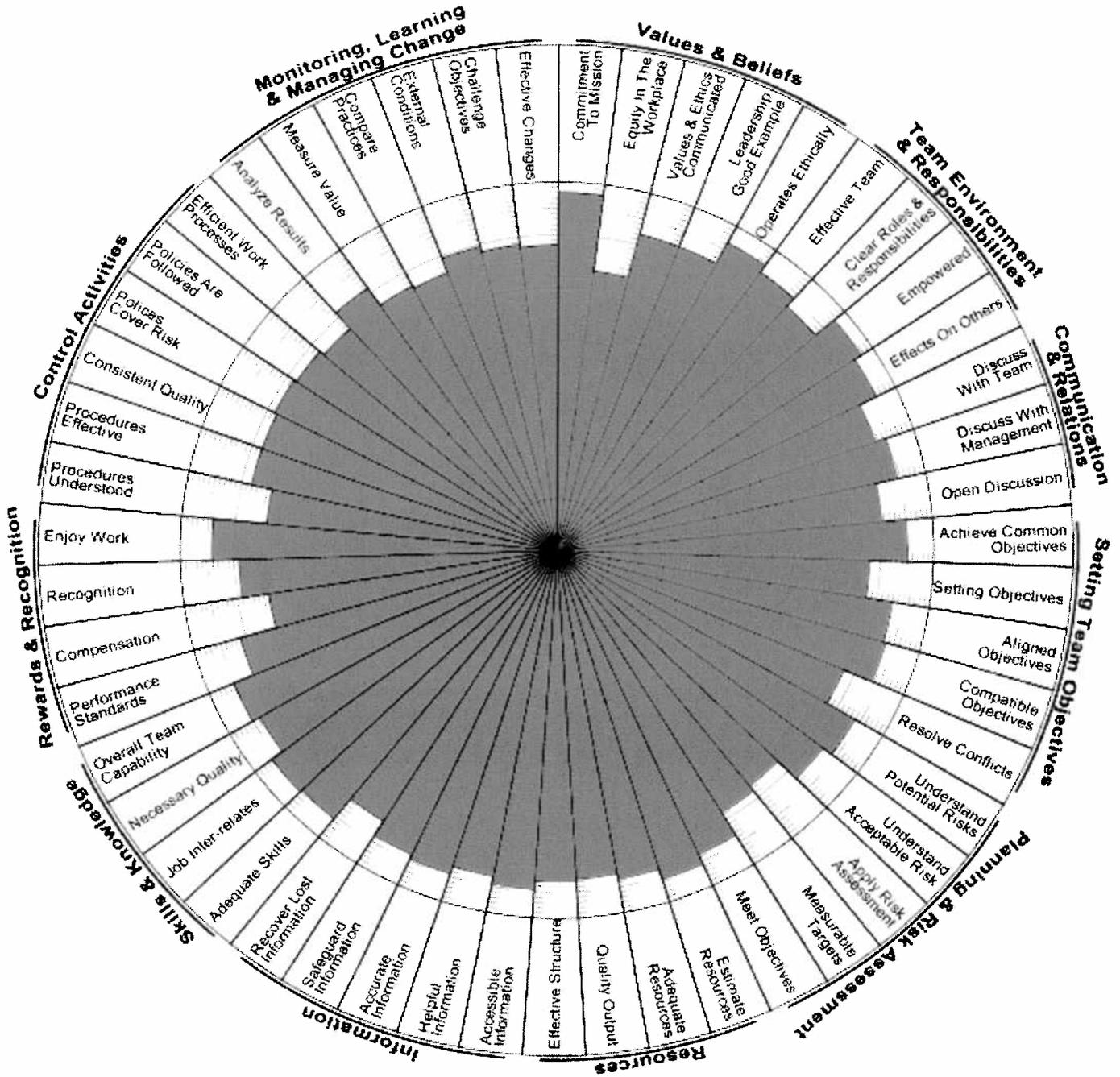
## **Workshop Summary**



**Internal Audit Department**

**Date: December 17, 2003**

# Control Profile



TM PDK Control Consulting International Ltd.  
 © 1995 PDK Control Consulting International Ltd.

## Summary Observations By The CSA Workshop Facilitators

The Internal Audit Department team members feel they have the values, ethics, skills and knowledge necessary to meet their objectives, good teamwork, and a good work environment. However, the team has concerns regarding compensation, equity issues, resources, and policies and procedures.

### Good News:

#### Values and Beliefs

The team strongly indicated that the department demonstrates commitment to its mission of providing reliable, independent, objective evaluations and business and financial advisory services to the Board of Supervisors and County management. Team members feel the department's values and ethics have been clearly communicated to them and that the "department operates in an ethical manner and with high integrity." They feel that management sets a good example and supports a very professional environment.

#### Teamwork

Team members stated that they have "fantastic teamwork." Staff feel they are empowered and supported by management and appreciate the autonomy of their work. They stated that they understand their roles and responsibilities and they "get the job done" and "all employees work hard and care about the quality of work."

#### Skills and Knowledge

The team stated that they are "very skilled and experienced". They pointed out that team members have a "variety of professional licenses and backgrounds that makes them well-rounded Auditors." They also said their training budgets and the tuition reimbursement program assist them in "maintaining skill sets with emerging trends". In addition, team members have many years of auditing experience..

#### Work Environment

The team feels they work in a good environment. They said they "enjoy being able to do different types of audit work within the department". They mentioned that the low turnover in their department is reflective of a good working environment and that they enjoy their work. They also said they have a great support staff, which helps them meet their objectives.

### Challenges Identified:

#### Compensation

Some team members indicated that they are not adequately compensated. They said the "County is benefiting from our certifications/licenses - we should be paid accordingly." They stated current compensation levels "do not address issues of 'skill-based' or 'impact of decisions rendered' pay." They also said the department has not determined whether administrative staff are adequately compensated.

#### Equity Issues

Some team members feel that employee recognition is inconsistent among the Audit Managers. They said, "There appears to be inequity in recognizing and rewarding employees' performance causing morale problems among the employees." In addition, "differences in workloads and levels of responsibility occur within the same job classification" and "Some staff is held to a strict budget and some are not." Team members also expressed concern that management has not yet delegated additional responsibilities to the recently promoted employees.

#### Resources

The team indicated they are concerned with the County's current budget problems. They said, "Our training budget and tuition reimbursement could be a concern because of the County's fiscal crisis" and "We don't want to lose the ability to reimburse staff for licenses/certifications." They stated they are concerned about "budget cuts and possible layoffs." The team also mentioned a need for more Information Technology Auditors and the need for Auditors to gain more information technology experience.

#### Policies and Procedures

The team indicated there was a need for workpaper standardization. Also, the team mentioned that the departmental administrative procedure manual needs to be completed. The team said there was some inefficiency in their procedures, for example, "Sometimes we list things over and over, such as findings/observations."



## **Audit Staffing Benchmarks**

Based on a benchmarking survey of 45 larger local government organizations, we applied a ratio of total County budget to auditors to determine our comparable staff size:

	Comparable	Actual IAD
Nationwide	30	16 <sup>1</sup>
CA	19.4	16 <sup>1</sup>

The above comparisons indicate our staffing should be increased. However, our auditors are seasoned experienced professionals possessing a number of professional certifications. The seasoning and certifications of our auditors translates into improved efficiency and effectiveness, giving us comfort with the adequacy of our current staffing size of 16 auditors.

<sup>1</sup> Total IAD staff of 22 less 4 administrative staff and Audit Director & Deputy Director. This methodology is comparable to the other larger local governments surveyed.

**2003 Local Government Audit Survey Results - CA**  
Sorted by Total Budget per Auditor

The Internal Audit Office of Fairfax County, VA performs an annual benchmarking survey of 50 of the largest local government audit departments in the United States. Each year, the Orange County Internal Audit Department participates in the survey. For the 2003 survey, 45 of the 50 audit departments responded. Of the 45, 11 were from California. Below are results from the survey.

Organization Name	# of Emp (A)	Total Budget (B)	# of Auditors (C)	# of Admin	# of Other Positions	Total Audit Dept Staff (D)	Audit Dept Budget	Ratio - Total Budget Per Auditor (B/C)
1 Alameda County, CA	9,279	1,900,000,000	7	1	0	8	800,000	271,428,571
2 San Diego City, CA	11,200	2,100,000,000	22	0	1.2	23.2	2,138,357	95,454,545
3 San Bernardino Cty, CA	19,000	2,600,000,000	19	3	2	24	1,100,000	136,842,105
4 Contra Costa Cty, CA	8,788	1,516,912,000	7	0	1	8	603,538	216,701,714
5 Los Angeles Cty, CA	95,000	16,482,000,000	74	3	0	77	8,954,500	222,729,730
6 San Diego County, CA	1,800	3,600,000,000	15	1	2	18	1,600,000	240,000,000
7 Sacramento Cty, CA	14,916	2,359,619,243	9	0	1	10	916,402	262,179,916
8 San Francisco, CA	28,000	4,900,000,000	18	1	0	19	2,100,000	272,222,222
9 Orange County, CA	17,741	4,908,600,000	16	4	2	22	2,236,178	306,787,500
10 Riverside County, CA	17,700	2,700,000,000	6	1	0	7	500,000	450,000,000
11 Los Angeles City, CA	40,000	12,000,000,000	25	1	3	29	3,600,000	480,000,000
<b>Totals</b>	<b>263,424</b>	<b>\$55,067,131,243</b>	<b>218</b>	<b>15</b>	<b>12</b>	<b>245</b>	<b>\$24,548,975</b>	<b>\$252,601,519</b>

19.4 projected auditors = \$4.908 billion County FY 02-03 budget divided by \$252.6 million.

**2003 Local Government Audit. Survey Results - Nationwide**  
**Sorted by Total Budget per Auditor**

The Internal Audit Office of Fairfax County, VA performs an annual benchmarking survey of 50 of the largest local government audit departments in the United States. Each year, the Orange County Internal Audit Department participates in the survey. For the 2003 survey, 45 of the 50 audit departments responded. Below are results from the survey.

Organization Name	# of Emp (A)	Total Budget (B)	# of Auditors (C)	# of Admin Positions	# of Other Positions	Total Audit Dept Staff (D)	Audit Dept Budget	Ratio - Total Budget Per Auditor (B/C)
1 Dallas County, TX	5,500	678,660,000	37	4	0	41	4,600,000	18,342,162
2 Memphis City, TN	9,296	461,000,000	11	1	0	12	850,000	41,909,091
3 San Antonio City, TX	13,204	1,404,000,000	26	2	2	30	2,021,164	54,000,000
4 Baltimore City, MD	15,871	2,100,469,921	36	3	0	39	2,995,640	58,346,387
5 Phoenix City, AZ	14,832	1,825,000,000	27	5	2	34	2,749,000	67,592,593
6 Philadelphia City, PA	31,967	5,378,862,636	76	11	11	98	7,099,236	70,774,508
7 Indianapolis City, IN	4,015	545,000,000	7	0	0	7	751,000	77,900,000

2007 Audit Plan &  
Department  
Organizational Charts



**COUNTY OF ORANGE**  
**INTERNAL AUDIT DEPARTMENT**  
**2004 Audit Plan**

**Approved by the Audit Oversight Committee**  
**Meeting Date: December 3, 2003**

**Peter M. Hughes, PhD., CPA, CIA, CFE, CITP**  
**Director, Internal Audit Department**

**400 Civic Center Drive West, Building 12, Room 232**  
**Santa Ana, CA 92701**  
**(714) 834-5475**



**COUNTY OF ORANGE**  
**Internal Audit Department**  
**2004 Audit Plan**

**Table of Contents**

	<u>PAGE</u>
<b>EXECUTIVE SUMMARY</b> .....	1
Mission Statement.....	1
Goals .....	1
Information Technology (IT) Issues .....	3
Dedication of Resources to Audit Related Services .....	3
<b>2004 DETAILED AUDIT PLAN</b> .....	4
<b>PRIOR YEAR ACCOMPLISHMENTS</b> .....	6
Core Audit Activity Accomplishments.....	6
Board Requested Audits or Special Request Audits.....	8
Additional Audit Activity Accomplishments .....	8
<b>DEPARTMENTAL ORGANIZATION CHART</b> .....	10
Primary Audit Activity Organizational Chart.....	11
Additional Audit Activity Organizational Chart.....	12
<b>COUNTYWIDE RISK ASSESSMENT METHODOLOGY</b> .....	13
<b>ATTACHMENT - RISK ASSESSMENT SCHEDULES</b>	A-1 - A-6



## EXECUTIVE SUMMARY

### MISSION STATEMENT

The mission of the Internal Audit Department (IAD) is to provide highly reliable, independent, objective evaluations and business and financial advisory services to the Board of Supervisors and County management. We assist them with their important business and financial decisions and help to protect and safeguard the County's resources and assets.

We support and assist the Board of Supervisors and County management in the realization of their specific business goals and objectives. Our contribution to this effort is testing and reporting on the effectiveness of their internal control systems and processes. County management relies on these systems and processes for safeguarding the County's assets and resources, for reasonable and prudent financial stewardship, for accurate recording and reporting, and for achieving the County's goals and objectives.

We are recognized for our expertise in assisting the County improve its business processes while strengthening the protective internal control environment the public expects, relies upon, and demands. We are committed to a process of continuous learning and improvement within our department to keep updated on developing and innovative industry practices. Such constant renewal keeps the IAD and its staff professionally current, refreshed, invigorated, and responsive to the County's needs for attestation, compliance assurance, accountability testing, and business improvement by implementing industry best-practices with regard to internal control and accounting systems and processes.

Internal Audit provides a variety of audit services to its primary client, the Board of Supervisors. They have the shared elected responsibility and accountability for the financial stewardship of the County. Another recipient of our audit services is County management who have the responsibility for day-to-day operation of the County departments and agencies. In addition, our published reports are used by various Federal and State regulatory agencies, the Grand Jury, the media, the investment community, and the public at large.

To meet our clients' expectations and for us to function effectively with reliability and credibility IAD must ensure our reviews and assessments of County operations are independent, accurate, and unbiased. Therefore IAD follows, when appropriate and necessary and depending on the type of audit being conducted, the exacting ethical and professional standards promulgated by the American Institute of Certified Public Accountants (AICPA), by the Institute of Internal Auditors (IIA), by the Information Systems Audit and Control Association (ISACA), and by the Government Accounting Office (GAO).

### GOALS

IAD continues to implement for calendar year 2004 the two fundamental strategic goals of this audit organization begun in prior years and which incorporated the proactive visions in the formation of the department. These two goals remain at the heart of our operation. We reassess them annually and they continue to be relevant in guiding the professional direction of the department.

1. We assist the Board of Supervisors and County management in ensuring the County's assets and resources are well safeguarded, the County's accounting and financial reporting is timely and accurate, and the County's management has timely information and relevant analysis for its business and economic decisions.



2. We provide professional assurance, attestation, and confidence to our clientele on the County's internal controls, accounting records, and financial and business operations through our published audit reports and reviews.

We have incorporated these Business Plan goals into our annual Audit Plan. Our Audit Plan is submitted, discussed, and approved at the beginning of each calendar year by the Audit Oversight Committee. We are dedicated to completing our audit plan while continuing to be flexible and responsive to the Board's requests for audit services.

The audit plan has at its core the traditional audits of "hard-controls;" such as segregation of duties, limiting access to cash, and accurate originating accounting entries and transactions. Examples of these traditional audits in our audit plan include our core business functions identified as Attestation Services audits (AS), Departmental Control Reviews (DCR), and Information Technology Audits (IT). Our reports contain opinions regarding the status of internal controls or the County's compliance with grant or other governing provisions. Our reports also include recommendations to management regarding improvements to specific accounting processes and internal controls. Based on follow-up work performed on the status of our recommendations, we are proud to say (and also compliment our partnership with County management because they see value in our recommendations) that County management substantially implements our recommendations on a timely basis.

We combine these three core groups of "hard control" audits (AS, DCR, and IT) with facilitated Control Self-Assessment (CSA) workshops to achieve the balanced audit coverage of the County we desire. The CSA workshops address the "soft control" aspects of a business operation; such as, communications, ethics and morale, and planning and risk assessment. In these workshops, we facilitate and attempt to discover if the work environment allows surfacing of business problems. The participants of the workshop and their management self-identify problems, issues, or concerns and ways they themselves can improve upon their own work environment. This process is an innovative and enlightened management approach to workplace problem resolution, recognizing that staff closest to the problem area owns the problem and usually has the solution.

For the prior year 2003, we successfully met our two key outcome measures. Our audit efforts and the diligence of County management in managing its operations and addressing their control environments contributed to the achievement of these measures. Our two key outcome measures were successful last year because:

- The County had no defalcation or reported excessive cash losses.
- A high percentage of clients reported they received information and/or recommendations that were helpful to them in safeguarding the County's assets and making business decisions. With few exceptions, our control recommendations were addressed by management and implemented.



## INFORMATION TECHNOLOGY (IT) ISSUES

The pace of technological advancement and the benefits to be realized by implementing these advances to improve County business operations is increasing at an accelerating speed. The Audit Oversight Committee recognized this issue at their December 5, 2001 meeting. Since then, we implemented an Information Technology (IT) focus to complement the audits we currently accomplish in the Attestation Services (AS) and Departmental Control Reviews (DCR).

We developed a long-term, two-tier IT plan to address the varied business needs of the County. The first tier addresses specific issues and areas in the County-wide Comprehensive Accounting and Personnel System (CAPS), the County's financial recording and reporting backbone. The second tier addresses the distributed computing taking place in County departments and agencies. The specifics of the two tiers are as follows:

1. A major replacement of CAPS is planned to begin in 2005. An RFP will be issued for the replacement system. Because of the importance and impact of CAPS, we coordinate audit coverage with the Auditor-Controller to determine the best approach. Until this replacement takes place, our audit focus will be to conduct narrowly scoped IT audits into areas of CAPS. We plan to contract certain technical aspects of this effort with consultants.
2. This year we developed and distributed an IT self-assessment questionnaire to the County departments during our risk assessment meetings with them. Our future vision is that we will promote self-assessment to the County's IT professionals and we will validate a sample of the departments' completed self-assessment questionnaires.

## DEDICATION OF RESOURCES TO AUDIT RELATED SERVICES

Our Audit Plan is based on **21,000** direct audit hours to be provided by 14 audit professionals. The audit hours for the Director and Deputy Director are not included in the above total and the time for the three Audit Managers is adjusted downward to allow them time for administrative management.

These hours are allocated to the following:

Attestation Services and Mandates (AS):	<b>5,060</b>
Information Technology (IT) audits:	<b>4,300</b>
Departmental Control Reviews (DCR):	<b>5,000</b>
Facilitated Control Self-Assessment (CSA):	<b>2,875</b>
Compliance Audits and controls consulting:	<b>2,345</b>

The plan also allocates an additional **1,420** hours for audit activities such as staffing the fraud hotline, reviewing cash losses, administering data collection of external audits, conducting training classes in County departments on practical internal control concepts and application, and performing the annual risk assessment.

Within the **21,000** hours, we reserved **2,400** hours to respond to Board requests for audit services. In addition to our 21,000 direct hours, we contract out to industry experts certain audits such as information technology audits and limited lease revenue reviews. We estimate that these consultants will provide **1,000** hours of work effort. Our 2004 Audit Plan is detailed on the following page.



**County of Orange Internal Audit Department  
2004 DETAILED AUDIT PLAN**

<i><b>Audit Name</b></i>	<i><b>Audit #</b></i>	<i><b>Budgeted Hours</b></i>
<b>ATTESTATION SERVICES &amp; MANDATES</b>		
Treasury Funds Audit - 12/31/03 (carry over)		1,500
Treasury Funds Audit - 3/31/04		400
Treasury Funds Audit - 6/30/04		400
Treasury Funds Audit - 9/30/04		400
Treasury Funds Audit - 12/31/04		100
Annual Treasury Investment Compliance Audit (YE 12/31/03)		800
DA Spousal Abuser Prosecution Grant - 6/30/04		160
DA Workers Comp/Auto Insurance Fraud Grant - 6/30/04		250
Auditing & Accounting Standards Update		200
Quarterly Treasury Compliance Reviews (scope/budget tbd)		800
Work Paper Close-Out & Final Report Issuance (audits from 2003 plan)		50
<b>Subtotal</b>		<b>5,060</b>
<b>INFORMATION TECHNOLOGY AUDITS</b>		
CAATs - Monthly Routines (on-going)		600
CAATs - Monthly Routines (development of new routines)		1,000
CAATs - Monthly Routines (cross-training & documentation of routines)		300
Review of CEO/IT - IT Governance		400
IT Self-Assessment Validation (trial dept) - HCA		400
Follow-up & Update - CAPS/Readiness Assessment		300
Follow-up - CAPS/Payroll Audit		200
Assist on IT Component of DCR (tbd)		100
Assist on IT Component of DCR (tbd)		100
Assist on IT Component of TFA (12/31/04)		100
Assist on IT Component of Treasury Compliance Audit (12/31/03)		100
IT General/Research		200
TBD - Application Audit		0
TBD - System Implementation Reviews		0
Reserve for Additional Audit Requests		500
<b>Subtotal</b>		<b>4,300</b>
<b>DEPARTMENTAL CONTROL REVIEWS (DCR)</b>		
Auditor/Controller - Tax Unit		300
Auditor/Controller - Collections Process		250
Auditor/Controller - Trust Funds		300
PFRD - Utility Billings		200
PFRD - Revolving Funds		250
PFRD - Trust Funds		350
Housing & Comm. Services/CEO - Redevelopment Agency		300
IWMD - Purchasing & Contract Administration		300
HCA - Cash Receipts & Accounts Receivable		300
HCA - Trust Funds		300
SSA - Revenues & Accounts Receivable		300



Budget Process Reviews	400
DCR Administration	100
Follow-Ups and Post Follow-Ups	900
Work Paper Close-Out & Final Report Issuance (audits from 2003 plan)	50
Reserve for Additional Audit Requests	400
<b>Subtotal</b>	<b>5,000</b>
<hr/>	
<b>CONTROL SELF-ASSESSMENT (CSA)</b>	
CSA - District Attorney (2 workshops)	475
CSA - HCA/Contracts (1 or 2 workshops)	475
CSA - Office on Aging (1 or 2 workshops)	475
CSA - Clerk-Recorder (3 or 4 workshops)	700
CSA - tbd	0
CSA Promotion & Orientation	200
Work Paper Close-Out & Final Report Issuance (audits from 2003 plan)	50
Reserve for Additional Audit Requests	500
<b>Subtotal</b>	<b>2,875</b>
<hr/>	
<b>COMPLIANCE</b>	
Administration of Limited Lease Revenue Reviews	100
PFRD/Canyon RV Park - Limited Lease Revenue Review	150
PFRD/City of Anaheim Parking - Limited Lease Revenue Review	200
PFRD/Bristol Instant Storage - Limited Lease Revenue Review	150
TBD - Limited Lease Revenue Review	150
TBD - Limited Lease Revenue Review	150
HIPAA Compliance Reviews	400
Reserve for Additional Audit Requests	1,000
Work Paper Close-Out & Final Report Issuance (audits from 2003 plan)	45
<b>Subtotal</b>	<b>2,345</b>
<hr/>	
<b>CONTROL RELATED &amp; OTHER ASSIGNMENTS</b>	
Annual Risk Assessment Audit Planning	500
Cash Losses	200
Fraud Hotline	120
External Audit Reporting	300
Technical Assistance to Other Dept/Agencies	300
<b>Subtotal</b>	<b>1,420</b>
<hr/>	
<b>Grand Total</b>	<b>21,000</b>
<hr/>	
<b>ADDITIONAL COVERAGE PROVIDED BY CONSULTANTS</b>	
IT Audits - to be determined	
Sheriff - Medical Benefits Review	
<b>Total</b>	<b>0</b>
<hr/>	



## **PRIOR YEAR ACCOMPLISHMENTS**

### **CORE AUDIT ACTIVITY ACCOMPLISHMENTS**

#### **Department Control Reviews (DCR)**

We completed all DCRs scheduled and budgeted in our 2003 Audit Plan. The DCRs focused on internal control reviews of cash receipts and cash disbursements involving trust funds, revolving funds, and special use department/agency funds. Cash receipt and disbursement DCRs are considered a core audit areas due to the inherent risk that exists in cash handling, and are initiated in departments/agencies where a significant amount of monies are collected and processed. Our review of department/agency funds also helps to ensure monies are being used in accordance with their established purposes. These reviews are valuable because they help identify funds/accounts with little or no activity or which contain unidentified monies that require further investigation and resolution by the department/agency. Additionally, we performed a review of the County's purchasing cards where we evaluated the process and controls over the administration, use, and oversight of the purchasing card program. We also performed a limited review of internal controls over the Public Administrator/Public Guardian property vault.

#### **Department Control Review Follow-Ups**

The Follow-Up review process is necessary to ensure that the audit recommendations resulting from our DCRs are implemented satisfactorily. During 2003, Internal Audit continued its "post follow-up" review process where follow-up reviews are performed to ensure audit recommendations not implemented in the initial follow-up review have been fully implemented. Five initial Follow-Ups and five Post Follow-Ups were completed in 2003.

#### **Attestation Services (AS)**

We will complete by year-end all financial and mandated audits listed in the Audit Plan on schedule. We have completed the Treasury Funds Audits for quarters ending 12/31/02, 3/31/03, and 6/30/03; Quarterly Treasury Compliance Review for 3/31/03 and 6/30/03; the DA Auto Insurance Fraud Grant, and the DA Workers' Compensation Fraud Grant. We are in the process of completing the Treasury Funds Audit for quarter ending 9/30/03; the Probation Audit for two years ending 6/30/03. We will be starting the DA Spousal Abuser Prosecution Grant in November 2003 and will complete the audit by the end of December 2003; and the Quarterly Treasury Compliance Review for 9/30/03, which will be completed by year-end.

#### **Information Technology (IT) Audits**

We will complete by 12/31/03 all seven goals for the 2003 IT audit coverage:

- 1) Application Audit: We completed an audit of the Auditor-Controller's internal controls for the laser check printing process.
- 2) System Implementation Review: We will complete our review of IWMD's implementation of a new system for fee collections and accounts receivable (Weighstation/Compuweigh and Great Plains).
- 3) Assist on an IT Component of a Financial Audit or Department Control Review: We completed a



general computer controls review at the Treasurer-Tax Collector as part of the 12/31/02 Treasury Funds Audit.

- 4) IT Self-Assessment Questionnaire: We developed an information technology self-assessment questionnaire (based upon the COBIT model from the Information Systems Audit and Control Association) for County departments use. The comprehensive questionnaire provides a standard for departments to self-assess their varied I/T operations and identify areas for potential improvement. The questionnaire was discussed and distributed during the risk assessment meetings held with the departments in September, October, and November 2003.
- 5) Computer Assisted Audit Techniques (CAATs): We performed our first CAAT routine for duplicate payments in May 2002. Since then, we continued to run the duplicate payment routines monthly and to date have identified \$122,692 in duplicate payments now in varied stages of recovery. Additionally, CAATs for 2003 included these additional routines:
  - We developed and performed on-going routines for: employees/vendor matches, retirees working in excess of established thresholds, direct deposit paychecks made to the same bank account, and vendors deleted from Vendor Master Lists. As a result of these routines, we identified matches of employees working as vendors and retirees working in excess of established thresholds. Upon researching the underlying circumstances for the matches, the applicable County departments also identified and implemented process improvements to prevent reoccurrences of the identified issues.
  - We developed and implemented a CAAT routine to improve audit efficiency when performing the quarterly Treasury Compliance Reviews, beginning with the quarter ending 3/31/03. The CAAT is used to analyze the Treasurer's investment portfolio and determine diversification percentages to compare with government regulations.
  - We developed several CAAT routines to obtain financial information (amounts and transaction activity) to be utilized in the annual risk assessment. For example, we were to able compile cash receipt activity and transactions by the department that processed the cash receipt rather than by the department/fund where the money was deposited (some departments process monies for other departments).
- 6) Countywide I/T Inventory: We compiled a listing of key systems being used in the County departments that we utilized as part of our I/T annual risk assessment. We also obtained relevant information, such as the platform, operating system, type of data, source/support for the system, and interfaces thereby increasing our understanding of the departments' I/T environment.
- 7) Update to CAP #34: By 12/31/03, we will submit an updated draft of County Accounting Procedure #34 (Development of Financial Computer Systems) to the Auditor-Controller's Office.

#### **Control Self-Assessment (CSA)**

We will complete all scheduled (seven) CSA workshops in our Audit Plan by December 31, 2002: three in Public Facilities and Resources Department (PFRD) and four in Planning and Development Services Department (PDSD). In PFRD, workshops were conducted for Watershed & Coastal Resources, Information & Technology Services, and the Permit Process. In PDSD, workshops were conducted for Management, Building Inspection, Building Plan Check, and Planning.



## BOARD REQUESTED AUDITS OR SPECIAL REQUEST AUDITS

During 2003, Internal Audit performed the following eight special audits and/or reviews resulting from requests by the Board of Supervisors, the CEO or Departments:

1. PDSB Budgetary Controls: As a result of the deficit in the Building & Safety Fund 113, we performed a review of budgetary controls for the Planning & Development Services Department.
2. Countywide Budget Process: We also performed a limited review of the County budget process to help ensure employees involved in the budget process had accountability and clearly defined roles and responsibilities.
3. CEO/HR Management Reclassification Process: We performed, with the assistance of consultants, an audit of the reclassification process for management employees. Our audit included customer surveys completed by the County departments.
4. CEO/HR Contract Administration Issues: To assist the CEO in responding to a Grand Jury report, we reviewed the CEO/HR's management of a Deloitte & Touche, LLP contract issued for the Performance Incentive Program (PIP).
5. CEO/HR Use of Unemployment ISF (Fund 291): During our review of the above Deloitte & Touche contract, we identified instances of non-insurance charges and transfers made from Fund 291. We issued a separate report for this issue.
6. HCA Subcontractor Review: We completed a preliminary survey at three health care clinics to determine whether they were maintaining adequate financial records.
7. PA/PG – Statement of Assets Transferred: We reviewed the Statement of Assets Transferred forms resulting from changes in the Public Administrator and Public Guardian positions.
8. PFRD Prevailing Wage Review: We performed a review of two contractors to determine whether they were in compliance with prevailing wage requirements.

## ADDITIONAL AUDIT ACTIVITY ACCOMPLISHMENTS

### Limited Reviews of Lease Revenue

These reviews are requested by PFRD and JWA and are performed on a fiscal year basis. We completed four scheduled limited reviews of lease revenue listed in the Audit Plan. We also completed two additional reviews and are in process of starting a third review that was not originally scheduled. To help accomplish the reviews, we utilized audit staff from a local Certified Public Accounting (CPA) firm under an existing contract. We also utilized our own internal audit staff for the more complex reviews.

### Technical Assistance to Others

We continued to provide assistance to various departments as requested. In 2003, we assisted PFRD with certain financial issues and audit strategies for the three key operators in the Dana Point Harbor. We also assisted PFRD by reviewing a proposed lease amendment for the Sunset Marina lease and certain capital improvement issues for the Strawberry Farms Golf Course lease.



**Cash Losses**

The Auditor-Controller has been given authority to approve replenishment of cash losses up to \$300. For cash losses more than \$300, the Auditor-Controller requests the Internal Audit Department to review the circumstances surrounding the loss and to evaluate the adequacy of corrective actions taken to prevent future losses. We are pleased to report that during 2003, there were only nine cash losses reported, and only two needing an investigation by Internal Audit. Many of the smaller cash losses involved the receipt of counterfeit bills and some instances from employees not adhering to established procedures and internal controls. More attentiveness to procedures and controls resulting from both our DCRs and department/agency internal reviews have been contributing factors in the decrease of cash losses.

**Fraud Hotline**

We processed 36 Hotline incidents: 12 incidents were referred to County departments/agencies for investigation, 15 incidents were referred to the Welfare Fraud Hotline for investigations, 2 were referred to outside agencies, and 7 were information requests and "other." To date, 6 of the 12 incidents referred to County departments/agencies for investigation remain open.

**Countywide Risk Assessment**

The Internal Audit Department performed a risk assessment for purposes of preparing the 2004 Annual Audit Plan. In 2003, we significantly enhanced our annual risk assessment process by incorporating reviews of the department/agency Business Plans, compiling financial information/activity by business process (e.g. cash receipts, disbursements, revenues, expenditures) for each department, and by meeting with Executive Management in the departments. As a result, we hope to provide additional value to management in our audit planning process by addressing areas perceived jointly as having higher risks.

Additionally, we expanded the annual risk assessment to include an inventory and assessment of key information systems used by the departments.

**Internal Controls Training Classes**

The Director and staff of Internal Audit were asked by departments to conduct internal controls training for their managers. Two such training classes were provided to HCA and the Registrar of Voters in 2003, as well as a presentation at a Department Head Meeting. This training was well received and the attendees appreciated the practicality of the materials presented.

**External Audit Activity**

Each quarter, we compiled and presented a report of external audits in process throughout the County to the Audit Oversight Committee, highlighting material findings.

**Peer Review**

During 2001, we successfully passed a Peer Review based on IIA standards and required by the Comptroller General of the United States in their published Government Auditing Standards. The Peer Review made minor recommendations to improve our auditing and management processes. During 2003, we implemented the outstanding recommendation involving a revision to our Audit Department Charter.

**CPA and Other Professional Certifications**

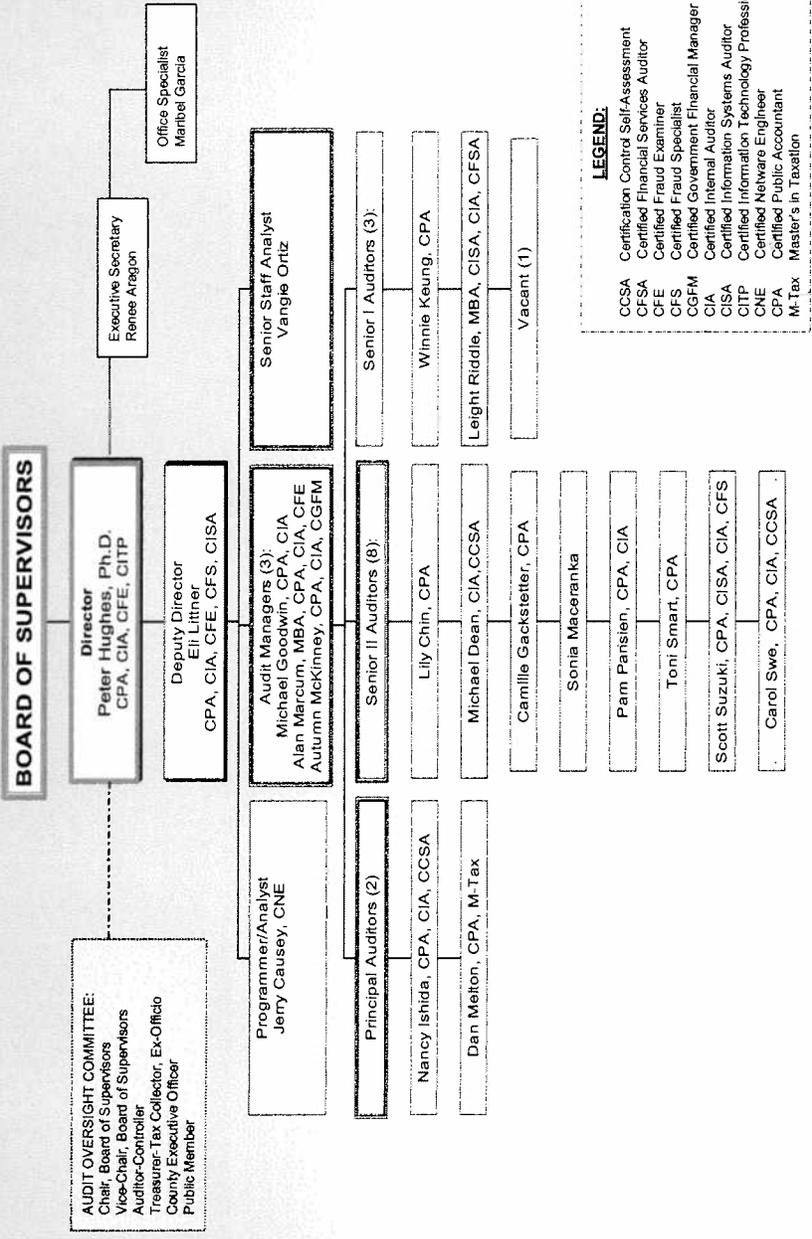
During 2003, one auditor submitted their Form E (Experience) package to the State Board of Accounting to receive the Certified Public Accountant (CPA) credential. The experience package was accepted and the CPA license was granted. Two auditors received the Certified Information System Auditor (CISA) credential. One auditor received the Certified Internal Auditor (CIA) credential.





County of Orange  
**Internal Audit Department**  
 Organizational Chart

Rev. 10-03



**LEGEND:**

- CCSA Certification Control Self-Assessment
- CFAA Certified Financial Services Auditor
- CFE Certified Fraud Examiner
- CFS Certified Fraud Specialist
- CGFM Certified Government Financial Manager
- CIA Certified Internal Auditor
- CISA Certified Information Systems Auditor
- CITP Certified Information Technology Professional
- CNE Certified Network Engineer
- CPA Certified Public Accountant
- M-Tax Master's in Taxation



Internal Audit Department  
 2004 Audit Plan

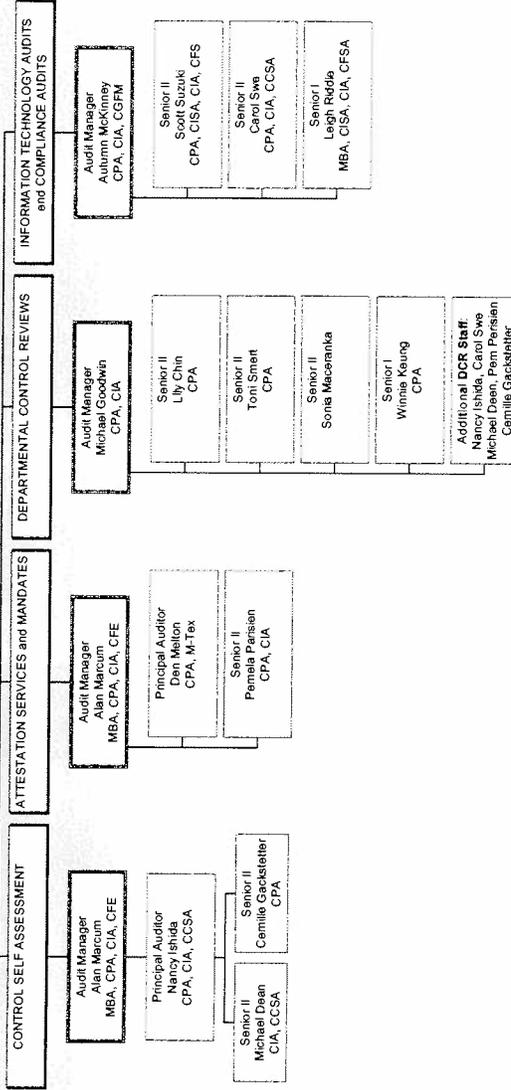
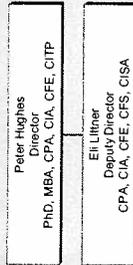
**PRIMARY AUDIT ACTIVITY ORGANIZATIONAL CHART**

2004 Audit Plan



**County of Orange  
Internal Audit Department  
Organizational Chart**

**PRIMARY AUDIT ACTIVITIES**



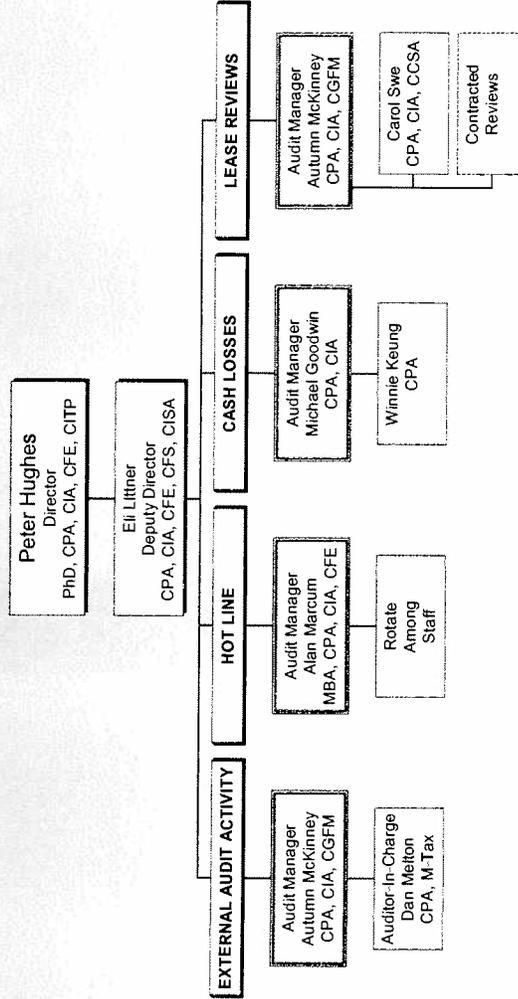
**ADDITIONAL AUDIT ACTIVITY ORGANIZATIONAL CHART**



2004 Audit Plan

**County of Orange  
Internal Audit Department  
Organizational Chart**

**ADDITIONAL AUDIT ACTIVITIES**



## COUNTYWIDE RISK ASSESSMENT METHODOLOGY

### **Overview:**

The Internal Audit Department performed a risk assessment for purposes of preparing the 2004 Annual Audit Plan. In 2003, we significantly enhanced our annual risk assessment process by meeting with Executive Management in the departments to discuss their operating environments and areas of importance and concern. By meeting with the departments, we hope to provide additional value to management in our audit planning process by addressing areas perceived jointly as having higher risks. Additionally, we expanded the risk assessment to include an inventory and assessment of key information systems used by the departments. Below is a discussion of our methodology for each area:

### **Departmental Control Reviews:**

Departmental Control Reviews (DCRs) are performed for processes involving cash receipts, revenues, accounts receivable, cash disbursements, revolving funds, purchasing/contract administration, trust /special department funds, payroll, and budgeting.

To determine risk ratings for these processes, we developed risk assessment worksheets for all departments/agencies, considering information we obtained from reviewing departmental business plans, meeting with the Executive management teams of the departments, and identifying financial volume and activity. We used the following criteria and relative weight factors in our assessment:

- Department/Agency Changes (20%): Included factors such as management and/or organizational changes, significant increases/decreases in staffing and workloads, new/eliminated programs, and significant changes in laws/regulations.
- Operating Environment (20%): Included factors related to the department's operating environment such as public image, laws/regulations, safety and environmental issues, sensitivity to economic factors, pending litigation, and business continuity.
- Last Audit Performed (10%): Identified all IAD internal control reviews performed on the above processes since 1996.
- Financial Activity/Volume (50%): Obtained a listing of all County funds and the controlling department/agency for each fund. From CAPS, we compiled FY 02-03 financial information (dollar volume, number and nature of transactions) for each process and for each controlling department.

Using the above criteria, each department/agency process was rated on a scale of 1 to 10 (10 being highest risk and 1 lowest risk) for each of the above weight factors. An overall risk score was then calculated showing areas of High (8 - 10), Moderate (4 - 7), and Low (1 -3) risk. The overall risk scores are shown on page 1 of the attached risk assessment schedules, and a schedule of our DCR audit coverage since 1996 is shown on page 2 of the attachment.

### **Control Self-Assessment Workshops:**

The CSA workshops are conducted in County departments on a voluntary basis. We contact the various department heads and inquire if there are any functions within their departments that could benefit from CSA workshops. In addition, we also regularly receive requests from department heads to conduct CSA workshops. Page 3 of the attachment lists by department the number of CSA workshops completed since 1999, which is when IAD started conducting CSA workshops.



**Information Technology Inventory and Assessment:**

We provided the County's departments with an I/T questionnaire in order to facilitate our I/T risk assessment process. The questionnaire asked for the name of the system, purpose, platform, operating system, interfaces, nature of data collected, implementation date, source (such as off the shelf vs. in-house developed), and upgrades/changes.

The departments completed the questionnaire only for each system they identified as critical or key to carrying out the mission of their respective department. From the completed questionnaires, we compiled a key system inventory. Examples of applications/systems not included in the inventory are: utilities (such as anti-virus, email, backup, and Microsoft operating system and office applications), terminal emulators (allows access to a mainframe computer via a personal computer), and systems of a limited/administrative nature (such as form generation, record retention, or telephone directories). We rated each system based upon the six relative weight factors below:

- Importance & Impact (30%): The importance and impact of the system to the County and department's mission. Systems having a countywide impact were rated high in this category.
- Complexity (20%): The complexity of the system taking into consideration the number of interfaces, the number of users and transactions, the nature of the database, and the nature of the calculations made by the system.
- Nature of Information (15%): The nature of the information controlled by the system such as financial, operational, or support. Systems controlling financial assets or data were rated high in this category.
- Sensitivity of Information (15%): The confidentiality of the information controlled by the system. Systems controlling HIPAA regulated information or personal information were rated high in this category.
- Maturity (10%): The length of time since the system was implemented or since significant upgrades occurred.
- Last Audit (10%): The number of years since the last audit.

Each system was rated on a scale of 1 to 5 (5 being highest risk and 1 being lowest risk) for each of the weighted factors. Then, an overall score was calculated and the system was ranked as high (400 or above), moderate (251 – 399), or low (below 250). Page 4-6 of the attachment is the inventory and ranking.

**See ATTACHMENT - RISK ASSESSMENT SCHEDULES**



This Risk Assessment provides an overview of where Internal Audit has allocated its staffing resources primarily in the Department Control Reviews. Because of audit coverage in other areas (e.g. Information Technology, CSA Workshops, and Mandated and Compliance audits), resources are limited. Therefore, all areas considered as High Risk are not included in the Annual Audit Plan, and will be addressed in future Audit Plans.

**BUSINESS PROCESSES:**

	Assessor	Auditor/Controller	County Executive Office	Child Support Services	Clerk of the Bd. of Supervisors	County Clerk-Recorder	County Counsel	District Attorney	Health Care Agency	Housing/Comm. Services	Integrated Waste Mgmt. Dept.	John Wayne Airport	OC Public Library	Public Facilities/Resources Dept.	Planning/Developmt. Svcs. Dept.	Probation	Public Defender	Registrar of Voters	Social Services Agency	Sheriff-Coroner	Treasurer/Tax Collector
<b>CASH RECEIPTS</b>	4	7	8	7	3	6	4	6	8	8	7	8	4	7	7	7	5	5	7	7	9
<b>REVENUES</b>	4	5	9	7	3	6	5	7	9	7	7	8	5	8	7	7	5	6	9	9	6
<b>ACCOUNTS RECEIVABLE</b>	3	8	8	6	3	4	4	7	9	8	7	8	4	7	6	7	6	7	8	9	8
<b>CASH DISBURSEMENTS (incl. Accts. Payable)</b>	4	8	8	7	3	5	4	5	9	6	6	7	4	6	6	6	6	6	7	8	9
<b>REVOLVING FUNDS (Annual Replenishments)</b>	6	4	6	5	3	5	5	7	8	6	5	6	4	8	5	7	6	4	8	9	5
<b>PROCUREMENT &amp; CONTRACT ADMINISTRATION</b>	3	7	9	6	3	4	4	6	9	7	6	7	4	8	6	7	4	6	9	8	6
<b>PAYROLL</b>	6	6	6	7	3	4	5	8	9	7	6	6	5	8	7	8	7	5	9	9	5
<b>TRUST FUNDS &amp; SPECIAL DEPARTMENT FUNDS</b>	3	8	6	6	2	5	4	4	9	6	7	5	2	6	6	7	4	5	9	7	6
<b>BUDGETING</b>	5	5	9	7	3	4	5	7	9	7	7	8	4	8	8	6	8	6	9	9	6
<b>AUDITS ON 2004 PLAN</b>																					

To be Audited Under 2004 Plan

Remaining to Audit "High" Rated Activity only (Ratings of 8-10)

High Rated Activity Audited Since 2000 (See Schedule of Prior Audit Coverage for the Years 1996 - 2003 on next page.)

**Note:** Risk ratings were based on reviews of Business Plans and meetings with Departments and Agencies using the following factors:

- Department/Agency Changes
- Operating Environment
- Prior Internal Audits
- Financial Volume and Activity

**LEGEND (see Note):**  
 1 - 3 Low Risk  
 4 - 7 Moderate Risk  
 8 - 10 High Risk

	Assessor	Auditor/Controller	County Executive Office	Child Support Services	Clerk of the Bd. of Supervisors	Community Services Agency	County Clerk-Recorder	County Counsel	District Attorney	Health Care Agency	Housing/Comm. Services	Integrated Waste Mgmt. Dept.	John Wayne Airport	OC Public Library	Public Facilities/Resources Dept.	Planning/Develop. Svcs. Dept.	Probation	Public Defender	Registrar of Voters	Social Services Agency	Sherris/Commer	Treasurer/Collector
<b>CASH RECEIPTS</b>		2001 (Collections)	2001, 2002 (Emp. Benefits)	2003		2001 (PA/PC)	1999, 2003	2000	1997, 1998, 2002	2000 (Billing & Rec.), 2001 (Emp. Health), 2001 (ACS)	1998	1997, 2000	2001		1998	2001			2000		2000 (Cl. Opal Financial Admin)	1997, Triennial Audit of TRO - 2002
<b>REVENUES</b>							1999	1999, Annual Grants	1999, Annual Grants						1998							1997, Triennial Audit of TRO - 2002
<b>ACCOUNTS RECEIVABLES</b>							1999	1999	2000 (Billing & Rec.)			1997, 2000	2001		1998							1997, Triennial Audit of TRO - 2002
<b>CASH DISBURSEMENTS - ACCOUNTS PAYABLE</b>			2002 (Emp. Benefits)				2003	1999, 2003, Annual Grants	1999, 2002, 2003 (Spec. Progs.)						1998, 2002				1997 (Fin. Aust.)			1997
<b>REVOLVING FUNDS</b>			2001	2003	2000	1996	1996	1996	1996, 2002 (Spec. Progs.)			1996	1994, 2001		1996 (EMA & GSA), 1998	2000	1996	2000	1994, 2000		1994, 2003	1997
<b>PROCUREMENT &amp; CONTRACT ADMINISTRATION</b>			1995, P-Cards 2003			P-Cards 2003	1999	1999				P-Cards 2003	P-Cards 2003	P-Cards 2003	1998		1998	P-Cards 2003				1997
<b>PAYROLL</b>							1999	1999							1998		1998					1997
<b>TRUST FUNDS &amp; SPECIAL DEPARTMENT FUNDS</b>				2003			1999, 2003	1999, 2003					2001		1998	2001	1998, Biennial Audits				2001 (Cl. Opal, 2003)	1997
<b>BUDGETING</b>			2003	2003			1999	1999							1998	2003	1998					1997

Legend:  
This schedule shows internal controls reviews performed since 1996. Shown are the years the audits were completed and the areas reviewed.

Audit Plan 2004  
Schedule of  
CSA Workshop Coverage

	Assessor	Auditor/Controller	County Executive Office	Child Support Services	Clerk of the Bd. of Supervisors	Community Services Agency	County Clerk-Recorder	County Counsel	District Attorney	Health Care Agency	Housing/Comm. Services	Integrated Waste Mgmt. Dept.	Internal Audit	John Wayne Airport	OC Public Library	Public Facilities/Resources Dept.	Planning/Develpmt. Svcs. Dept.	Probation	Public Defender	Registrar of Voters	Social Services Agency	Sheriff-Coroner	Treasurer/Tax Collector	
1999	8															17					2			
2000					1					3					3		3					7		
2001			4			4						3		2				4						2
2002					3			2	2															
2003													1			3								

Legend:  
This schedule shows the number of CSA workshops performed since 1999.

KEY INFORMATION SYSTEMS INVENTORY

AGENCY/DEPARTMENT	APPLICATION/SYSTEM	DESCRIPTION	RISK RATING	LAST AUDIT
<b>HIGHER RISK SYSTEMS - ALL</b>				
1 Assessor	ATS (Assessment Tax System)	property assessment/annual roll	High	
2 Auditor-Controller	CAPS Advantage Finance 2.2	accounts payable, disbursements	High	#2246 CAPS Upgrade Readiness (2002)
3 Auditor-Controller	ATS (Assessment Tax System)	tax calculations & allocations	High	
4 Auditor-Controller	CAPS Advantage Finance 2.2	payroll	High	#2247 Payroll Risk Assessment (2002)
5 Auditor-Controller	CAPS Advantage Finance 2.2	general ledger, financial reporting	High	Annual CAFR - external audit (Y/E 6/30/02)
6 Auditor-Controller	CAPS Advantage Finance 2.2	job cost, cost allocation, labor distribution	High	
7 Auditor-Controller & Other Depts	VTI (lifetime Virtual Timecard)	time keeping for multiple departments	High	#2065 VTI System Review (2000)
8 CEO/Human Resources	CAPS Advantage Human Resources 2.3	personnel	High	#2246 CAPS Upgrade Readiness (2002)
9 CEO/Human Resources	CAPS Advantage Human Resources 2.3	position control	High	#2246 CAPS Upgrade Readiness (2002)
10 CEO/Purchasing	CAPS Advantage Finance 2.2	purchasing	High	
11 HCA	Public Health Billing - Practice Expert Plus	patient data & billing of all claim types for clinics	High	
12 TTC/Tax Collector	ATS (Assessment Tax System)	tax bill generation and collection of taxes	High	
13 TTC/Treasurer	Quantum	treasury management system	High	#2208 12/31/02 TFA Audit - general controls (2002)
<b>MODERATE RISK SYSTEMS - BY CATEGORY</b>				
<b>CASE MANAGEMENT OR CASE TRACKING SYSTEMS</b>				
1 County Counsel	CountyLaw (CyCom)	case & document management for attorneys	Moderate	
2 District Attorney	CMS (Case Management System)	tracks filing status of criminal cases	Moderate	
3 District Attorney	Consumer, Major Fraud, Environmental Violations	tracks cases under investigation prior to filing	Moderate	
4 District Attorney	Special Assignment Investigations	tracks special cases under investigation prior to filing	Moderate	
5 District Attorney	Child Abduction	track abducted children	Moderate	
6 District Attorney	Felony Projects Case Tracking	tracks felony cases under investigation prior to filing	Moderate	
7 District Attorney	Welfare Fraud Case Tracking	tracks welfare cases under investigation prior to filing	Moderate	
8 HCA/Public Health	CCS - ChildWatch	medical case mgmt & fincl assist for disabled children	Moderate	
9 Probation	CMS (Case Management System)	probation case management for adults & juveniles	Moderate	
10 Public Defender	CMS (Case Management System)	manage & tracks PD cases	Moderate	
<b>CONSORTIA OR STATE MANAGED SYSTEMS</b>				
1 Child Support Services	ARS (ACES Replacement System)	child support case management (consortia system)	Moderate	#2330 DCR - Cash Receipts - limited review of user access (2003)
2 H&CS/Special Programs	JTA (Job Training Automation System)	track/report clients receiving job training (state system)	Moderate	
3 HCA/Maternal Child Health	CATS (Common Application Transaction System)	client registration and eligibility system (state system)	Moderate	
4 HCA/Public Health	AVSS (Automated Vital Statistics System)	birth, death, disease data collection (UCSB system)	Moderate	
5 HCA/Public Health	ISIS (Integrated State Information System)	WIC nutritional data system (state system)	Moderate	
6 SSA	WCDS (Welfare Client Data System)	determine eligibility, calculate benefits (consortia sys)	Moderate	
7 SSA	CWS/CMS (Child Welfare Svcs/Case Mgmt System)	case mgmt for children in custody (County hosted)	Moderate	
<b>FINANCIAL &amp; FINANCIAL RELATED SYSTEMS</b>				
1 Auditor-Controller	Rxlaser	laser check printing	Moderate	
2 Auditor-Controller	CUBS Collection System	billing and collection for various departments	Moderate	#2326 Laser Check Review (2003)
3 Auditor-Controller	ERMI (Electronic Report Management & Imaging)	financial report archiving	Moderate	
4 Child Support Services	Dissonaster	calculate child support payments due	Moderate	
5 Child Support Services	Payment ID	scan checks & input cash pymts for upload to ARS	Moderate	
6 Clerk-Recorder	Cashiering system	cash receipting application	Moderate	#2244 Cashiering System Implementation Review (2002)
7 Integrated Waste Management	CompuWeigh/Weightstation	landfill cash receipting	Moderate	
8 Integrated Waste Management	Great Plains eEnterprise	accounts receivable	Moderate	
9 John Wayne Airport	McGann Parking Revenue Control System	track parking revenues & ticket counts	Moderate	
10 PFRD/Gomatics & Land Info	E-Commerce System	sells downloads of maps and land information	Moderate	
11 PFRD/H&P	Cashiering POS	cashiering for more than 20 HB&P locations	Moderate	
12 PFRD/Public Works	ProgPay (Progress Payment System)	construction bids and payment management system	Moderate	
13 Probation	PFS (Probation Financial System)	manages financial obligations of probationers	Moderate	#2105 Mandated Audit - limited I/T coverage (2001)
14 TTC/Tax Collector	Netvanlage Cashiering System	cash receipts application	Moderate	
15 TT C/Tax Collector	Remittance Processing System	check scanning & payment posting	Moderate	
<b>MULTI-DEPARTMENT OR MULTI-FUNCTION/ENTERPRISE SYSTEMS</b>				
1 Auditor-Controller	CAPS/Fixed Asset System (AC42)	fixed asset accounting	Moderate	
2 CEO/Budget	Brass (CAPS)	budgeting	Moderate	
3 Clerk of the Board	ATS (Assessment Tax System)	property tax assessment appeals tracking	Moderate	

KEY INFORMATION SYSTEMS INVENTORY

AGENCY/DEPARTMENT		APPLICATION/SYSTEM	DESCRIPTION	RISK RATING	LAST AUDIT
4	H&CS/Housing	SERA (Section Eight Rental Assistance)	applications, eligibility, benefit calculations, & pymts	Moderate	#2223 DCR - Disbursements & Related I/T Processes (2002)
5	HCA/Animal Care	Chameleon	animal care operations (kennel, veterinary, licensing)	Moderate	
6	HCA/Environmental Health	Envision	tracks field inspections/violations & generates billings	Moderate	
7	Library	iBistro	library management system for patrons & materials	Moderate	
8	PDSD	APPS (Automated Permitting and Planning System)	enterprise system for permit processing & accounting	Moderate	
<b>OTHER/OPERATIONAL SYSTEMS</b>					
1	Child Support Services	Chrono	document case events/history	Moderate	
2	Child Support Services	SwiftView ActiveX Control	view printed ARS forms on-line	Moderate	
3	Clerk-Recorder	CATS 2000	issue marriage licenses	Moderate	
4	Clerk-Recorder	Grantor/Grantee	maintain public records for real property	Moderate	
5	Clerk-Recorder	Vitals 2000	issue certificates (birth, death, marriage)	Moderate	
6	Clerk-Recorder	Electronic Recording	electronic recording of real property documents	Moderate	
7	Clerk-Recorder	FBN (Fictitious Business Name)	business name database	Moderate	
8	H&CS/Office on Aging	SAMS (Senior Access Management System)	records services provided & funds used by contractors	Moderate	
9	H&CS/Office on Aging	Refer (Office on Aging Information & Referral)	provides and tracks resource information for seniors	Moderate	
10	H&CS/Veterans Service Office	VID (Veterans Information Database)	claims filing and statistics	Moderate	
11	HCA	Contract Services - UCI	monitor services provided by UCI under contract	Moderate	
12	HCA	Contract Services - Western Medical	monitor services provided by WestMed	Moderate	
13	HCA/Correctional Medical	CMS (Correctional Medical Services)	medical records & tracking of pharmacy medications	Moderate	
14	HCA/Public Health	CaseWatch	management of AIDS cases & services	Moderate	
15	HCA/Public Health	Immunization and Vaccine	tracks patient immunization and vaccine usage	Moderate	
16	John Wayne Airport	Access Control System	monitor entrance/exits of all secured access areas	Moderate	
17	PFRD/Agricultural Commissioner	Weights & Measures	reporting and billing for inspections	Moderate	
18	PFRD/Engineering & Permits	County Property Permits	records & tracks information on county permits	Moderate	
19	PFRD/Facilities Operations	FM1 (Facilities Management)	manage maintenance work orders & billing countywide	Moderate	
20	PFRD/Public Works	MainStar (operations & maintenance)	track work requests from public complaint to completion	Moderate	
21	PFRD/Transportation	FleetAnywhere	manage all transportation fees, charges, billing	Moderate	
22	Probation	JAIS (Juvenile Intake Assessment System)	juvenile intake assessment	Moderate	
23	Probation	Adult Probationer - Shared Terms & Conditions	shares info on adult probationers w/law enforcement	Moderate	
24	Probation	AI (Adult Intake System)	automates the first stage of the adult intake process	Moderate	
25	Probation	CABS (Computerized Arrest & Booking System)	store photos of all probationers	Moderate	
26	Probation	Penal Code 1210 Violations system	information sharing w/HCA & drug treatment providers	Moderate	
27	Probation/Institutional Services	IMS (Institution Management System)	juvenile in-custody mgmt - booking, assessing, tracking	Moderate	
28	Registration & Elections	EIMS (Election Information Management System)	voter registration info, election data, precinct info	Moderate	
29	Registration & Elections	BOSS (Ballot Original Software System)	creates ballots and tabulation databases	Moderate	
30	Registration & Elections	Mapitude	GIS for precinct and district boundaries	Moderate	
<b>PERSONNEL SYSTEMS</b>					
1	CEO/Human Resources	ORS (Online Recruitment System)	on-line job application management	Moderate	
2	CEO/Human Resources	TRAC	applicant tracking	Moderate	
<b>SELF-GOVERNED/SELF-MONITORED SYSTEMS</b>					
1	Sheriff-Coroner	various	Because of the circumstances surrounding the S-C systems (confidentiality, compliance with DOJ rules, etc.), their systems are self-monitored.	Moderate	
<b>TREASURY SYSTEMS</b>					
1	TTC/Treasurer	Bloomberg	on-line securities trading	Moderate	
2	TTC/Treasurer	Gateway	middleware between Quantum and Bloomberg	Moderate	
3	TTC/Treasurer	GQ	reconciles Quantum to Bloomberg	Moderate	
4	TTC/Treasurer	Check Reconciliation	demand account reconciliations	Moderate	
5	TTC/Treasurer	Fund Accounting	middleware for converting A-C data	Moderate	
6	TTC/Treasurer	Deposit Order Reconciliation	D/O reconciliation	Moderate	
7	TTC/Treasurer	Back Office	cash accounting system	Moderate	
<b>LOWER RISK SYSTEMS - ALL</b>					
1	CEO/Human Resources	Virtual Rideshare Survey	commuter survey information	Low	
2	CEO/Human Resources	Online Training Registration	class enrollment management	Low	

KEY INFORMATION SYSTEMS INVENTORY

AGENCY/DEPARTMENT	APPLICATION/SYSTEM	DESCRIPTION	RISK RATING	LAST AUDIT
3	CEO/Information & Technology	NSD Portal	Low	
4	CEO/Information & Technology	GUARD (Global User Access Request Database)	Low	
5	CEO/Information & Technology	ELVIS (Electronic Labor Verification Info System)	Low	
6	Child Support Services	UIFSA Documaker	Low	
7	Child Support Services	Clerk-Recorder Abstract Imaging	Low	
8	Child Support Services	Union Bank Check Vision	Low	
9	Child Support Services	Wells Fargo Check Viewing	Low	
10	Child Support Services	File Automation System	Low	
11	Child Support Services	Merdien / MTE	Low	
12	Clerk of the Board	CAMS (Comprehensive Agenda Mgmt Solution)	Low	
13	District Attorney	Personnel Threats	Low	
14	District Attorney	Branch Court Services	Low	
15	District Attorney	Juvenile Truancy Tracking	Low	
16	District Attorney	Petty Cash Check Generation	Low	
17	District Attorney	MCLE (Mandatory Legal Education Credit tracking)	Low	
18	HCA/Information Technology	TouchPaper	Low	
19	John Wayne Airport	ABT (Airport Business Toolbox)	Low	
20	John Wayne Airport	CAD (Computer Assisted Design)	Low	
21	John Wayne Airport	TAMIS (Tracor Airport Management Info Systems)	Low	
22	John Wayne Airport	FMMS (Facilities Maintenance Management System)	Low	
23	John Wayne Airport	AVI (Automated Vehicle Identification)	Low	
24	John Wayne Airport	FIDS/BIDS (Flight & Baggage Information System)	Low	
25	John Wayne Airport	Automated Attendant	Low	
26	PDSD & PFRD	Expediter	Low	
27	PFRD	Management Status Report	Low	
28	PFRD/HB&P	OSO (Overage/Shortage Online Reporting System)	Low	
29	PFRD/Publishing Services	Publishing Services Automated Requisitions	Low	
13	Higher Risk Systems			
80	Moderate Risk Systems			
29	Lower Risk Systems			
122	Total Systems			

13	Higher Risk Systems
80	Moderate Risk Systems
29	Lower Risk Systems
122	Total Systems



# County of Orange

## Internal Audit Department

### Customer Survey of Audit Services

Name of Auditor(s): \_\_\_\_\_

Name of Audit: \_\_\_\_\_

Please rate 1 to 5  
 1 being Strongly Disagree  
 5 being Strongly Agree  
 (The higher the score the better the evaluation)

Score	Evaluation Factors
	1. Were the auditor(s) professional and courteous?
	2. Did the auditor(s) communicate the objectives of the audit?
	3. Did the auditor(s) discuss findings with you in a timely manner?
	4. Did the auditor provide helpful, reasonable, and practical recommendations?
	5. Did the auditor listen to your concerns and explore options in a partnering way?
	6. Was the audit report clear and accurate?
	7. Did the auditor(s) demonstrate satisfactory technically knowledgeable relating to internal control?
	8. Were your experiences with the auditor(s) positive?
	9. Would you recommend the services of the auditor(s) to your colleagues?
	10. Would you choose this auditor(s) to conduct other audit assignments?

Thank you for your insights and comments, we value your input.

Customers Name: \_\_\_\_\_

Date: \_\_\_\_\_

Customers Title: \_\_\_\_\_





**INTERNAL AUDIT DEPARTMENT  
Risk Assessment Questionnaire**  
Department / Agency: \_

General Factors	Notes	*Risk Rating		
		Dept.	IAD	Comb.
<p><u>Department/Agency Changes:</u> This factor represents the degree of continuity within the Department/Agency since the last audit (or 5 years). Items to be discussed include:</p> <ul style="list-style-type: none"> <li>- Management/staff turnover.</li> <li>- Significant increases/decreases in staffing and/or duties.</li> <li>- New or eliminated programs/functions.</li> <li>- Significant changes in laws/regulations.</li> <li>- Reorganization/organizational changes.</li> <li>- Information Technology systems.</li> </ul> <p><u>Operating Environment:</u> This factor reflects the exposure or extent to which the Department/Agency may be affected its operating environment. Items to be discussed include:</p> <ul style="list-style-type: none"> <li>- Public image.</li> <li>- Safety/environmental concerns.</li> <li>- Government regulation and reporting.</li> <li>- Decentralized management.</li> <li>- Operating results highly sensitive to economic factors.</li> <li>- Difficulties in achieving business goals.</li> <li>- Pending litigation.</li> <li>- Business continuity</li> </ul> <p><u>Risk Assessment:</u> Describe the Department/Agency's risk assessment process.</p> <p><u>Internal Controls:</u> The design and adequacy of an internal control structure is one indication of exposure. Items to be discussed include:</p> <ul style="list-style-type: none"> <li>- Management's responsibility for internal controls.</li> <li>- Management has monitoring processes to assess the performance of internal controls (i.e. self-assessments, reviews, hotlines, etc.).</li> </ul>				

**INTERNAL AUDIT DEPARTMENT  
Risk Assessment Questionnaire**

<b>Financial Process</b>	<b>\$ Volume</b>	<b>Nature of Transactions</b> (centralized/decentralized, manual/automated, number of transactions)	<b>Audit Coverage</b> (includes internal and external audits)	<b>*Risk Rating</b> Dept. / IAD Comb. Agcy.		
Cash Receipts						
Revenues/Accounts Receivable/Collections						
Fee Recovery		Last Fee Revision:				
Cash Disbursements – Accounts Payables						
Revolving Funds						
Procurement/Contract Administration						
Payroll						

# INTERNAL AUDIT DEPARTMENT Risk Assessment Questionnaire

Financial Process	\$ Volume	Nature of Transactions (centralized/decentralized, manual/automated, number of transactions)	Audit Coverage (includes internal and external audits)	*Risk Rating	
				Dept. / Agcy.	IAD Comb.
Trust Funds/Special Department Funds					
Budgeting					

Department/Agency Meeting Date: \_\_\_\_\_

Present from Department/Agency: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

Present from Internal Audit: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_



**INTERNAL AUDIT DEPARTMENT  
INFORMATION TECHNOLOGY  
RISK ASSESSMENT QUESTIONNAIRE**

**Dr. Peter Hughes, Director**  
400 W Civic Center Drive 232  
Santa Ana California 92701-4521  
714.834.5475 (main)  
714.834.2880 (fax)

**INSTRUCTIONS**

- To be completed by the departmental/agency I/T manager.
- List all applications utilized by your department/agency on this page.
- For each application listed that is considered key, please complete the questionnaire on the next page.
- Contact Scott Suzuki (Senior Internal Auditor) @ 714.834.7651 with any questions regarding this questionnaire.

<b>DEPARTMENT/ AGENCY</b>	
<b>I/T MANAGER</b>	
<b>APPLICATION(S)</b> List all applications	•

**COMPLETE THE WORKSHEET ON THE NEXT PAGE FOR EACH ABOVE LISTED APPLICATION CONSIDERED TO BE KEY**

COMPLETE THIS WORKSHEET FOR EACH KEY APPLICATION

<p><b>APPLICATION NAME</b> Name, acronym, and version/release number (if applicable)</p>	
<p><b>PURPOSE</b> Functions performed by the system</p>	
<p><b>PLATFORM</b> Mainframe, AS/400, server, etc.</p>	
<p><b>OPERATING SYSTEM</b> Windows XP/2000/NT, Unix, etc.</p>	
<p><b>INTERFACES</b> With other applications, including those outside your department/agency</p>	
<p><b>NATURE OF DATA COLLECTED</b> Financial accounting, personal information, statistical data, etc.</p>	
<p><b>IMPLEMENTATION DATE</b> Approximate</p>	
<p><b>SOURCE</b> Off-the-shelf - unmodified; Off-the-shelf - modified; Developed - in-house; Developed - third-party</p>	
<p><b>SUPPORT</b> In-house or third-party</p>	
<p><b>UPGRADES/ CHANGES</b> Enhancements to system, program and/or platform changes (other than patches)</p>	
<p><b>LAST AUDIT</b> Date of last audit and by whom (including reviews by consultants)</p>	
<p><b>PROBLEMS/ CONCERNS</b> Security, data integrity, processing, change control, etc.</p>	

AREA	RATING CRITERIA	RATING
<b>CRITICALITY</b>	40% 5 - Application is critical to the County's mission 4 3 - Application is critical to the department/agency's function 2 1 - Application is non-critical	
<b>COMPLEXITY</b>	20% 5 - Application interfaces with external systems; complicated database; complex operations 4 3 - Application is moderately complex 2 1 - Application is not complex; stand-alone, few users	
<b>INFORMATION CONTROLLED</b>	20% 5 - Application tracks financial assets and/or confidential data 4 3 - Application tracks assets less readily disposable or subject to fraud and/or theft 2 1 - Application contains public information or less sensitive data	
<b>SYSTEM LOAD</b>	10% 5 - Application processes hundreds of transactions per day 4 3 - Application processes hundreds of transactions per week 2 1 - Application processes hundreds of transactions per month	
<b>MATURITY</b>	10% 5 - Application was deployed less than one year ago 4 3 - Application is in its second year or its first year after significant upgrades/modifications 2 1 - Application is in its third year or later	





**INTERNAL AUDIT DEPARTMENT**  
**DEPT/AGENCY**  
**AUDIT # - Y/E**

PREPARER  
 REVIEWER

**SUBJECT** GENERAL I/T CONTROLS QUESTIONNAIRE

**PURPOSE** To perform [W/P] audit program step [step number] and review the organization's general computer controls.

General I/T controls related to all aspects of the I/T function, including administration, software acquisition and maintenance, physical and online security over access to hardware and software and related data, back-up planning in the event of unexpected emergencies, and hardware controls.

There are six major categories of general controls:

- Security planning and management – provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the organization's I/T-related controls
- Access controls – limit or detect access to I/T resources and protect these resources against unauthorized modification, loss, or disclosure
- Application software development and change controls – prevent unauthorized programs or modifications to an existing program from being implemented
- System software – controls that limit and monitor access to system programs that control the I/T hardware and secure applications supported by the system
- Segregation of duties – policies and procedures that prevent one individual from controlling key aspects of the I/T-related operation
- Service continuity – controls to ensure critical operations continue without interruption or are promptly resumed when unexpected events occur; ensure critical data is protected

Complete the following form via corroborative inquiry (where possible) with I/T management and personnel.

**SOURCE**

CONTROL QUESTION		Y/N/NA	REMARKS
<b>SECURITY PROGRAM PLANNING &amp; MANAGEMENT</b>			
<b>RISK ASSESSMENT</b>	1. Are risk assessments performed and documented?		Risk assessments considers data sensitivity and integrity and the range of risks to the entity's systems and data; identifies threats and vulnerabilities
<b>SECURITY PROGRAM PLAN</b>	2. Is a security plan documented and approved?		Describes the security program policies and procedures including major facilities and operations, training, personnel controls, incident response, continuity of support, technical security.
	3. Is the plan kept current?		Should be periodically reviewed and reflect current conditions
<b>SECURITY MANAGEMENT STRUCTURE</b>	4. Has a security management structure been established?		Assigning personnel to develop, communicate, and monitor compliance with security policies
	5. Is there an information security manager?		Sufficient authority, independence, access to resources, training
	6. Are information security responsibilities clearly assigned?		Responsibilities and expected behavior of all users including who owns computer resources/data files

CONTROL QUESTION		Y/N/NA	REMARKS
	7. Is there an ongoing security awareness program?		Including first time training for employees, contractors, users and IT staff on the left.
	8. Are security policies distributed to all employees?		
	9. Is there an incident response capability enabled?		
<b>PERSONNEL POLICIES</b>	10. Are references and/or background checks performed on employees with access to critical/confidential data?		
	11. Are confidentiality or security agreements required for employees with access to critical/confidential data?		
	12. Are scheduled vacations required?		
	13. Are regular job or shift rotations required?		
	14. Are there termination and transfer procedures?		Ext. interviews, return of company assets, notification to IT security.
	15. Are skill needs accurately identified in job descriptions?		
	16. Is there a training program?		IT personnel have the expertise to carry out their responsibilities.
<b>SECURITY PROGRAM MONITORING</b>	18. Is the information security program subjected to periodic review?		
	19. Do major applications undergo independent review every three (3) years?		
<b>ACCESS CONTROLS</b>			
<b>CLASSIFY INFORMATION RESOURCES</b>	20. Have classifications and criteria been established and communicated to resource owners?		Determine the level of protection and then classify on categories and criteria.
	21. Have resources been classified based on risk assessments?		Owners classify information based on risk assessments which identify threats, vulnerabilities, and potential negative effects.
<b>AUTHORIZED USERS</b>	22. Are user access authorizations documented and approved?		Standard forms, approved, sent to security managers.
	23. Do owners periodically review access authorization listings for appropriateness?		
	24. Is remote access limited and justified in writing?		
	25. Do security managers review access authorizations?		Review and document any questionable access requests.
	26. Are changes to security profiles by security managers reviewed by an independent party?		
	27. Is security notified immediately upon the termination of an employee?		
	28. Are emergency and temporary access authorizations documented, approved, and automatically terminated?		
	29. Are forms used to document approval for archiving, deleting, or sharing data files?		

	CONTROL QUESTION	Y/N/NA	REMARKS
	30. Are there policies for how data programs and files are to be protected when shared with other entities?		Owners should determine with whom and by what means resources can be shared
<b>PHYSICAL CONTROLS</b>	31. Have facilities housing sensitive and critical resources been identified?		
	32. Have significant threats against sensitive and critical resources been identified?		
	33. Is access to sensitive areas limited by use of entry devices?		
	34. Does management periodically review lists of employees with access to sensitive facilities?		
	35. Are keys or other entry devices required to access the data center?		
	36. Are unissued keys and entry devices secured?		
	37. Do emergency procedures ensure only authorized personnel are allowed to re-enter after an emergency?		
<b>VISITORS</b>	38. Are visitors to sensitive areas formally signed in and escorted?		
	39. Are entry codes changed periodically?		
	40. Are visitors, contractors, and maintenance personnel properly authenticated via appointments or identification checks?		
<b>PASSWORDS</b>	41. Are password assigned for specific individuals and not groups?		
	42. Are passwords controlled by the user and not subject to disclosure or sharing per policy?		
	43. Are passwords changed periodically (30-90 days)?		
	44. Are passwords not displayed when entered?		
	45. Are passwords at least six (6) alphanumeric characters in length		
	46. Are password prohibited from reuse for at least six (6) generations?		
	47. Is the use of names or words prohibited?		
	48. Are generic user ID's and passwords not used?		
	49. Are attempts to logon with invalid passwords or user ID's limited to three (3) attempts?		
	50. Is the account lockout duration set for indefinite/until reset by administrator?		
	51. Are personnel files matched to actual system users or are user ID's periodically reviewed for terminated/ transferred employees?		
	52. Are password files encrypted?		

CONTROL QUESTION		Y/N/NA	REMARKS
	53. Do users of tokens, key cards, or other key devices maintain possession of what they have been assigned?		
	54. Do users of tokens, key cards, or other key devices understand they must not loan/share these items and must report lost/stolen items immediately?		
<b>ACCESS PATHS</b>	55. Is an analysis of logical access paths conducted whenever system changes are made?		
<b>DATA FILES AND SOFTWARE</b>	56. Is security software utilized to restrict access?		
	57. Is access to security software limited to those charged with security administration duties?		
	58. Are workstations automatically logged off after a period of inactivity?		
	59. Are inactive user accounts monitored and/or removed when not needed?		
	60. Are parameters of security software set to provide access to files as authorized and restrict access in all other instances?		
	61. Are naming conventions used for resources?		
<b>DATA DICTIONARY AND DATABASES</b>	62. Are there logical controls over the database and data dictionary which restrict access to data files as necessary?		
	63. Is the use of database utilities limited and monitored?		
	64. Are access and changes to the database software controlled?		
	65. Is the access to security profiles in the data dictionary and database security tables limited?		
<b>TELECOM-MUNICATION ACCESS</b>	66. Is the use of dial-in remote access limited?		Dial-up capabilities only
	67. Is there a dial-in access control software in use?		
	68. Does it verify user ID's and passwords before granting access?		
	69. Does it protect sensitive data during transmission?		
	70. Does it automatically disconnect at the end of a session?		
	71. Does it maintain activity logs?		
	72. Does it restrict access to tables that define network options, resources, and user profiles?		
	73. Does it allow only authorized users to shut-down network components?		
	74. Does it monitor dial-up access by monitoring the source of calls or by disconnecting and dialing back at preauthorized phone numbers?		
	75. Does it restrict in-house access to telecommunications software?		

CONTROL QUESTION		Y/N/NA	REMARKS
	76. Does it control changes to telecommunications software?		
	77. Does it ensure data is not accessed or modified by unauthorized users?		
	78. Does it restrict and monitor access to telecommunications hardware and facilities?		Security audits
	79. Does the opening screen viewed by a user provide a warning against unauthorized use and that activity will be monitored?		
	80. Are dial-in numbers not published and changed periodically?		
<b>ENCRYPTION</b>	81. Is encryption used to protect sensitive data?		
<b>EQUIPMENT DISPOSITION</b>	82. Are there procedures to clear sensitive data and software from discarded or transferred equipment and/or media		
<b>MONITORING ACCESS</b>	83. Is all activity involving access to and modifications of sensitive data logged?		
	84. Are security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, reported to management and investigated?		
	85. Do security managers investigate security violations and report results to management?		
	86. Are violations summarized and reported to senior management?		
	87. Are access control policies and techniques modified when violations and related risk assessments indicate that such changes are appropriate?		
<b>APPLICATION DEVELOPMENT</b>			
<b>SOFTWARE DEVELOPMENT LIFE CYCLE</b>	88. Is there a documented SDLC methodology?		
	89. Have program staff and other employees involved in developing and testing software been trained in the use of the organization's SDLC?		
	90. Are software change request forms used to document requests and related approvals?		
	91. Are change requests approved by both system users and I/T?		
	92. Have clear policies restricting the use of personal and public domain software been developed and enforced?		
	93. Is virus identification software in use?		
<b>TESTING</b>	94. Have test plan standards been developed for all levels of testing that define responsibilities for each user group?		
	95. Are detailed system specifications prepared by the programmer and reviewed by management?		

CONTROL QUESTION		Y/N/NA	REMARKS
	96. Are software changes documented so they can be traced from authorization to the final approved code?		
	97. Are test plans which define responsibilities for each user group documented and approved?		
	98. Are unit, integration, and system testing performed and approved before system deployment?		
	99. Is a comprehensive set of test transaction and data developed which represents various activities and conditions that will be encountered during processing?		
	100. Is live data not used in testing of program changes (except to build test data files)?		
	101. Are test results reviewed and documented?		
	102. Are program changes moved into production only upon documented approval from users and I/T management?		
	103. Is documentation updated for software, hardware, I/T support, and users updated when a new or modified system is implemented?		
	104. Do I/T personnel periodically review production program changes to determine whether access controls and change controls have been followed?		
	105. Are emergency change procedures documented?		
	106. Are emergency changes approved by I/T management?		
	107. Are standardized procedures used to distribute new software for implementation?		Only for entities with multiple locations
	108. Are implementation orders, including effective date, provided to all locations where they are maintained on file?		
<b>SOFTWARE LIBRARIES</b>	109. Is library management software used to produce audit trails of program changes?		Mainframe and mid-range computers
	110. Is library management software used to maintain program version numbers?		
	111. Is library management software used to record and report program changes?		
	112. Is library management software used to maintain creation/data information for production modules?		
	113. Is library management software used to maintain copies of previous versions?		
	114. Is library management software used to control concurrent updates?		
	115. Are separate libraries maintained for program development and maintenance, testing, and production programs?		
	116. Is source code maintained in a separate library?		

CONTROL QUESTION		Y/N/NA	REMARKS
	117. Is access to all programs, including production code, source code, and extra program copies, protected by access control software and operating system security?		
	118. Are all deposits and withdrawals of programs tapes to and from the library logged?		
	119. Does a group independent of the users and programmers control the movement of programs and data among libraries?		
	120. Are before and after images of program code maintained and compared to ensure only approved changes are made?		
	121. Do programmers not have access to production data?		
<b>SYSTEM SOFTWARE ACCESS</b>			
	122. Do policies and procedures for restricting access to systems software exist and are they up to date?		Mainframe and mid-range computers
	123. Is access to system software restricted to a limited number of personnel?		
	124. Are application programmers and computer operators prohibited from accessing system software?		
	125. Is there approved documentation justifying access to system software?		
	126. Are the access capabilities of system programmers periodically reviewed for propriety?		
	127. Is the operating system configured to prevent circumvention of security software and application controls?		
	128. Is all access to system software files logged automatically?		
	129. Are vendor supplied default logon ID's and passwords disabled?		
	130. Is remote access to the system master console restricted?		
<b>SYSTEM UTILITIES</b>			
	131. Are there polices and procedures for using and monitoring use of system software utilities?		Mainframe and mid-range computers
	132. Are responsibilities for using sensitive system utilities clearly defined?		
	133. Are responsibilities for monitoring use clearly defined?		
	134. Is the use of sensitive system utilities logged using access control software reports or job accounting data?		
	135. Is the use of privileged system software and utilities reviewed by I/T management?		
	136. Is inappropriate or unusual activity in using utilities investigated?		

CONTROL QUESTION		Y/N/NA	REMARKS
	137. Are system programmers activities monitored and reviewed?		
	138. Are management reviews performed to determine if control techniques for monitoring use of sensitive system software are functioning as intended?		
<b>CHANGES</b>	139. Do policies and procedures exist for identifying, selecting, installing, and modifying system software?		
	140. Do procedures exist for identifying and documenting system software problems?		
	141. Do new system software versions or products and modifications to existing system software receive proper authorization via a change request document?		
	142. Are new system software versions or products and modifications to existing system software tested and approved before implementation?		
	143. Do procedures exist for controlling emergency changes?		
	144. Is installation of system software scheduled to minimize the impact on data processing and is advance notice given to users?		
	145. Is migration of tested and approved system software to production use performed by an independent library control group?		
	146. Are outdated versions of system software removed from production libraries?		
	147. Is the installation of all system software logged to establish an audit trail?		
	148. Is vendor supplied software still supported by the vendor?		
	149. Is all system software current and does it have complete documentation?		
<b>SEGREGATION OF DUTIES</b>			
<b>INCOMPATIBLE DUTIES</b>	150. Do policies and procedures for segregating duties exist?		
	151. Are distinct systems support functions performed by different individuals?		See Segregation of Duties Matrix
	152. Does no individual have complete control over incompatible transaction processing functions?		See Internal Controls Questionnaire
	153. Are compensating controls performed for organizations with limited resources?		See Internal Controls Questionnaire
	154. Are I/T personnel not users of the organization's applications?		
	155. Are daily operating procedures for the data center adequately documented?		

<b>SUBJECT</b>	GENERAL I/T CONTROLS QUESTIONNAIRE	<b>AUDIT</b>		<b>PAGE</b>	<b>WIP</b>
<b>DEPT/AGCY</b>		<b>PRINT DATE</b>	2/17/2004 09:48	<b>8 / 12</b>	
<b>URL</b>	C:\Documents and Settings\Scott\My Documents\Audits\Forms\IT ICQ 4.doc				

CONTROL QUESTION		Y/N/NA	REMARKS
	156. Do documented job descriptions accurately reflect assigned duties and responsibilities?		
	157. Do documented job descriptions included definitions of knowledge, skills, and abilities required for successful performance of the position?		
	158. Do employees fully understand their duties and responsibilities?		
	159. Does senior management provide adequate training to emphasize segregation of duties principles?		
	160. Are responsibilities for restricting access by job positions clearly defined, understood, and followed?		
<b>ACCESS CONTROLS</b>	161. Do physical and logical controls help restrict employees to authorized actions?		
	162. Are employee's performances monitored to ensure objectives in job descriptions are carried out?		
	163. Are management reviews performed to determine that control techniques for segregating incompatible duties are functioning as intended?		
<b>MONITORING</b>	164. Are documented procedures available for I/T employees?		
	165. Do operator instruction manuals provide guidance on system operation?		
	166. Do application manuals provide instruction on operating specific applications?		
	167. Are operators prevented from overriding file label or equipment error messages?		
	168. Are personnel provided with adequate supervision and review?		
	169. Are operator activities recorded automatically in a system history log?		
	170. So supervisors periodically review the system history log?		
	171. Is system startup monitored and performed by authorized personnel only?		
	172. Are parameters set during the initial program load (IPL) in accordance with established procedures?		
	<b>SERVICE CONTINUITY</b>		
<b>ASSESSMENT</b>	173. Is there a list of critical operations and data that prioritizes data and operations?		
	174. Have resources supporting critical operations been identified and documented?		
	175. Have emergency processing priorities been documented and approved?		
<b>PREVENTION</b>	176. Are backup files created on a prescribed basis?		

CONTROL QUESTION	Y/N/NA	REMARKS
177. Are backup files rotated off-site?		
178. Are system and application documentation stored at an off-site location?		
179. Is the backup storage site removed from the primary site?		
180. Is the backup storage site protected by environmental and physical access controls?		
181. Have fire suppression and prevention devices been installed?		
182. Is there adequate HVAC (heating, ventilation, air conditioning) with redundancy?		
183. Do building plumbing lines not endanger the data center or are shut-off valves and procedures documented?		
184. Does a UPS (uninterruptible power supply) or backup generator protect critical I/T resources?		
185. Are environmental controls periodically tested?		
186. Is eating, drinking, and smoking prohibited in I/T facilities?		
187. Have I/T employees received training and do they understand their emergency roles and responsibilities?		
188. Do I/T employees receive periodic emergency incident training?		
189. Are emergency procedures periodically tested?		
190. Do hardware maintenance policies and procedures exist?		
191. Is routine periodic hardware preventative maintenance scheduled and performed?		
192. Is all maintenance performed documented?		
193. Is there flexibility in data processing operations to accommodate scheduled and unscheduled maintenance?		
194. Is there spare backup hardware available for critical applications?		
195. Is there a help desk function?		
196. Are goals for the availability of data processing and on-line services established?		
197. Are records maintained on the actual performance in meeting service schedules?		
198. Are problems and delays encountered, the reason, and the elapsed time for resolution recorded and analyzed?		
199. Does management periodically review and compare actual service levels with established goals?		

CONTROL QUESTION		Y/N/NA	REMARKS
<b>CONTINGENCY PLAN</b>	200. Are changes of hardware and software scheduled to minimize the impact on operations?		
	201. Is advance notice given to users of hardware or software changes?		
	202. Is there a documented contingency/disaster recovery plan?		
	203. Does it reflect current conditions?		
	204. Has it been approved by key user groups including senior management and I/T management?		
	205. Does it clearly assign responsibilities for recovery?		
	206. Does it include detailed instructions for restoring operations?		
	207. Does it identify an alternative processing facility and backup storage facility?		
	208. Does it include procedures to follow when the data/service center is unable to receive or transmit data?		
	209. Does it identify critical files?		
	210. Is it detailed enough to be understood by all of the organization's managers?		
	211. Does it include identification of computer and telecommunications hardware?		
	212. Has it been distributed to all appropriate personnel?		
	213. Does the plan provide for back-up personnel?		
	214. Have user departments developed adequate manual processing procedures until I/T resources are restored?		
	215. Are several copies of the contingency plan stored securely at off-site locations?		
	216. Is the contingency plan periodically reassessed to reflect changes to hardware, software, and personnel?		
	217. Have contracts been established for a back-up data center and other needed facilities?		
	218. Have alternative telecommunication services been arranged?		
	219. Have arrangements for travel and lodging of necessary personnel been arranged?		
<b>TESTING</b>	220. Has the current contingency plan been tested under conditions that simulate a disaster?		
	221. Have test results been documented and presented to senior management?		
	222. Was the contingency plan corrected for any deficiencies identified during testing?		

<b>SUBJECT</b>	GENERAL I/T CONTROLS QUESTIONNAIRE	<b>AUDIT</b>		<b>PAGE</b>	<b>W/P</b>
<b>DEPT/AGCY</b>		<b>PRINT DATE</b>	2/17/2004 09:48	<b>12 / 12</b>	
<b>URL</b>	C:\Documents and Settings\Scott\My Documents\Audits\Forms\IT ICQ 4.doc				



**INTERNAL AUDIT DEPARTMENT**  
**[PROJECT NAME]**  
**AUDIT #XXXX – AS OF [DATE]**

PREPARER \_\_\_\_\_  
 REVIEWER \_\_\_\_\_

<b>SUBJECT</b>	<b>INFORMATION TECHNOLOGY BACKGROUND QUESTIONNAIRE</b>
<b>PURPOSE</b>	Perform D.1 Audit Program step G.4 and gain an understanding of the organization's I/T operations.
<b>REQUIRED</b>	Contact the organization's information systems manager, systems analysts, and technical specialists and complete this worksheet.
<b>SOURCE</b>	This worksheet was completed via discussion with

<b>ORGANIZATION &amp; STAFFING</b>	<i>Describe the organization and staff at the entity's data processing and software development sites. Obtain an organization chart, if available.</i>		
	<b>NAME</b>	<b>TITLE/DUTIES</b>	<b>CONTACT</b>
<b>ENVIRONMENT</b>	<i>Describe the significance and nature of programs and functions supported by automated systems.</i>		
	<i>Describe the types of computer processing performed (stand alone, distributed, or networked).</i>		
	<i>Describe the significant wired communications networks (physical and logical), wireless networks, and interfaces to other computer systems. Obtain a network diagram.</i>		
<b>HARDWARE</b>	<i>Describe the CPU including manufacturer(s), year acquired, location(s), and operating system(s) (version).</i>		
	<i>Describe file servers including manufacturer, year acquired, location, and operating system (version).</i>		
	<i>Describe any networked, portable, and stand-alone computers, and/or PDAs including manufacturer(s), location(s), and operating system(s) (version).</i>		
	<i>Describe printers including manufacturer(s) and location(s)</i>		
<b>SOFTWARE</b>	<i>Describe the general types and extent of significant software used (manufacturer, version, implementation date and whether in-house developed, purchased-not modified, purchased-modified by in-house or vendor)</i>		
	<i>Describe any program development tools including vendor, application, and version (TSO, ICCF, ISPF).</i>		
	<i>Describe any programming language compilers (RPG, Obsidian).</i>		
	<i>Describe any database management applications (DB2, IMS, IDMS, ADABAS, Oracle, Datacom).</i>		

	<i>Describe any report writing applications (Crystal Reports, Easytrieve).</i>
	<i>Describe any tape management applications (CA-1, TMS, EPAT).</i>
	<i>Describe any program library software (Panvalet, Librarian, Endeavor).</i>
	<i>Describe any job scheduling applications (CA-7, Manager, Scheduler).</i>
<b>INFORMATION SECURITY</b>	<i>Describe the nature of software utilities used at computer processing locations that provide the ability to add, alter, or delete information stored in data files, databases, and program libraries.</i>
	<i>Describe the nature of software used to restrict access to programs and data at computer processing locations (ACF2, RACF, Topsecret).</i>
	<i>Describe any dial-up security software (Defender, Leehma, Auditor)</i>
<b>OPERATIONS</b>	<i>Describe where data is input and reported.</i>
	<i>Describe any dial-up and/or remote access capabilities.</i>
	<i>Describe how EDI is used (if applicable).</i>
	<i>Describe significant changes since any prior audits/reviews.</i>
	<i>Describe the entity's reliance on service bureaus or other agencies for computer processing support.</i>
	<i>Describe the results of past internal and external reviews.</i>
	<i>Describe any recent software implementations or hardware upgrades and any future plans.</i>
	<i>Describe any changes in the I/T organization, culture, or practices.</i>
	<i>Describe any significant staffing changes.</i>
	<i>Describe any problems users have identified in data processing (e.g., system failures, errors in processing results, delays or loss of data, difficulty in obtaining changes to systems, lack of training or support, difficulties with conversions or changes to new systems).</i>
	<i>Describe I/T management concerns related to the I/T environment.</i>