Choice and Consequence
2009 COSO Monitoring
Ten Big Things for Small Shops
How confident are you with your audit results?

In today’s increasingly challenging business environment, organizations are looking to internal audit to take on the role of trusted advisors that provide ongoing assurance. Our technology provides the analytic capabilities to give you greater insight into key risk areas in your audit...

confidence in your results...

freedom from doubt

Your Technology Committee has been hard at work upgrading the library and soliciting new contributions. Go to the AHIA Web site (www.AHIA.org) to see the improvements to our Audit Library:

- Older PDF documents have been converted to easily useable formats!
- There has been a significant increase in the number of documents available!
- This is an invaluable resource to all of our members!
- Cash prizes to be awarded to top submitters!
- Thank you to all who have donated documents to this project!

The campaign will continue—submit your items to AuditLibrary@ahia.org today!
New Perspectives is a refereed and peer-reviewed journal intended to focus on topics critical to professionals involved in healthcare internal auditing, compliance, and monitoring.

New Perspectives is published quarterly — March, June, September, and December.

Yearly subscription rates, including postage are $65, payable in U.S. funds. No refunds or cancellations. Send publication and subscription inquiries, address changes and other inquiries to the Association of Healthcare Internal Auditors, Inc.

10200 W. 44th Ave. #304
Wheat Ridge, CO  80033
Phone: (303) 327-7546
Toll-Free Phone: (888) 275-2442
Fax: (303) 422-8894
E-mail: ahia@ahia.org.

New Perspectives, its editors and the Association of Healthcare Internal Auditors, Inc. are not responsible for the opinions and statements of its contributors and advertisers. The authors do not necessarily reflect the official policies of AHIA nor does AHIA endorse any products. AHIA does not attest to the originality of the author’s content.

Reprints of any portion of New Perspectives may be used for educational or instructional purposes only, provided the following statement appears on each reprint: “Reprinted with permission from New Perspectives, Journal of the Association of Healthcare Internal Auditors, Inc. Volume/Number.”

Copyright 2009, Association of Healthcare Internal Auditors, Inc.

Feature Articles

5  Ten Big Things for Small Audit Departments
   by Steve Stanek

8  CobiT Framework: Bon Secours Health System Best Practice
   by John Gulitti, CISA, CISSP and Bryon Neaman, CPA, CIA

14  2009 COSO Monitoring Guidance—FAQs
    by Sridhar Ramamoorti, Ph.D., ACA, CPA, CITP, CIA, CFE, CFSA, CRP, CGAP, CGFM, CIA, FCPA

19  Auditing Pay Practices: When the CEO Talks, We Listen
    by Renee Jaenicke, CPA, CIA

26  Reconsidering Audit Opinions: Audit Report Redesign
    by Jason McKinney, CIA, MBA

35  Establishing the Foundations: Effectively Monitoring Internal Control Systems
    by Sridhar Ramamoorti, Ph.D., ACA, CPA, CITP, CIA, CFE, CFSA, CRP, CGAP, CGFM, CIA, FCPA, Forrest Frazier, CPA and Jessica Dill, CIA

39  Ethics and Healthcare: Every Choice Has a Consequence
    by Chuck Gallagher

45  Interview with AHIA Chair Mark Eddy, CPA

51  Moving to the Next Level: Consulting Skills for Internal Auditors
    by John J. Hall, CPA

Columns

12  Ethics at Work: The Lessons of Susan Boyle for Ethics Programs
    by Marianne M. Jennings, J.D.

17  From The IIA: What’s Your Professional Quotient?
    by Trish Harris

24  Legal Insights: HITECH Act
    by Hope R. Levy-Biehl

30  Report Writing: A Few Good Words—Writing Report Opinions
    by Sally F. Cutler

33  Construction Auditing: Auditing Field Reports and Logs
    by Ron Risner

42  Billing and Reimbursement: Here Come National Drug Codes, ICD-10, Modifier 25, and RAC Extrapolation
    by Duane C. Abbey, Ph.D., CPA

44  Letters to the Auditor: Birds of a Feather…and How Their Behavior can Help an Auditor
    by John Landreth, CPA, CFE, CHC

47  The IT Perspective Column: Privacy: Our Next Organizational Challenge?
    by Dan Swanson

55  Accounting Matters Column: Economic Stimulus: Major Implications for Privacy and Security of Electronic Health Records
    by Jan Hertzberg, CISA, CISSP., and Jim St. Clair, CISSP, PMP

About AHIA

57  New Perspectives Journal Wins Awards for Publication Excellence

59  AHIA Membership Application
From the Editor

By Kenneth E. Spence, CFE

We’ve said it before—“It’s a great time to be an internal auditor!” For us the era of the internal auditor began with the dot-coms in 1995. Most of those firms bet on brand recognition and market share, but without a sustainable business model against which to execute. They also managed to evade deployment of sound business best practices. In 2000 that bubble burst. Not long after, starting in late 2001 came a string of seemingly singular events that made Enron, WorldCom, Global Crossing, Adelphia, Tyco, HealthSouth and others household names. Different companies in different industries in different parts of the country but the same old song—corporate fraud and misconduct. The line of ethical misconduct was crossed many times, largely enabled by gatekeepers’ duties seemingly obfuscated by lucrative financial incentives.

Enter Sarbanes-Oxley with the requirement to evaluate systems of internal controls. Many in senior management complained about the cost to comply. Few, if any, were sympathetic about the significant cost ineffective and missing internal controls had on investors as well as on investor confidence in our country’s financial systems.

Hello sub-prime mortgage mess. In 2007 we awoke to why our homes had been going up in value so quickly. It also brought us charges of more corporate fraud and misconduct, in addition to incredible top-management compensation packages. How do you spell greed? A call for corporate transparency went out across the land. The electorate brought the country a new administration in Washington which promptly ushered in ‘bailouts’ and new legislation. Lay-offs, rising unemployment, foreclosures, mergers, bankruptcies, consumer spending reductions, increased taxes, and public services cutbacks have been the fallout.

Internal auditing has established a beachhead amidst these conflicts. Soon you will be updating your risk assessment and developing next year’s audit plan. In times like this your audit plan should include those risks that impede adequate cash flow, access to capital, and liquidity. It should also address inventories (booked and un-booked), and confirm billing and accounts receivables processes. Other identified key risks and their mitigation scenarios (best case, worst case, and steady state) need to be on the audit plan. You should watch those balance sheet items carefully. We hope you will consider New Perspectives articles as part of your planning process. They highlight many other issues you should be concerned with.

The lineup of articles in this issue of New Perspectives provides an excellent basis for moving forward in the new audit year. Whether it’s the latest on COSO Monitoring Guidance, or implementing a CobiT Framework, auditing a new payroll system, employing consulting skills, understanding consequences of choices, redesigning audit reporting, or advice for small audit shops. It’s all there, and our cast of outstanding columnists continues to shower you with their sage wisdom.

We can be certain of uncertainty. The epidemic of greed, fraud, and corporate misconduct will persist, thus giving pro-active internal audit departments many opportunities to provide valued services to their organizations. The tag line in an Aspen, Colorado newspaper says it best we think, “If you don’t want it printed, don’t let it happen.” That could be our battle cry in these turbulent times.

Read well. NP
From the Chair

Development

By Mark Eddy, CPA

This column should be published at approximately the time of the AHIA National Conference. As such, I’d like to discuss—development. I hope you have or will be attending our San Diego, CA conference. The Conference Committee worked diligently to create a solid multi-track education opportunity for you and all our teammates.

Self-development has never been more important or challenging than now. We’ve looked previously at the value AHIA provides; this continues to be a challenge during these interesting economic times.

What is the biggest impact the economic crisis has had on internal auditing? Our ongoing self-development keeps us focused on adding value to our organizations and, thus, maximizing our importance as assets to our stakeholders.

The Obama administration and Congress have expressed a willingness to overhaul our healthcare system. My opinion of whether any potential change is good or bad is irrelevant. What is important is our professional preparedness to assist our organizations through whatever changes may be enacted. I am reminded of the saying that “progress requires change, but not all change is progress.” In my column last quarter, I addressed the need for internal auditors to be conversant regarding several topics such as revenue streams, payment models, cash flow and capital generation. Additionally, we must read, listen, discuss, and consider potential change implications to healthcare delivery methods, quality requirements, reimbursement structures, and other areas. How will we help our organizations survive and thrive in a change environment? Invest time in your self-development in conjunction with your teammates at the office, in government, and in AHIA and other professional associations.

I hope your self-development reading is varied. Don’t get bored reading the same thing; keep it fresh and gain others’ perspectives of how they look at life. Many of us report to the audit committee and/or perform audit procedures related to governance. I recently read The Snowball Warren Buffett and the Business of Life by Alice Schroeder and found one paragraph from the book to be quite insightful.

“He said he had a short set of questions for the audit committee at Berkshire Hathaway:

- If the auditor had prepared the financial statements herself (as opposed to their being prepared by the company’s management), would they have been prepared the same way?
- If the auditor were an investor, could he understand how the company had performed financially from the way the financial statements were presented and described?
- If the auditor were in charge, would the company follow the same internal audit procedures?
- Did the auditor know about anything the company had done to change the timing of when sales or costs were reported to investors?

If auditors are put on the spot, Buffett said, they will do their duty. If they are not put on the spot…well, we have seen the results of that.”

These questions drive to the core of auditor independence and objectivity, knowledge of the business and industry, internal controls, regulatory compliance, and transparent reporting. These questions are as relevant to the internal auditor as to the external auditor. Ask yourself these questions about your own organization. Are you comfortable with your answers? Would your audit committee be comfortable with your answers? If not or you don’t know the answers, perhaps you have identified some areas on which to focus your self-development. Look for classes, or network and discuss with your fellow AHIA teammates—the Listserv might be a useful tool.

Sincerely,
Mark Eddy
Chair, AHIA
Dear Editor:

One of the things I like about New Perspectives is the connections. In the February 2009 issue, I made the following connections:

One of the co-authors of the article Prevent Construction Fraud: Using Good Internal Controls is Ed Williams. I heard Ed speak on Data Mining at last year’s AHIA conference. It was a great presentation which I took back to my team. We selected some of his recommendations, applied them, and benefited from the analyses. Based on his presentation at AHIA, I, in my role as a committee chair for another professional organization, invited Ed to speak on the same topic. He did a great job (again) and received high scores as a speaker. His current article on construction fraud fit in with the construction audits we have underway.

The article on The Board and Wild Animals Don’t Like Surprises contributed by columnist John Landreth was especially timely as our Board was recently asking how we could take our ERM process to the next level. I shared the article with them as part of our discussion. It was timely, pertinent, and covered a broad range of issues for Board consideration. It connected with the Board, as the list of issues written about is what we had discussed internally and with our auditors.

And finally, the article on IT Internal Audit: Safeguarding your Hospital’s Risks authored by Scott Smith provided me with some good perspective as we work through our IT internal control risk assessment. We engaged a consulting firm to help guide us through this process. The article helped us ask the right questions and scope the engagement appropriately. When I saw that he was the author, I made a point of reading his article.

New Perspectives is practical, focused, and addresses current IA issues and concerns. Keep up the good work.

Catherine Wakefield, CPA, CIA, CHC, FHIMA
Vice President, Corporate Compliance and Internal Audit
MultiCare Health System
Tacoma, WA 98415-0299

Healthcare Organization ERM: Five First Steps
Dear Editor:

Enterprise risk management is a ‘hot topic’ in internal audit and management circles these days. Many publications give a general idea of what ERM is about, but there are few sources for usable guidance in approaching a risk assessment project encompassing the entire enterprise.

Justine Dover’s article (February 2008 issue) Healthcare Organization ERM: Five First Steps, lays out a step-by-step process for obtaining executive inputs concerning possible risks; organizing and displaying this information; and seeking answers regarding how to control and reduce the most significant risks.

One side comment: I’d be very interested in the rest of Justine’s questionnaire (only a few questions were presented). But, as a practical tool to jump-start a risk assessment effort, this article rocks! Thanks, Justine.

Dan McCroskey
Internal Business Auditor
MedCentral Health System
335 Glessner Ave.
Mansfield, OH 44903

continued on page 7

Tell us what you think of this issue of New Perspectives. We can be reached at:
Email: newkes@comcast.net or editor@AHIA.org
Post: 49 Park Street
Newport, NH 03773

Letters may be edited for clarity and length.
Ten Big Things for Small Audit Departments

By Steve Stanek

Executive Summary

Internal auditors face a problem common to many others in the business world: bigger responsibilities—but not-so-big resources. This is especially true in small internal audit departments, where resources are sparse and growing responsibilities can stretch them dangerously thin. As a result of this, it’s important to discuss ten big things small audit shops do incorrectly, and how they can do things right, using resources more efficiently.

Joel Kramer, Managing Director of the Internal Audit Division of the MIS Training Institute, speaks from experience on this topic as a former Director of Internal Audit, “I have made every one of these mistakes,” he says.

Mistake 1: Acting like a Large Department

“Many small departments try to act like big ones,” says Kramer. “They have too many manuals and forms, too many meetings, too much review, too much report writing. They do not realize they do not need all the bells and whistles. If you have a small department, do you really need a complicated time-reporting system that a department of 50 or 100 has? Probably not.”

The idea, of course, is to do what is necessary to add value to the organization using the resources that are available. Trying to make a small department look like a large one can add bureaucracy rather than value, according to Kramer. He recalls one small audit department that required three complete work paper reviews before issuing the audit report. “When people come from public accounting, they bring the public accounting mentality with them,” he says. “That was the case here.”

He says there are three main ways to do more with less: improve productivity of processes; be more risk-based to eliminate audit steps and audits that do not focus on key risks; and make full use of technologies.

Mistake 2: Hiring the Wrong People

Kramer says many internal audit shops focus too much on people from the Big Four firms, hire people who are not self-starters, are too compliance oriented or are too much of a specialist.

“A small department cannot afford a bad hire,” Kramer says. “If you have a department of eight people and one is a loser, 12 percent of your department is not performing.” He suggests two strategies to reduce the chances of making a bad hire. One is to have potential auditees review final candidates. Those people can bring a fresh and valuable perspective to the hiring process. Another is to have the in-charges meet candidates to assess how they may work together.

“When you bring the people in charge to the process, they feel really involved and have such different insights,” Kramer says. “When you are a director or manager, your natural inclination is to look at the potential growth in people. The in-charge will ask, ‘How will this person work with me in the trenches?’ It is really important to maximize both.”

Mistake 3: Making Audits Too Long

Long audits consume resources that could be used elsewhere. They often result from a lack of focus on key risks and end up at least partly unread, according to Kramer. “We ask, ‘How long should an audit be?’ I was brought up with asking, ‘What is management’s ability to absorb your findings?’ An audit should be only as long as management’s ability to absorb,” Kramer says. “Maybe you do not look at the entire revenue cycle during one audit. Maybe you accomplish this in three or four shorter audits. If you have shorter audits you have shorter reports, and management has reports that are easier to read, understand and absorb.”

Mistake 4: Lacking Creativity in Acquiring People

Small audit departments often have difficulty competing with large companies when it comes to hiring staff. One way around the problem is to use recovery firms that receive a portion of whatever funds are recovered as a result of audits. The organization makes some financial recovery without having to add staff. Audit shops can also borrow people within the organization. Another excellent source could be people who have recently left the organization in a buy-out or retirement.

“Some people do not fully retire,” Kramer says. “They want to continue using their brain. There are wonderful people like this who could help.”

Sometimes certain specialty firms conduct audits at a lower cost than the in-house audit shop. “As an example, there are people who specialize in construction or derivative auditing who can be productive from the first day,” Kramer says.
Kramer says many small audit departments do a poor job of promoting the ways in which the department adds value to the organization. He suggests audit departments create an annual report of two to three pages to show what the department has brought to the company in the last year. He also suggests using an intranet, brochures and newsletters to promote the department.

This promotion can be done in a variety of ways, including providing useful suggestions for employees. “You could provide tips for traveling with a laptop computer, as an example,” Kramer says. “Or you could let them know, ‘Here is why we need to ask this,’ when you are looking at certain expenses.” Marketing resources can help polish up reports, especially with the help of a professional graphics department.

Attending the right meetings is important, too. “You want to be strategic with meetings, so they help you better position the department,” Kramer says. “Let people know we have people; here is how we use them; here are their tools; here is their knowledge and experience. You want to engage people in the organization to use the skills of the people in the audit department, and that is what your marketing message should do.”

**Mistake 6: Failing to Effectively Network**

Kramer reports that he is often surprised at how little the people in small internal audit departments network with others either within or outside the organization. There are usually internal groups, as well as industry groups whose members could be helpful to internal auditors.

Kramer says, when he was an internal audit director, he developed an internal group that included the assistant controller, people from international marketing, and the domestic manufacturing department. They would meet periodically to discuss what his department was doing and tell him what was happening in their areas.

“I wanted to ensure I was using resources effectively,” Kramer says. “It worked very well.” He also suggests becoming active in the local chapter of The Institute of Internal Auditors (IIA) and attending MIS/IIA conferences and symposia as well as other events where fellow professionals would be present. Professional training also can be used as a networking opportunity. “Pick training where you can network,” Kramer says.

**Mistake 7: Reinventing the Wheel**

Too many small departments fail to use resources that are already in hand, including the attest firm and networking groups. They also err in assuming certain risks do not apply to small departments when, in fact, they do.

“People will share,” Kramer says. “Go to a class list of where you were in training and find someone there who could help you—be flexible. Last year’s risks are not necessarily this year’s risks.”

**Mistake 8: Improperly Using Technology**

Many small departments create too many forms and templates, flowchart too deeply, ban use of the Internet, and do not strategize retrieval packages, according to Kramer.

“There is good technology and bad technology,” he says. “I have heard of many instances where technology has slowed things. I have asked [ACL executives], ‘What is the percentage of clients that use their software to its maximum capacity?’ They say no more than 20 percent. Many times people do not use IDEA [Data Analysis Software], ACL, or other packages properly. People get too comfortable with templates, and that can stifle their creativity.”

**Mistake 9: Improperly Using Senior Management**

Another common mistake is a failure to deliver information top management and audit committee members need. Sometimes reports are issued at the wrong time. Other times reports overwhelm readers with too much information or provide the wrong information.

“Audit committees need guidance from internal audit,” Kramer says. “If you want more resources, have your department report ready before the budget process, so they can see the value internal audit can provide.”

Information overload is another problem. “Many reports give too much information and too little knowledge,” Kramer says. “In the financial services industry now, people are going to be looking hard at this,” noting collapses of major financial institutions or government loans and bailouts despite the reporting requirements of the Sarbanes-Oxley Act (SOX) and other laws and regulations.

**Mistake 10: Thinking World-Class Departments must be Big**

Kramer stresses that world-class status has nothing to do with size. Being able to define what would add value to the organization and take appropriate actions makes an audit shop world-class.

“It is important to have good people, address key risks, and set doable goals for adding value,” Kramer says. “In the last five years, we have had SOX, Enterprise Risk Management, significant changes in technology, and headlines like Société Générale (a European financial services company that reported billions of dollars of losses in fraudulent trading). If audit shops improve and modify to keep up with these changes, they will add value. It is not about doing something 100 percent better. It is about doing 100 things one percent better.”

**What Is A Small Department?**

Kramer considers a small audit shop to be one with fewer than 10 employees. He stresses, though, that even the largest companies can have small audit shops.

“A few years ago, I held seminars for a small department, which included people from Fortune 50 companies,” he says. “Sometimes you have small groups within a larger department that treat themselves as separate.” Usually this is done to focus resources on a particular area of...
the company, from either a business or geographic perspective. He recalls one large US company that devoted a small audit group within a larger department to one small unit in Europe.

Kramer admits one potential benefit of a small operation can be the ability to run itself leaner than a large operation. Small internal audit operations though, have the same responsibilities as large shops.

“They must ensure compliance with the same laws, address the same risks as other companies in their industry, and face the same questions from the audit committee. The challenge to a small shop is to do these things with whatever resources they have.” NP

Steve Stanek is a contributing writer to KnowledgeLeader. Reprinted with permission of KnowledgeLeader(SM) provided by Protiviti®. ©2008 Protiviti Inc. All rights reserved.
30-day free trials to KnowledgeLeader are available. AHIA and KnowledgeLeader have an affinity relationship which permits AHIA members to purchase KnowledgeLeader subscriptions at a discount ($500 per user per year vs. $595).

Letters — continued from page 4

Ethics at Work: Of Puzzles and Faint Signals

Marianne Jennings has done it again—provided us with invaluable insight into some of the most amazing stories of business ethics and conduct gone amuck! Her column in the last issue, “Ethics at Work: Of Puzzles and Faint Signals”, provides internal audit practitioners with advice and guidance that goes beyond the professional standards and textbook analytics and procedures we many times unquestioningly employ. A lot of the lists of “red flags” for fraud that we rely on now seem grossly deficient. Thanks to Marianne we now know that numbers can be too good to be true, we should beware of the icon, and icons surround themselves with weakness and/or friends and relatives.

Mike Fabrizius
Vice President, Internal Audit
Sharp HealthCare

HIPAA enforcement is here.
Feel ready?
It’s time for a CheckUp™

CheckUp™: CMS HIPAA Security Readiness Audit

Securing the mission of care.

IT Security | Compliance | eDiscovery
IT Audit | Data Protection | BC/DR
Risk Assessment
www.cynergistek.com
CobiT Framework: Bon Secours Health System Best Practice

By John Gulitti, CISA, CISSP and Bryon Neaman, CPA, CIA

Executive Summary

Convincing IT and management concerning application of sound internal control can at times be a challenge. Internal auditors have an ally in Control Objectives for Information and related Technology (CobiT). Representing experts’ consensus of good practices, CobiT sets forth a commonsense framework that internal auditors can rely upon for guidance when considering the effectiveness of internal controls in information technology (IT).

The Audit Services department at Bon Secours introduced the CobiT framework to educate management about internal control in IT applications and systems and to obtain its acceptance for use in audits. By combining this framework with Bon Secours own policies, Internal Audit is now able to successfully apply this approach to system implementation projects and general technology audits. Using color-coded scorecards quickly communicates the status of system implementation and application control effectiveness in the IT audits the department undertakes.

Introduction

Control Objectives for Information and related Technology (CobiT), authored by the IT Governance Institute (ITGI) and promulgated by the Information Systems Audit and Control Association, is an ideal framework for considering the effectiveness of internal controls governing information technology. CobiT, as defined by the ITGI, “provides good practices across a domain and process framework and presents activities in a manageable and logical structure. CobiT’s good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.”

The Bon Secours Health System Inc. (BSHSI) Internal Audit services team serves as an independent, objective, assurance and advisory service designed to add value and improve operational effectiveness of our organization. The work of BSHSI Internal Audit includes robust and pervasive reviews of complex technology platforms and applications supporting healthcare operations. This includes electronic medical records (EMR), system enterprise resource planning (ERP), and data center operation facilities that support twenty-eight different healthcare entities that provide a combination of acute care, senior services, and home care programs.

The CobiT framework was introduced to BSHSI Senior IT Management in 2005 in an effort to educate and gain acceptance of its use. The initial goal was to be able to provide a relevant accepted governance authority that complimented existing information technology control policies in order to provide Internal Audit with additional standards to audit against. In addition, it allowed us to remain independent with respect to establishing IT policy.

The four CobiT domains; Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME) have provided us direction in our technology audit work. This article will focus on our use of these domains in system implementation and general information technology audits.

Applying CobiT in System Implementation Reviews

It is the policy of the Bon Secours Internal Audit to provide timely reporting of audit results to management and the Audit and Compliance Committee. Consistent with this policy is the provision of real-time assessments pertaining to the implementation of significant applications. These assessments are performed prior to application implementation to give management and the Audit and Compliance Committee an objective view of the ‘readiness’ of the application, from a technology and user perspective. Our assessments are issued in a scorecard reporting format.

The use of a scorecard report is an ongoing measurement of risk and control monitoring to determine if a process or project is being managed within acceptable standards or controls. A scorecard provides the reader with current assessments on the status of task completions, assessments on the status of the proper balancing of risks and controls across several project areas, timely notification to management of any variances (including deficiencies that do not meet control expectations), and a consistent scoring methodology using red, yellow and green indicators.

A practical use of scorecard reporting is illustrated by our current implementation of an electronic medical
A clinical information system that will assist in the transformation of the organization. The timeline for the implementation is a committed five-year rollout which began in 2007 and is expected to end in 2012 or sooner. There are three phases for the project. The first phase of the implementation was a six month planning period. The second phase was a 12 to 18-month development of clinical content and workflow design. The third phase is a system-wide rollout and optimization period.

The currently defined control areas are primarily targeted at information systems concepts. Internal Audit has defined nineteen individual sections that comprise our systems development life cycle which spans all three phases of the EMR project. Along with our existing information technology standards for project management, the expected controls and risks, if controls were not in place, were identified from various sections of CobiT and used to develop test work to assess the implementation at various stages.

Some of the specific control areas evaluated as part of our scorecard report include:

- Budget (PO 5.3 IT Budget Process and PO 5.4 Cost Management)
- Project Management (PO10.7 Integrated Project Plan)
- Status Reporting (PO10.13 Project Performance Measurement, Reporting, and Monitoring)
- Model Build (AI 2.2 Detailed Design and AI 2.5 Configuration and Implementation of Acquired Application Software)
- Software Change Management, (AI6.1 Change Standards and Procedures and AI7.4 Test Environment)
- Unit Testing, (AI7.2 Test Plan)
- Data Conversion, Validation and Interfaces, (AI7.5 System and Data Conversion) System Integration Testing (AI 17.7 Final Acceptance Test)
- Training, (AI 17.1 Training and DS 7.1 Identification of Education and Training Needs & DS 7.2 Delivery of Training and Education)
- Go-Live (AI 4.2 Knowledge Transfer to Business Management, (AI 4.3 Knowledge Transfer to End Users and AI 4.4 Knowledge Transfer to Operations and Support Staff)

We have found that by using interim scorecard reporting we can communicate identified opportunities for control enhancement to management in a timely manner and in a format that is consistent with normal project status reports. When evaluating the adequacy of controls for a scorecard, a score of Green indicates the area is meeting stated objectives in defined strategy. A score of Yellow indicates the area contains one or more key expected controls that are not being executed according to defined strategy, and a score of Red indicates that the successful implementation may be jeopardized because controls are inadequate.

The following is an example of a section of our scorecard for Software Change Management.

### Applying CobiT in General Technology Audits

When using CobiT in our general information technology audits, the process of incorporating the framework to our audit work is broken down into numerous stages. The first stage is to compare the scope of the audit with the CobiT control objectives for the function or process being audited. For instance, in a recent physical security audit, our scope was to determine the effectiveness

### Scorecard for Software Change Management

<table>
<thead>
<tr>
<th>Control Area</th>
<th>Expected Controls</th>
<th>Risk if Expected Controls Not in Place</th>
<th>Key Areas Needing Improvement</th>
<th>Strategy</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Software Change Management (CobiT® - AI6.1 Change Standards and Procedures and AI7.4 Test Environment)</td>
<td>A. Unauthorized or improper changes to software impact the implementation timeline and critical path.</td>
<td>Change management processes do not require approval by key stakeholders.</td>
<td>YELLOW</td>
<td>GREEN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>B. Improper changes to application could cause extensive re-testing.</td>
<td></td>
<td></td>
<td>GREEN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C. Timing of changes could affect the work load of individuals.</td>
<td></td>
<td></td>
<td>GREEN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>D. Environments are out of sync resulting in incorrect work flows and potential errors.</td>
<td>The current TRAINING environment has not been maintained with changes applied to Production resulting in end users not being trained on current workflows and processes.</td>
<td></td>
<td>GREEN</td>
<td></td>
</tr>
</tbody>
</table>

September 2009  
Association of Healthcare Internal Auditors  
New Perspectives  
9
of Information Technology’s physical access controls that ensure computing facilities access is properly authorized, and protections and safeguards were in place, in order to ensure the availability of information systems assets. A gap analysis between the documented control environment and CobiT control objectives was performed. This was our starting point in the planning process that was accomplished by reviewing the organization’s current policies and procedures for physical security against CobiT (section DS12, Manage the Physical Environment). Our goal was to ensure we had identified all the control objectives for the audit scope. In this case there were five specific control objectives within DS 12. We eliminated section DS 12.1, Site Selection and Layout because it was evaluated and risk assessed previously during initial construction of the facilities. It was concluded that our scope was in accord with the remaining sections of DS12. In the event we concluded the scope of our test work had not identified all the control objectives as identified by CobiT, we would have risk assessed each of the missing elements to determine if they should be added to our scope.

Next, we compared the steps in our existing audit programs to the activities in the CobiT control practices. The goal in this step was to ensure we had identified the appropriate testing activities. When there is no existing audit program, we develop the audit programs using the CobiT control practices. To continue with our physical security example, we developed our audit programs by describing the risks (exposures and effects) that may result from the failure to achieve each objective, the desired control, and the detailed test work to be completed. The following is an example from our audit program highlighting external signage.

We identified unauthorized access to areas when signage specifies high risk areas such as a data center or communication closet. The signage makes it easy for people intent on destruction to identify and locate them. Our desired control stated, (per CobiT DS12.2.2), “ensure that external signs and other identification of sensitive IT sites are discreet.” Our test work included steps to visually observe the entrances to IT locations for indicative signage.

Additionally, we add audit activities required by organizational policy, legal or regulatory guidelines. As a healthcare organization, we are required to comply with HIPAA privacy and security regulations. As part of the physical security audit we also wanted to ensure the testing included assessing compliance with HIPAA standards for physical security. The Physical Safeguards section outlines the necessity of a Facility Security Plan. The covered entity is required “to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.” This regulation aligns with the CobiT Control Objectives section 12.3, Physical Access which advises an organization to, “define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.”

To validate control with respect to this requirement, one of our testing steps to satisfy the Physical Access section was to determine whether locks and electronic monitoring devices such as key card badges and video cameras were in place.

In instances where key card badges were in use, we completed additional testing. This testing consisted of determining if access rights were reviewed on a regular basis. We also tested to determine if monitoring was taking place at all physical locations that hosted critical systems. To accomplish this, we developed Computer Aided Audit Techniques (CAATs) to complete our analysis. This required us to obtain a data extract from the key card system of all people who had been granted access to locations that host critical systems. We also got a data extract from the human resource system of all active employees. Once we secured and normalized both files, we were able to compare the data to identify individuals with access who were no longer active employees. The outcome told us how effectively management utilized employee termination reports received from Human Resources. It also identified where opportunities to institute this reporting were required.

A second form of monitoring tested focused on access times. This required us to obtain another data extract from the key card system that listed all individuals granted access by date and time. Based on the normal operating hours of our Information Technology teams, we established the time window starting at midnight to 6:00 a.m. to evaluate against. All instances of granted access during this time frame were considered exceptions and required management to explain the reason and evaluate these after-hours accesses for appropriateness. The results, in some cases, provided management with the opportunity to improve processes for reviewing access logs on an ongoing basis.

In cases where we note exceptions to the control, we quote the control practices from the organization’s existing information security policies and additionally provide support with references to CobiT. As an example, the following is an excerpt from an audit finding: Information Security policy, Protection from Malicious Software requires operating system security patches be installed and updated on systems at all times. CobiT control practices (DS 5.10.4) also recommend maintaining currency of operating system software by applying all relevant security patches and major updates to the system in a timely manner.

Summary
These few examples demonstrate how CobiT has provided management, and the Audit and Compliance Committee, assurances the control environment is being evaluated against existing information technology control policies complimented by an accepted governance authority. It ensures Internal Audit remains independent from establishing IT policy. For us, CobiT is becoming an organizational way of life. NP
At Grant Thornton, we understand the complex business issues facing today’s health care industry. Our industry-focused professionals work to keep you informed of tomorrow’s issues today.

GrantThornton
Audit Tax Advisory
www.GrantThornton.com

Passion for serving clients, technical expertise and partner involvement have been the hallmark of Grant Thornton LLP in the U.S. for more than 80 years. Plus you get the benefits of Grant Thornton International member firms in 112 countries. Call National Managing Partner Anne McGeorge at 866.328.1247 or visit us at www.GrantThornton.com/healthcare.

Find out how it feels to work with people who love what they do!
Ethics at Work

The Lessons of Susan Boyle for Ethics Programs

By Marianne M. Jennings

For those of you who have been ensconced in the Galapagos and have not heard of Susan Boyle, she is the stunning singer from the mother country’s version of American Idol, Britain’s Got Talent. Ms. Boyle, 47, was jeered when she appeared on stage to perform for the insouciant Simon and his cynical co-judges and even more cynical audience. She sang like an angel, and all were stunned. She has given us the quintessential Cinderella story. From a childhood filled with bullying and struggles with learning disabilities to an adult life devoted to caring for her ill mother, Ms. Boyle offers lessons on depth, on dreams, and, for good measure, on ethics and compliance. Herewith the morals for ethics officers from the Susan Boyle story.

Lesson #1—You Never Know Where You Will Find Gold

Ms. Boyle has not been trained formally and her sole experience was singing with her church choir. We doubted her ability because we could see nothing in her background that signaled talent. In our highly-credentialed world, we develop blinders that prevent us from seeing issues and using valuable information because we cannot get past the weak résumé of the source. Yet in ethical lapses by organizations we do find that there were those within the organizations or outsiders who worked with the organization who tried to warn us but were ignored. Roger Barnes, an employee in the Comptroller’s Office at Fannie Mae in 2004, tried several ways, with detailed memos, to explain the financial missteps and accounting improprieties at Fannie Mae. He was not an executive, he was just an employee and he was ignored. He was also right. Fannie had to make a $7-billion restatement in 2005.

Jim Chanos of Kynikos Investments, a firm no one had heard of, raised questions about Enron that zeroed in on the very accounting and operational issues that would eventually bring about the company’s near-destruction. When he raised those issues, he was vilified. John Olson, an analyst in Houston (and who trusts an analyst from Houston?) was dismissed out-of-hand by Jeffrey Skilling who said that Olson, “Just doesn’t get it.”

At WorldCom there were the bookkeepers who questioned the accounting and were dismissed out of hand. At the defunct Kidder Peabody it was worse. Those who raised questions about a star trader’s numbers were dismissed. And often a nurse who has seen a physician’s error is ignored or jeered. The nurse is, more often than not, right. Recently, an employee disclosed to his supervisor that there was pervasive sharing of answers on the company’s annual training exam. The supervisor dismissed the quiet employee as mistaken. It was not until the employee’s exit interview that the company looked into the allegations and found that the cheating on the annual exam was indeed widespread and longstanding. The company not only had the problem; it lost a good employee through its too-quick-to-dismiss attitude toward a good employee.

Even customers have ideas and information that too often is ignored because we within the organization are the ones with the knowledge and credentials. At a retail store, a customer told the store manager that she had seen an assistant store manager taking clothes from the racks to her car. The manager felt it was too obvious a tactic to be true. An undercover investigator, hired after the shrinkage rate at the store began to see a steady increase, verified what the customer had told the manager months earlier. Listen to the information, regardless of the source. Follow up, despite the lack of credentials. The outward appearance is not an indication of the depth that lies beneath.

#2—The Converse: Outward Appearances May Not Be What They Seem To Be, So Avoid the Confirmation-of-Facts Syndrome

The contestants who competed with Susan Boyle had all the image consultants, outward appearance and trappings of talent. They looked the part. We are taken in by those superficial

The ethics officer needs to unabashedly dig beneath the trappings.
signals of credibility. Look no farther than Bernie Madoff, Lehman Brothers, Merrill and Bear Stearns. There they all were — the titans of the financial markets, who assured us through their appearances and accoutrements that they were the best-of-the-best. When we succumb to the trappings, we fall victim to confirmation of facts. We have certain beliefs and assumptions about individuals and companies because of appearances, so miss signals and even inconsistencies that should be red flags. For example, two years before HealthSouth’s multi-billion-dollar restatement, there was litigation in which employee affidavits documented fraud issues and maintained that the company’s growth was not real. Yet, HealthSouth was the model for the new way of delivering health care, so how could it have problems? At UnitedHealth, it took statistical studies before the board confronted Dr. William McGuire with the problems with options backdating. Star quality can mask misconduct. The ethics officer needs to unabashedly dig beneath the trappings. As New York’s investigation into its officials’ conduct in managing the pension plan unfolds, the revelations about webs of conflicts and the arrests continue to stun because of the star power of those within the treasurer’s office and investment funds who stand accused of a longstanding pay-to-play system of rewards.

Every ethics or compliance officer has experienced the push-back from a manager or officer who responds to an investigation of an employee by saying, “I can’t believe he would be involved in anything such as that!” In the healthcare field we tend to have a bias about really looking into the conduct of the “star,” the doctor or other executive because their departure, we are told, would be the end of civilization. However, just because they look good in person, on paper, and even on the job does not mean there is not trouble afoot.

Lesson #3—Authenticity

Susan Boyle is just herself. In all she says and in all she has done, she remains herself. There is no affectation, no pretense and no dishonesty. This lesson is critical for the ethics officer who wants credibility. The ethics officer who joins in on questionable management activity has no hope in investigations, enforcement, or credibility with employees. For example, at Hewlett-Packard, lawyers and ethics officers alike failed to throw down the flag on the pretexting that had been ordered by the board as a way of monitoring what directors were doing. The conduct was wrong, but the HP folks were looking for a loophole instead of shutting it down.

Good ethics officers never pledge anonymity; they promise only to do all that they can to maintain it. Good ethics officers follow through on investigations and questions. Persistence brings credibility within the organization. The recent legal dust-ups over the responsibility of in-house counsel to disclose to employees who represents whom when questioning begins, is an area of challenge for authenticity. nondisclosure brings, harms credibility and candor.

Who would have thought that an incident from our pop culture could teach us so much about ourselves? Susan Boyle has surprised us with her voice, but stunned us with her forced introspection of our tendency to conclude without facts, judge without looking deeper, and compromise when we know the truth is not yet out there. In the shadow of this 21st century warbler, we realize we could use a little less pre-judgment and great deal more in personal growth, reflection and insight.

Marianne M. Jennings is a professor of Legal and Ethical Studies at the W. P. Carey School of Business, Arizona State University where she teaches graduate courses in the MBA program. Professor Jennings has authored hundreds of articles in academic, professional, and trade journals. Her latest book ‘Business Ethics: Case Studies and Readings,’ was published in January 2009. Her book, ‘The Seven Signs of Ethical Collapse’ (St. Martin’s Press), published in 2006, has received several book awards, including recognition from Library Journal. She may be reached at Marianne.Jennings@asu.edu.

Nothing gives a person so much advantage over another as to remain always cool and unruffled under all circumstances.
~Thomas Jefferson
In 2007, Grant Thornton LLP was selected to lead the development of the new monitoring guidance from COSO (see www.coso.org), and Trent Gazzaway, national managing partner of Corporate Governance, served as project leader. Dr. Sri Ramamoorti, a member of the Editorial Committee of New Perspectives since 2004, is a Corporate Governance partner with Grant Thornton LLP and was on the COSO monitoring guidance authoring team. Sri answers these frequently asked questions to provide background information and help the readers of New Perspectives understand the COSO Monitoring Guidance that was issued in February 2009.

1. Who is COSO and why did they write guidance on monitoring internal control systems?

COSO stands for the Committee of Sponsoring Organizations of the “Treadway Commission” (the National Commission on Fraudulent Financial Reporting was headed by Mr. James Treadway, a lawyer, and issued its report in 1987). The sponsoring organizations of COSO are: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Management Accountants (IMA), the Institute of Internal Auditors (IIA) and Financial Executives International (FEI). The current COSO Chairman of the Board is Dr. Larry E. Rittenberg, Ernst & Young Professor of Accounting at the University of Wisconsin at Madison.

From inception, COSO sought to understand and explore the underlying source of fraudulent financial reporting, typically arising out of weak, circumvented, or overridden internal controls over financial reporting.

Accordingly, they developed the primary guidance titled, “Internal Control—Integrated Framework,” originally published in 1992. The COSO Internal Controls—Integrated Framework established the essential elements of what a good internal control system should contain and look like in general. It is important to understand that it really was always designed to be a conceptual framework to inform practice about what internal control might look like; however, it wasn’t designed to be a normative or prescriptive standard as to how effective internal control should be designed in any and all organizations.

The COSO framework itself has five components: control environment, risk assessment, control activities that help manage or mitigate risk, information and communication that make sure the internal control system has the right information flowing throughout it, and sitting on top of it all, the fifth component is monitoring. Monitoring is supposed to ensure that internal control operates effectively and continues to operate effectively over time. In that vein, when we look at the intent of Sarbanes Oxley Section 404, which is for management to take responsibility for internal control and to be in a position to tell investors that they have good internal control, COSO already had a model and a mechanism for how to support that belief. That model and mechanism is the monitoring component.

If monitoring operates effectively, it should not be a great leap to be able to say publicly that internal control is operating effectively. Yet, we saw companies spending huge amounts of time and energy to comply with the Sarbanes Oxley Section 404 requirements. That had to be happening for one of two reasons: (1) either companies had good monitoring and were not taking credit for it, or (2) they didn’t have good monitoring where they needed it. All of that has nothing to do with Sarbanes-Oxley and everything to do with just what good monitoring looks like. So COSO decided, rightfully so, I think, that we really needed to develop some guidance on what good monitoring looks like so that companies could recognize and take credit for it and fix it where they need it, as well as to get away from these massive fourth-quarter exercises to evaluate internal control.

2. Who is on the team that developed the guidance? What process did they follow to create the guidance?

To find the list of everyone involved, please refer to the published guidance. The people involved on the project are listed at the beginning of both the introduction (downloadable for free from www.coso.org) and the three volumes.

- The COSO board has a total of seven members involved in the project.
- The Grant Thornton team who worked as the primary writers of the material were: Trent Gazzaway (project leader), Jim Burton, Russ Gates (DuPage Consulting LLC), Keith Newton, Sri Ramamoorti, Rick Wood (Canada) and Jay Brietz. We were the primary team vetting the major theoretical issues.
- We also had an internal review team of four people: Andy Bailey, Dorsey Baskin, Craig Emrick (Moody’s Investor Services) and Phil
monitoring throughout the year. This monitoring helps you prioritize the risks and appropriately allocate resources to risk. It allows you to focus on the key controls that need more monitoring attention. When monitoring stops, it's because we know for a fact that internal control systems are not controlled. The biggest reason to have effective monitoring is because we know for a fact that monitoring stops at a general trust for the people that are doing the work. There’s a general belief that if there hasn’t been a problem in the past, and things seem to be working O.K. from an operations perspective, everything must be O.K. from an internal control perspective. Every single restatement that has happened due to error or fraud originated at some point with a general belief that things were O.K. until the discovery that things weren’t O.K., and then it was too late to correct it. We would like to see companies take a more proactive approach for developing the feedback mechanisms so they gather direct information about the effectiveness of internal control throughout the period when they need to.

5. If my company is private, will this new guidance apply?

There is a general belief that the only companies that need to apply this guidance are public companies subject to Sarbanes-Oxley. That really couldn’t be further from the truth. If you generally buy the notion that it is highly desirable to have control over everything that could materially impact your financial statements, then you should not need Sarbanes-Oxley to tell you that! That should be a goal of every organization.

If you get beyond financial reporting, you want to have a reasonable basis that your internal control over operations, compliance with laws and regulations, health and safety issues, and a whole host of issues are working effectively throughout the year. This monitoring guidance is designed to help you do that: to help you prioritize the risks and understand how monitoring can make you comfortable that an internal control system is effective, without necessarily looking at every single internal control, but by focusing on key controls. All the notions in the guidance are applicable to any company, for-profit, not-for-profit, private or public. It doesn’t matter.

6. Why should we follow this guidance? What are the risks if we don’t?

The biggest reason to have effective monitoring is because we know for a fact that internal control systems that are not monitored effectively deteriorate over time. When people aren’t supervised effectively, eventually, what they’re supposed to be doing doesn’t get done or doesn’t get done properly. When that happens, risk increases and the longer it happens, the more risk increases until there’s a catastrophic failure.

Business is changing so much faster than it did 20 years ago. It’s so much more complex today. Risk can occur in a much quicker timeframe and have a greater impact in a shorter period of time than it could just 10 or 20 years ago. So the importance of monitoring is actually increasing as business gets more and more complex.

7. Will following the COSO guidance reduce overall costs of internal control monitoring?

It will reduce the overall cost of the internal control system over time. What I mean by that is if you don’t have
good monitoring, your internal control system is going to deteriorate over time. Not performing effective monitoring is akin to assuming the risk from deferred maintenance.

No organization, whether you’re dealing with financial reporting, operations or compliance with laws and regulations, can afford for material errors to occur. That’s why they are called material errors—they have a significant negative impact on the organization’s objectives. Although effective monitoring doesn’t completely eliminate the risk that a material error is going to occur, it does significantly reduce it. It should, in theory, reduce the overall costs of the entire internal control system over time.

Applying this guidance will reduce the actual cost of internal control monitoring to the extent that companies are performing a massive fourth-quarter exercise that is redundant or being performed solely because there is no other monitoring information available. It will at least spread it out throughout the year instead of being focused in one quarter and could actually reduce the overall cost. NP
From street smarts to emotional intelligence to knowledge of rocket science, there are numerous categories for what one knows. In today’s information-rich world, we have limitless opportunities to grow our knowledge and proficiency. Attending seminars and conferences, participating in online training, reading books that cover a broad spectrum of relevant topics and practices, studying for a professional certification exam, and learning from others through practical, hands-on experience all feed into our individual and collective professionalism.

However, nothing is more important to professionalism than the principles that guide a profession. And for internal auditing, those principles reside within the International Professional Practices Framework (IPPF). Promulgated by The Institute of Internal Auditors (IIA), the IPPF comprises the authoritative guidance for the internal audit profession. This means that the process used to develop, vet, and deliver IPPF guidance is consistent with that of other global guidance-setting bodies worthy of trust. This process ensures transparency, timeliness, clarity, and consistency.

The two categories of authoritative internal audit guidance are MANDATORY and STRONGLY RECOMMENDED. To be in conformance with The IIA’s guidance, a practitioner must follow the mandatory guidance. And although professionals are encouraged to follow the strongly recommended guidance, doing so is not required.

A Professionalism Imperative

The mandatory elements of the IPPF include the official Definition of Internal Auditing, the International Standards for the Professional Practice of Internal Auditing (International Standards), and the Code of Ethics. All of these elements are available free of charge on The IIA’s Web site at www.theiia.org.

The Code of Ethics

The Code of Ethics states the principles and expectations governing behavior of individuals and organizations in the conduct of internal auditing. It describes the minimum requirements for conduct, and behavioral expectations rather than specific activities.

When practitioners adhere to this guidance, they are allowed to state in their reports that, “This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.” This statement clearly depicts the internal audit activity as professional and represents its commitment to best practices and high standards.

Internal Auditing Defined

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Strongly Recommended

Through the IPPF, internal auditors have ready access to additional authoritative guidance that will enhance their professionalism, but with which conformance is not required. Endorsed by The IIA, this strongly recommended guidance provides additional information about and support for conforming to the International Standards and Code of Ethics. Delivered in the form of Practice Advisories, Position Papers, or Practice Guides, it provides timely information on governance, risk, and internal control.
Practice Advisories assist internal auditors in applying the Definition of Internal Auditing, the Code of Ethics, and the International Standards. They address internal auditing’s approach, methodologies, and considerations, but do not cover detail processes or procedures. They promote good practices, including those relating to international, country, or industry-specific issues; specific types of engagements; and legal or regulatory issues. For example, the Practice Advisory “Managing the Risk of the Internal Audit Activity” delineates the risks of audit failure and false assurance, examines reputation risks, and suggests ways to mitigate all three of these risks.

Position Papers assist a wide range of interested parties—including those not in the internal audit profession—in understanding significant governance, risk, or control issues and delineating related roles and responsibilities of internal auditing. For example, “The Role of Internal Auditing in Enterprise Risk Management,” looks beneath the surface of ERM to offer in-depth insights on how internal auditors can make a significant difference in the effectiveness of an organization’s risk management.

Practice Guides provide detailed guidance for conducting internal audit activities, and include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. The Practice Guide category includes such guidance as the Global Technology Audit Guide (GTAG) series. GTAGs provide practical, how-to information about auditing information technology. A recent GTAG—Auditing IT Projects—covers common project management risks and their assessment, examines key focus areas for this type of audit, and explains how internal auditors can actively participate in the review of the projects while maintaining independence.

Ongoing Professionalism

To ensure ongoing professionalism of the internal audit activity and conformance with the International Standards, a Quality Assurance and Improvement Program must be in place. This program includes periodic internal assessments and an external quality assessment (QA) every five years. The external QA demonstrates the activity’s commitment to quality and professionalism, documents its “professionalism quotient,” and delineates recommendations for improvement, based on the International Standards and best internal audit practices. NP

Contributed by Trish Harris on behalf of The Institute of Internal Auditors. The Institute of Internal Auditors (IIA) is the internal audit profession’s global voice, recognized authority, acknowledged leader, chief advocate and principle educator worldwide. Established in 1941, The IIA serves members from all around the world in internal auditing, governance, internal control, IT auditing, education and security. For more information about The IIA, please visit www.theiia.org.
Auditing Pay Practices: When the CEO Talks, We Listen

By Renee Jaenicke, CPA, CIA

Executive Summary
This article discusses our department’s audit of Renown Health’s pay practices, a 946-bed integrated health network located in Reno, Nevada. It was a learning process for us as this was an initial review after conversion from ADP to the Kronos Work Force Management System, a change we were not involved with. Our department lacked IS auditing experience so we opted to collaborate with staff from key departments associated with our work force compensation processes. This proved to be an important element of our overall success. Utilizing their knowledge and our audit expertise the initial audit produced results that more than paid for our department’s annual budget.

Introduction
What do you do when the chief executive officer (CEO) tells you he wants to dedicate one full-time equivalent (FTE) to auditing pay practices year-round? You listen! Prior to this our auditing primarily focused on assisting our external auditors with the annual financial audit. Our first risk based annual audit plan included auditing pay practices. When we presented the results of the risk assessment to the CEO, he stated that he wanted an FTE dedicated to auditing pay practices. This is a tall order since Renown Health has 4,700 employees working at two acute care hospitals, one rehab hospital, a skilled nursing facility, several outpatient clinics and urgent care locations, a medical group, an insurance provider, a group purchasing organization, and a collection agency. Dedicating one FTE to pay practices from a five person staff can be a challenge. However, we are glad we listened!

Obtaining the Data
For this audit to be effective, we needed to have a good deal of data. Since this was an initial post-conversion audit we waited until we had six pay periods of data to review. At Renown, the Decision Support Department performs data downloads and electronic analyses for all departments in the hospital system. As you would imagine, the analysts in this department had their hands full already! They were not used to Internal Audit adding to their already heavy workload. We first solicited their assistance by meeting with the Decision Support Director to explain the value of 100% testing and to establish a productive working relationship with his staff. Once he was on board, we needed to define clearly what we wanted. Our data pull was quite involved, and included the following types of information:

- Employee master data as of the last date of the last pay period.
- Payroll register data for six pay periods.
- Electronic timecard edits and approvals.

Performing the Audit
To date we have performed this audit for three of Renown’s entities: the two acute care hospitals, and our ambulatory centers.

First Pay Practices Audit
We performed the first audit on the larger of our two acute care hospitals. This was our initial operational audit using data analysis and we were not quite sure how to best go about it. This audit took 641 hours to perform because we struggled figuring out the best way to analyze the data. Because we have a limited budget, we could not afford automated technology such as ACL. One

1 This program is also available in the AHIA Audit Library.
team member understood a little about Microsoft Access, so she agreed to try it and become our ‘pay practices guru’. The Access queries took some time to develop.

Equally important was establishing the relationship with Human Resources and Payroll, as well as understanding the data we received. Before analyzing anything, we worked with HR and Payroll to obtain a sound grasp of:

- Pay codes: productive versus non-productive; premium versus non-premium; shift differentials.
- Job codes: how to identify full-time; part-time; per-diem; and more than one job code for the same employee (floats).

As with most internal audit organizations, we try to adopt the principle of ‘no surprises’. That is why it was important to have the buy-in and assistance with HR and Payroll. A representative from HR and from Payroll reviewed each audit step’s results to ensure that we understood the data correctly. Consequently, when we presented the audit report draft, there was agreement with the issues. In fact, they welcomed the audit! It helped them to ensure the identified inconsistencies do not reassert themselves.

Second and Third Pay Practices Audits

We performed the second audit on Renown’s remaining acute care hospital. For this audit, we developed Microsoft Access database queries for each audit step and our audit clients began to gain a better idea of our process. The third audit included all our ambulatory centers. Because we now had a defined process in place and had built productive working relationships with our audit clients the third audit took only 30% of the time the first audit required.

We also had gotten better at analyzing the data and continued to make improvements as we went along. Two specific improvements we made during the third audit relate to how we received data. For example:

- We attempted to determine the electronic timecard edits that increased and decreased pay. Initially, we received downloads that separately indicated the edits that increased pay and the edits which decreased pay. In the first two audits, the Payroll Manager manually reviewed those edits with the highest number of occurrences and found that some of the edits did not actually increase or decrease pay when considered in conjunction with other edits. As such, it would be difficult to develop a consistent algorithm to determine increases and decreases. Also, the Payroll Manager’s process was manual and tedious. Therefore, we decided to change the reporting to include only employees and departments with the largest number of manual edits. As a result, we reported more accurately and reduced the time the Payroll Manager spent working with us on the audit.
- In the first two audits, we considered incremental overtime as being one hour or less per pay period (two weeks). By the third audit, we were able to receive more detailed data which allowed us to define incremental overtime on a weekly basis. As a result we could more effectively determine employees that were actually working incremental overtime without needing to wait until the end of the pay period.

Pay Practices Audit Results

Our work identified three common themes across each of the audits:

A representative from HR and from Payroll reviewed each audit step’s results to ensure that we understood the data correctly. Consequently, when we presented the audit report draft, there was agreement with the issues.

- Policy and practices were not always in sync. In some cases, the practice needed alteration; in others it made more sense to update the policy.
- Kronos users did not understand how to use the system effectively. The Payroll Manager developed Kronos classes to address the concerns expressed when we met with supervisors. These classes are nearly always full.
- We could be saving money by more closely monitoring how what we pay employees in both pay and benefits aligns with the FTE status. We estimate this generated an approximate $2 million in cost savings—which is four times our department’s annual budget!

As a result of our three pay practices audits, the Decision Support department staff designed the same queries, which run on a regular basis and are posted to a Payroll Dashboard. This dashboard is
available to all Renown Health leaders. These queries now cover both of our acute-care hospitals, our rehab hospital, urgent care and imaging centers, the retail locations within the hospitals, and our HMO. This enables continuous monitoring coverage of the entire organization.

HR representatives now are able to meet with each location’s leaders on a regular basis to discuss the reports and how we can ensure that Renown is paying employees correctly. The dashboard reports are hardwired, so we are now going to change our approach to the pay practices audits. Instead of performing the queries ourselves, we may use the queries to determine the extent to which the dashboard reports are effective at addressing the issues noted. Will we still need an FTE next year dedicated to pay practices? We’ll see!

Some of these queries were developed by reviewing an article in New Perspectives by Cliff Therrien (February 2008).

Success Demands More Work

The CEO was so satisfied with the results of our audits, he asked us to do more work related to payroll—meaning to identify potential ghost employees! A ghost employee is someone who receives a paycheck but doesn’t work for the organization. This situation usually requires collusion—between the manager and ‘employee’, or between HR and ‘employee’.

Before the era of direct deposit, identifying ghost employees was accomplished by requiring in-person payouts, meaning each employee is required to personally pick up and sign for their paycheck. Most of our employees’ pay is direct deposited to their bank accounts now. So it is not feasible to hold someone’s pay until they sign for a direct deposit stub. We pondered what audit steps might indicate the existence of a ghost employee. Some of these queries were developed by reviewing an article in New Perspectives by Cliff Therrien (February 2008). By themselves, our query results would not indicate a ghost employee, but when considered in conjunction with others, would indicate further research is required.

Some of our investigation required manual work. For example, based on previous experiences of one of our team members, we looked for employees with the same address as Mail Boxes Etc.®, hotels, or similar locations. We also looked for employees with the same address as vendors. While this match may not necessarily indicate a ghost employee it would indicate that completion of a conflict of interest form is warranted. The Payroll Manager worked with us to submit information to the Social Security Administration (SSA). We found that some married employees had not changed their names with the SSA. Other of our queries included looking for employees who were paid outside their job code range; base pay not within job code range, and duplicates (e.g., more than one employee with the same address, same social security number, same direct deposit bank account, etc.). Each time we identified a match using a ghost employee query, we considered it a potential exception.

We then created a grid by employee, listing each employee, and the query number in a column. We determined which employees had the most potential exceptions and rank ordered these exceptions from highest to lowest. We found hundreds of employees had more than one exception.

Now, we had to determine whether any were actually ghost employees. It was necessary to work with HR to make this determination. But we needed to do this without working with someone who could add a ghost employee to the employee master and/or the payroll master. After consultation with the Vice President of HR, we looked for the employees with more than one exception, who had not logged into the online mandatory compliance training module. Unfortunately, this module does not generate a log-in report. The folks at HR manually looked up 650 employees. These efforts identified four employees who had more than one potential exception and had not logged in to complete online training. We arranged to have these employees pay stubs handed to them by an HR representative. The audit result: No ghost employees were identified! Through these audit procedures we were able to provide assurance that ghost employees did not exist in our organization.

Audit Successes

- The audit identified approximately $2 million cost savings by changing the how the organization pays annual leave. This made our department a profit center with our first audit!
- As a result of the audit, queries and reports were developed that all of leaders in the organization can use to continuously monitor the pay practices of their respective departments.
- By developing standardized working papers, queries, and reports in Access we reduced our audit time by 43% for the second audit and 70% for the third audit.
- Our meetings with supervisors identified misunderstandings about how to perform scheduling and ensure compliance with policies in Kronos. Some of them asked for step-by-step instructions for how to input and edit electronic timecard data. Others asked for an updated pay code list with descriptions. We aren’t Kronos experts, so we sent these comments to the Payroll Manager, who developed Kronos courses based on these interviews. These courses filled up quickly.

The audit identified approximately $2 million cost savings by changing the how the organization pays annual leave.
Audit Program for Pay Practices Audits

System Rules and Reports
1. Match pay rules and system edits to current HR policies and the union contract. (Performed once).
2. Determine what reports are already available from Kronos that can be sent to Supervisors on a regular basis.

Analytical Review
3. Identify the departments and employees with the most call back pay.
4. Identify the departments and employees with the most on-call pay.
5. Identify the departments and employees with the most overtime.
6. Identify the departments and employees with the most manual edits.

Application of Policies and Procedures, Compliance
1. Identify employees with call back pay but no on-call pay.
2. Identify employees with both licensed and non-licensed call pay.
3. Identify employees with licensed call pay who do not have a licensed position.
4. Identify employees with on-call and call-back pay, who work in departments not eligible for this type of pay.
5. Identify employees paid for more than 80 regular hours per pay period.
6. Identify employees receiving bereavement, jury duty, and/or continuing education pay who do not qualify for it.
7. Identify employees receiving shift differential who are not eligible to receive it.
8. Identify employees receiving relocation pay or moving expense reimbursement more than six months after hire date.
9. Identify exempt employees with premium pay.
10. Identify employees whose total work, paid leave, and unpaid leave total less or more than their required FTE hours for all six pay periods.

Efficiencies and Cost Savings
1. Identify employees with on-call pay but no call-back pay (do they really need to be on-call).
2. Identify employees and department with the most incremental overtime.
3. Identify employees paid for more than 18 hours/day average.
4. Identify employees paid more than $10,000 gross and/or $5,000 net in one pay period and review back-up.
5. Identify employees with productive + non-productive hours > standard FTE hours during the same pay period.
6. Identify per diem employees with zero or less than 20 hours and tie to departments with the most overtime.

Authorization
1. Determine whether employees can approve their own timecards as both employee and supervisor.
2. Determine individuals below supervisor who can approve time cards.
3. Determine whether employees can approve as supervisor, timecards for individuals outside their cost center or roll-up.
4. Determine timecards not approved by employees.
5. Determine timecards not approved by supervisors.
6. Determine timecards not approved by either employees or supervisors.

Consistent Pay Practices
Select a sample of supervisors and interview them regarding their understanding of the policies and procedures and have them walk us through how to approve a time card.

Audit Program for Ghost Employees Review

Using Payroll and HR Databases
1. List employees with PO Box addresses.
2. List more than one employee with the same address.
3. List employees in alphabetical order to determine if an employee name has more than one employee ID.
4. List employees in social security number (SSN) order to determine if an employee has more than one SSN.
5. List employees in employee number order to determine if any employee number is out of the normal range.
6. List more than one employee with the same direct deposit account.
7. List employees listed on the latest payroll register but not on the employee master and vice versa.
8. Identify employees with a base rate outside the job code range and obtain authorization for difference.

Using Payroll, HR, and Other Databases
1. List employees not on the system email listing.
2. List employees with the same SSN as the Tax ID for vendors listed in the vendor master.

Manual Work Required
1. Identify employees with the same address as hotels in the area.
2. Identify employees with the same address as Mailbox Etc. or other similar locations.

This program is also available in the AHIA Audit Library.
What We Learned

• Ensure that the Decision Support staff understands exactly what is required, and develops a consistent and reviewed protocol for pulling the data. This way, if someone in Decision Support leaves, another person can provide the data without reinventing the wheel.

• These audits required commitment by HR and Payroll to work with us to ensure we understood the query results. We didn’t want to just crunch numbers. We wanted to know what those numbers meant. This took substantial amounts of their time. Therefore, it is important that Human Resources and Payroll are involved in audit planning and understand the commitment they are making before starting to audit.

• We wanted to establish a positive relationship with people during this audit. This was our first audit, and we wanted to make a good impression. It was important to us not to simply write a report with query results and say “fix it.” We understood that HR and Payroll have perspectives that could help us. Initially, we thought it might be tedious to validate every result with HR and Payroll during fieldwork. However, we soon realized that this investment during the process paid large dividends because at the end of the audit, everyone understood the issues and what needed to be done to address them.

Conclusion

Although we are a small department with new auditors and initially were not sure how to accomplish the CEO’s request, we figured out how we could do it, instead of thinking about why we could not. We did this by working together as a team to come up with ideas about how to use the tools and the knowledge already resident in the department. The individual with Microsoft Access knowledge agreed to increase her knowledge of that product. Other team members contributed ideas on what queries she could run in Access. An individual who had experience looking for ghost employees came up with ideas about how to track them down. We worked with HR to identify their concerns related to compliance with their policies. We met with supervisors to understand their concerns regarding Kronos. It took a lot of work and learning along the way, but in the end, we addressed the CEO’s concerns, established positive working relationships with others at many levels, and saved the organization from expending millions more dollars than necessary!

Renée Jaenicke is the Internal Audit Director at Renown Health, an integrated health network in northern Nevada. She leads a department of five which performs operational audits and external audit work. Chartered in July 2008, her department has identified approximately $2 million in cost savings and just over $1 million increased net revenue opportunities. She may be reached at (775) 982-4117 or via email at RJaenicke@renown.org.
On February 17, 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH Act or HITECH) as part of the American Recovery and Reinvestment Act of 2009 (ARRA). After years of state and local efforts to develop health information infrastructure through the use of health information technology (HIT) and electronic health records (EHRs), the Federal government has taken its first significant step to drive national EHR adoption. In HITECH, Congress uses three basic mechanisms to promote EHR adoption:

- **Pork**, in the form of financial incentives, grants, and loans to defray EHR adoption costs
- **Penalties** down the road for failure to adopt and ‘meaningfully’ use EHRs
- **Privacy** enhancements, to ensure public confidence in the integrity of a nationwide health information infrastructure

Through HITECH, Congress has sent a strong signal of its support for nationwide EHR adoption. For purposes of this column, we highlight two major areas covered by HITECH: (i) Medicare and Medicaid provider incentives and penalties; and (ii) changes to HIPAA and new regulation of personal health record vendors.

**Medicare and Medicaid Provider Incentives and Penalties**

The bulk of federal funds allocated to HIT under HITECH come in the form of enhanced Medicare and Medicaid payments. Providers meeting the criteria for ‘meaningful’ EHR use will have a right to these entitlement payments, as opposed to the discretionary grant funding allocable to other entities that develop, test, provide training for, and analyze the use of, EHRs.

Beginning in 2011, HITECH provides financial incentives and penalties to encourage Medicare-participating physicians and hospitals to move quickly toward adopting ‘certified’ EHR technology. Early-adopting eligible Medicare providers who become ‘meaningful’ EHR users over the next 2-3 years will maximize their incentive payments under Medicare. Late-adopting Medicare providers who wait until after 2015 will have no opportunity to recoup costs associated with the mandated shift toward EHR.

Starting in 2011, HITECH also provides several financial incentives and disincentives to drive EHR adoption among Medicaid providers. The Act authorizes two types of federal matching: (1) a 100% match to States for incentive payments made to Medicaid providers; and (2) a 90% match to States for administration of EHR incentive payments.

Individual providers must waive Medicare incentive payments if they choose to take Medicaid incentive payments. Congress believed that payments to eligible professionals under either program alone would be sufficient to cover substantially all of the costs of adopting certified EHR. This assumption may be flawed. Individual providers should consider compiling evidence for HHS concerning their costs related to adoption and use of EHR.

Children’s hospitals, and acute care hospitals with at least 10% Medicaid volume, can qualify for Medicaid incentive payments. Qualifying institutions can receive both Medicare and Medicaid incentive payments. Medicaid incentive payments to hospitals are calculated similarly to Medicare, (i.e. based on discharges and proportion of
Notably, the Medicare and Medicaid incentive programs make payments after the fact: providers must make up-front investments in EHRs. Both the Medicare and Medicaid incentive programs require that providers certify and/or demonstrate ‘meaningful use’ of certified EHR technology to qualify for payments. However, precisely what ‘meaningful use’ of certified EHR technology entails, as well as the quality measures that physicians will be required to document and report, will be established by the Secretary through the rulemaking process. The Act’s incentives and penalties may be insufficient to drive adoption of EHR technology. In addition, the Act does not expressly provide EHR adoption incentive payments to labs, ASCs, clinics, or long-term care providers. In addition, HITECH does not appear to address the eligibility of physician organizations, such as IPAs.

**Changes to HIPAA and Regulation of PHR Vendors**

HITECH’s drafters showed acute awareness that EHR frightens privacy advocates and large segments of the public, because of the perceived heightened risk it presents for the inappropriate access, disclosure and use of medical information. As a result, the amendments to HIPAA that HITECH contains require providers and suppliers who access patient protected health information (PHI) to abide by enhanced patient privacy and security obligations. HITECH vastly expands HIPAA’s potency and will require correspondingly intensive compliance efforts by providers, suppliers, and now business associates, including self-disclosures of breaches to federal officials and a fining system.

HITECH, which previously applied only to ‘covered entities’ (i.e., healthcare providers, plans, and clearinghouses), now applies directly to business associates, who previously were subject only to contractual liability to covered entities under business associate agreements. Personal health record (PHR) vendors, who previously were outside the scope of HIPAA if their business dealings were directly with consumers, are now subject to privacy and security provisions administered by the Federal Trade Commission (FTC). The Act beefs up the enforcement and penalty provisions of HIPAA, makes them applicable both to covered entities and business associates, and requires the disclosure of security breaches to affected patients, the government, and in some cases the media.

The Act contains several important changes to the Security Rule. The Act defines a ‘breach’ under HIPAA broadly to include unauthorized acquisition, access, use, or disclosure of PHI which compromises the security, privacy, or integrity of PHI maintained by or on behalf of a person. Importantly, the Act excludes from the definition of ‘breach’ unintentional acquisition, access, use, or disclosure of such information, if made in good faith and within the course and scope of the employment or other contractual relationship and if such information is not further acquired, accessed, used, or disclosed.

The federal government will begin providing annual guidance on the most effective and appropriate technical safeguards for complying with the HIPAA Security Rule. Compliance officers should study the annual guidance carefully, as such guidance may de facto have the force of law in determining whether an entity’s actions are sufficiently reasonable to safeguard electronic PHI under HIPAA.

The Act fine-tunes various Privacy Rule provisions, including those on marketing, fundraising, disclosure accountings, disclosure restrictions, and individual patient access to EHRs, and PHR vendor breach notification requirements. The Act requires the Secretary to issue guidance on what ‘minimum necessary’ means for Privacy Rule purposes by August 2010. The Act provides that a covered entity or business associate may not directly or indirectly receive remuneration in exchange for any PHI without a valid authorization specifically indicating that the PHI may be sold by the entity receiving the PHI. This prohibition does not apply in certain limited instances.

The net effect of these amendments is to make HIPAA a vastly more potent and encompassing regulatory scheme for patient privacy. As the potential harm for security breaches rises with the adoption of a nationwide EHR, HITECH seeks a corresponding reinforcement of Federal privacy and security law.

Hope Levy-Biehl, J.D., is a principal with the national health law firm of Hooper, Lundy and Bookman, Inc., the largest law practice in the country dedicated exclusively to the representation of health care providers. Her practice focuses primarily on assisting providers, including hospitals, laboratories, and pharmacies with regulatory compliance, licensure and certification, payment, and operational issues. She can be contacted by phone at (310) 551-8140 or by email at hlevybiehl@health-law.com.
Reconsidering Audit Opinions: 
Audit Report Redesign

By Jason McKinney, CIA, MBA

Executive Summary
Internal auditors are responsible for ensuring audit customers receive accurate, unbiased, relevant, and actionable information on internal control issues and related risks. Although IIA Standards define certain requisites, there are significant allowances for flexibility and customization of the audit report format(s). Internal auditors should take advantage of that flexibility to maximize Audit Committee, Executive Management, and Auditee satisfaction while rendering reports that are useful and relevant within our organizations.

This article summarizes our redesign process and the rationale behind incorporating COSO descriptors to clarify reporting of risk attributes. We seized an opportunity to make our reports more management-friendly and believe the outcome is a better overall product for our organization.

Introduction
Reporting risk impact and likelihood can be a daunting task in the healthcare environment. The combination of the organic risk landscape, complex subject matter, and time scarcity of those in leadership roles requires clear and succinct reporting of risk attributes. Our department aspired to improve audit reporting by addressing the divide between our opinion concerning the effectiveness of controls and the materiality of the risk that ineffective controls pose to the organization.

Where We Started
Our standard report format contained all the requisite components of the IIA Standards. First, a Purpose and Scope paragraph informed the reader why the audit was performed (enterprise risk assessment or management request), followed by a bulleted list of the primary risks/processes included in the scope of the audit. The Background section followed; typically a few paragraphs with high level information about the department or process audited. Next, the Opinion paragraph stated the opinion rendered concerning the overall effectiveness of controls. Audit findings followed, which we term “Opportunities for Improvement.” Each finding included statements of Cause, Condition, Criteria, Effect, and our Recommendations for corrective actions. A Management Action Plan, Responsible Party and Completion Date followed each recommendation.

Although our format was good in many respects, we believed it could be better. Motivation came from management pushback concerning an audit opinion. In this case, we were evaluating controls over a portion of a program (essentially where the organization was with the program implementation at the time), not the overall effectiveness of the program. Although management generally agreed with our recommendations, they were intolerant of the audit opinion. Their reasoning was that the related process risks were reported from a micro view and did not pose significant organizational risks. One member of senior management stated, “This is a swing and a miss from a risk assessment standpoint.”

Our longstanding departmental policy was to issue a binary positive assurance opinion as a required component of each audit report. The format of the opinion was to state that the controls audited were ‘effective’, ‘effective, except for’ (a qualified opinion), or ‘not effective.’ Opinions were limited to the risks and processes audited as defined by the scope, and we included verbiage to alert the reader to that fact. Lax controls over a non-critical area would result in a ‘not effective’ opinion, regardless of the relative importance of the process or areas audited at the entity level. The link between the audit opinion and audit scope was sometimes misunderstood or disregarded, even by sophisticated readers.

We began to consider the value of rendering an Opinion. It was possible (probable, in fact, in light of our experience) that the opinion could lead to misplaced reliance on, or suspicion of, controls outside the scope of the audit. Worse yet, audit opinions could skew perception of the overall control environment! The organizational significance of audit findings could be misunderstood, either by 1) not clearly stating the relative importance, at an organizational level, of the process objective for which the control relates (perception of which may be skewed by the audit opinion and/or the experiences...
and knowledge of individual readers, or 2) vaguely worded statements of effect. Our project focused on adding clarity to reduce this tangible risk of misperception.

Management’s Perspective
I preface this section by stating the obvious: Internal Auditors will occasionally experience a conflict with management. Our redesign efforts were not intended to eliminate the potential for conflict. One executive stated this was “conflict by design,” and that really made sense given our role in governance and the nature of our work. Even so, auditors enhance the value of the audit function when they work in close collaboration with management. In the absence of exceptional circumstances, this can occur without compromising independence or objectivity.

Although our format was good in many respects, we believed it could be better.

Management shared their concern over the reputational risk incurred when requesting an audit and the potential that the Audit Committee viewed a distorted picture. Why request an audit of an area with poor controls knowing there will be an increased risk of a negative opinion, and that opinion is shared with the Audit Committee? Furthermore, due to the number of management requests (and associated negative opinions), the Audit Committee may misperceive the overall risk landscape.

Singular focus on audit opinions could result in misplaced reliance on, or suspicion of, the overall control environment and divert focus from audit recommendations. Management had made a number of recent audit requests, and we were concerned our collaboration was at risk.

Reconciling Industry Practices and IIA Standards
We became interested in the practices of other healthcare audit shops. Scott Stevenson at Emory University was kind enough to share the results of his survey of various healthcare systems regarding audit report formats. Results were clear that the industry is split in terms of preference for rendering Opinions versus Conclusions. Of the 13 responses to the Emory survey, six respondents rendered an audit opinion and seven did not.

One respondent included an interesting comment: “We do not include formal opinions and our Audit Committee thus far prefers it that way. Since very few of our audits are repetitive or routine, rendering opinions without management controversy can sometimes be difficult.” We verified that eliminating the Opinion posed no risk of non-compliance with IIA reporting standards which state: “Final communication of engagement results should, where appropriate, contain the internal auditor’s overall opinion and or conclusions.” (2410.A1) Our work was completed prior to the April, 2009 publication of the IIA Practice Guide titled “Formulating and Expressing Audit Opinions”. However, the Practice Guide affirmed many of our concerns. Although some Audit Committees require that departments issue opinions either at the micro or macro level; the Practice Guide warns that the organization must implement suitable criteria on which to base the opinion, including:

- Clear articulation of the definition of control
- Management understanding of a satisfactory level of control
- Clear articulation of management’s risk tolerances including materiality thresholds

The Practice Guide further states “In the absence of such principles, it is recommended that internal auditing should not render an opinion, since there is no frame or reference to objectively support the internal auditor’s conclusion.” The IIA clearly speaks to the risk of misplaced reliance on audit opinions; and discourages issuing an opinion in the absence of definitive criteria and clear organizational understanding and awareness. The next step was to decide the appropriate format and content of our Conclusion.

Format and Content of the Audit Conclusion
We were fortunate in that several peer departments were willing to share their report formats. One department’s Conclusion simply stated those areas where controls were found lacking. Therefore, if an item included in the Scope did not have a related Finding, the assumption was that controls were effective for that risk. We liked the general principle, but felt we needed to somehow communicate the relative impact at the entity level of the control risks identified in the report.

We turned to COSO for guidance. We decided to adopt the COSO descriptors and use them to reference inherent and residual risk impact and likelihood both at the entity and business process level (source: COSO Enterprise Risk Management—Integrated Framework):

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td>Insignificant</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Minor</td>
</tr>
<tr>
<td>Possible</td>
<td>Moderate</td>
</tr>
<tr>
<td>Likely</td>
<td>Major</td>
</tr>
<tr>
<td>Almost Certain</td>
<td>Catastrophic</td>
</tr>
</tbody>
</table>

What we believed was critical from the Audit Committee’s perspective was whether or not the control issues identified in the report are ‘likely’ to represent a ‘major’ risk at the entity level. We adopted that Conclusion; either inherent control risks are ‘Major’ at the entity level or not. Business process or departmental risks (micro view risks) are communicated within the Statement of Effect in each audit finding. The evaluation of risk impact is based on our assessment of inherent risk (risk in the absence of mitigating actions). Our reports now speak to both inherent and residual risks at the business process or departmental level.

While our Conclusion is based on inherent risk; we chose to include an affirming statement regarding our perception of management’s residual risk tolerance. We believe this provides additional assurance to the Audit Committee. IIA Standards
require auditors to address instances where management’s risk tolerance is deemed unacceptable to the organization. IIA Performance Standard 2600 states:

“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.”

While not required, we decided to make an affirming statement in every audit where management has submitted an action plan that acceptably limits residual risk.

The following is an example of the revised Conclusion assuming no major organizational risks were noted:

CONCLUSION

The results of our review indicate that there are opportunities for control improvements within the following area:

• Control Issue #1:
• Control Issue #2:

The audit did not identify any control weaknesses that individually or in aggregate are likely to present a major organizational (enterprise) risk. We believe management’s risk tolerance related to the issues noted is acceptable. Included are management’s action plans developed by John Doe, Applicable Service Line Director. These matters are offered for consideration in the spirit of continuously improving quality within Roper Saint Francis Healthcare.

See an example Statement of Effect within an Audit Finding below:

Inherent risk (risk in the absence of corrective action) related to this internal control issue may have a major impact on the process objective of ABC. This issue may increase the risk that the organization is out of compliance with governmental regulations. The completion of the management action plan detailed below will limit residual legal and financial risks to a level we consider minor.

Framework for Organizational Risk: The Impact Risk Matrix

How do we decide when a risk is major? Without a framework to guide decision making, there was a real risk that the Conclusion could be misperceived. To the extent possible, we wanted consensus from the Audit Committee as to the types of events that we collectively view as constituting a major organizational risk.

Again we turned to COSO for guidance. We developed a tool termed an “Impact Risk Matrix” that identifies a series of risk categories and risk events that we consider to present major organizational risks. While the matrix is not an exhaustive list, it does provide examples and a general framework for judgmental decision making.

For those risks that are quantitative in nature, we choose the same materiality threshold that our SOX Phase 1 team adopted for financial statement materiality. The threshold is ½ of one percent of total assets, revenues, or expenses (either point in time or annual impact depending on the account impacted). That was the easy part; qualitative risk factors were more difficult.

Given our Conclusion speaks to the cumulative risk impact (infinite variety of risk combinations that individually are not material but in aggregate are), auditor judgment prevails. No matrix will contemplate every combination of risk factors. Qualitative risks pose the most difficulty in terms of defining impact. However, we believe the matrix enhances our ability to make consistent Conclusions. The format of the Conclusion helps as well; there are only two options, the risks are ‘likely’ to present ‘Major’ organizational impact or not.

An excerpt from our Impact Risk Matrix is below (note that most events have implications to more than one risk category):

Other risk categories include Financial, Strategic, Legal, and Information
Systems. The matrix is a liquid document and must be periodically updated to remain relevant. We intend to share the matrix with Management and the Audit Committee at least annually for comment.

Summary and Conclusion

We were hopeful, after our investment of time and effort, that management and the Audit Committee would be receptive to these changes. We quickly obtained management’s approval and they appreciated our efforts to address their concerns. Although we knew the Audit Committee Chair was generally in agreement, we had not met with the full Committee; and were anxious to hear their input. We presented a summary PowerPoint™ presentation and waited on their response. After several questions, the Committee approved the new format and complimented the work. What a relief!

There are infinite variations of audit report formats. No format is widely accepted as best practice; if there were we would all already be using it. Reality is that every organization has specific preferences and tastes. For us, this format has bridged the gap between materiality and control effectiveness. From our perspective, we now communicate a clearer message to our Audit Committee, have addressed management’s concerns, and remain in compliance with IIA requisites. That makes this format ideal for our organization. NP

Jason McKinney, CIA, MBA, is a Senior Manager in the Internal Audit Services department of the Bon Secours Health System. Jason has managed the audit function for Roper Saint Francis Healthcare (RSFH), a joint venture between Bon Secours, the Medical Society of South Carolina, and Carolinas Healthcare System for the last nine years. He can be reached via email at jason.mckinney@rsfh.com.

About the only thing that comes to us without effort is old age.
~Gloria Pitzer
Report Writing

A Few Good Words—Writing Report Opinions

By Sally F. Cutler

Until now, your reports have been issued without a formal “opinion.” You’ve taken this approach because you believe it enables you to more effectively persuade management to take action. But now your audit committee wants you to include a formal opinion—and an overall rating—on every report. You’re wondering how you can meet the audit committee’s need without alienating your audit customers, with whom you have steadily been building a trusting and productive relationship.

This column will define whole-report opinions and will explore why and how internal auditors write them. Included will be the pros and cons of rating systems: their value for audit committees and executives as well as their potential to create conflicts with management. Finally, the column will address multi-report opinions—an increasingly frequent audit-committee request. The column will place these ideas in the context of recent guidance on opinion writing.

Whole-Report (Micro) “Opinions”

Whole-report opinions are high-level conclusions about the overall import of the observations within a single report. They may be called “micro” opinions to distinguish them from opinions that span multiple reports, which may be called “macro” opinions.

The guidance provided by The Institute of Internal Auditors says that whole-report opinions are “evaluations of the effects of observations and recommendations” and that they “put the observations and recommendations in perspective based on their overall implications.” This language points to a crucial aspect of a whole-report opinion, namely, that it is more than a summary. Consider this example:

You audited procurement, and one aspect you looked at was background checks on contract personnel, including those providing patient services. You have a spreadsheet with data for a sample of 25 such active contract personnel. The spreadsheet documents whether a background check was conducted for each contractor and whether all components of the background check were completed. The spreadsheet shows that background checks were not conducted for Contractors A and B; it also shows that drug testing—a required aspect of the background check—was pending for Contractors C, D, and E. All five of these contractors were providing services.

One possible summary of this detail is, “We sampled 25 active contract personnel providing patient services and found 5 for whom required background checks either were not conducted or were incomplete.” However, a conclusion about the findings goes further. For example, a conclusion might say, “Patients may have been put at risk because background checks on some contract personnel providing patient services either were not performed or were incomplete.” Moreover, if supported by interviews and observations, your conclusion might go on to say something like, “Deficiencies in performing background checks resulted from a lack of centrally assigned responsibility for this activity, with departments interpreting the requirements in differing ways.”

Conclusions, then, are broader statements—founded on facts—that rise to the level of describing the effects (risks) and causes of the conditions you found.

A whole-report conclusion—an opinion—describes the themes or commonalities across an entire report. Thus, an opinion focuses on higher-level and often systemic issues revealed by the audit. An opinion reaches to the level of providing
a consolidated view of the “overall implications” of the findings.

For example, say that your audit of procurement found not only differing interpretations related to background checks but also conflicting interpretations of other procurement requirements. Your overall conclusion could be that the organization risked patient safety and operating effectiveness by using inappropriate vendors in essential and non-essential areas because procurement management was not coordinating procurement activities (a control-environment issue) and was not communicating effectively with management in other areas of the organization.

Rating System Pros and Cons

Positive Impacts of Ratings

When used, a whole-report rating system is part of the auditor’s opinion. It consolidates the opinion into an easy-to-grasp phrase, numeric value, or color. Thus, audit committees and executive readers favor rating systems, and the reasons are easy to see:

• A rating system provides an instant view of the auditor’s opinion.
• The rating provides context for everything else in the report, both in terms of significance and urgency.
• Reports can be more easily compared, as can audit results for units across the organization.
• Ratings help management set priorities.

Common and Not-so-Common Rating Systems

Most such systems use three ratings. They may be given descriptors, most often unsatisfactory, needs improvement, and satisfactory. Alternatively, they may be numbered or assigned colors (the “traffic light” colors of red, yellow, and green). This three-point system is straightforward and communicates a simple range within the opinion.

Organizations aiming for more clarity in the middle category of a three-point system may split the needs improvement rating. The new descriptors may be needs significant improvement and needs improvement, or they may be mostly unsatisfactory and mostly satisfactory. A color-based system may add orange between yellow and red.

Some innovative organizations have enhanced their report ratings by displaying other dimensions along with the report rating. They do so to provide the audit committee and senior executives with a comprehensive view of the control environment. One such organization provides these three dimensions:

• Inherent risk (high, medium, low). This is the risk that placed the audit on the audit plan in the first place.
• Residual risk, which is the actual report rating (unsatisfactory, needs improvement, satisfactory). This rating is based on the issues found during the audit.
• Management awareness (high, medium, low). This rating is based on management’s self-identification of issues—and resulting actions—before the audit began as well as on whether issues in the report are repeat issues.

Whatever the rating system, you’ll be wise to periodically check that the ratings continue to function in communicating relative concern. Thus, unless an organization is exceptional, we would expect a distribution of ratings—albeit neither an even distribution nor a bell-shaped curve. A rating system needs revision if, for example, all or almost all reports receive a needs improvement rating; never or rarely is an unsatisfactory or satisfactory rating issued.

Formulation of the Rating

A whole-report rating is arrived at by tempering objective criteria with professional judgment. Objective criteria may include any or all of the following:

• The number of high-priority observations in the report
• The nature and extent of the risks (for example, pervasive health-and-safety issues weighing more heavily than sporadic accounting errors)
• The nature and extent of the causes (for example, findings resulting from intentional bypasses weighing more heavily than those resulting from staff making one-off errors)
• Whether issues found are repeat issues from previous audits

Once ratings criteria are established, however, auditors must add perspective and be willing to use judgment in making the final rating decision. Important factors include the auditor’s perception of management responsiveness and the compounding of risks across observations.

Negative Impacts of Ratings

Audit committees and executives favor ratings, but management often does not. The very clarity that makes ratings attractive to audit committees and executives makes ratings unattractive to our management audit customers. They may feel that ratings oversimplify complex issues, are unfairly judgmental, or suppress audit-customer efforts to rectify problems.

The tensions over ratings can impact the auditor’s relationship with the audit customer. We auditors claim to be helping management achieve better governance, risk management, and controls, but then we apply a rating—a grade—to management’s efforts. The rating may feel to management like punishment.

Furthermore, some auditors find that management is fixated on improving the report rating, taking the focus off the issues themselves. In some organizations, the negotiation of the rating obstructs report issuance; in others, where ratings have consequences for job security and careers, escalations and delays can be common.

Furthermore, many auditors must interact with audit customers on repeated engagements, and relationships can be poisoned by protracted ratings battles. Auditors focused on adding value
through management action may question how ratings move the organization in a productive direction.

**To Rate or Not To Rate**

In deciding whether or not to rate your reports, you should weigh a number of factors:

- **Your organization**
  - What is your organization’s culture? Other areas of your organization may commonly rate activities and outcomes; if so, internal audit will better align with the organization by adopting ratings.
  - How large is your organization? The more lines of business, operating units, and geographies within your organization, the more useful ratings are.
  - How much change is your organization undergoing? The more your organization is changing, the more useful ratings are.

- **Your audit function**
  - How many audits do you conduct? The more audits you conduct, the more useful ratings are.
  - How responsive is management in closing issues? Ratings are useful in helping management see the priority of closure.

- **Audit committees and executives favor ratings, but management often does not.**

- **Multi-Report (Macro) “Opinions”**

  The convergence of financial and operational pressures on organizations has increased interest in internal audit offering multi-report (macro) “Opinions.” Internal audit functions have long summarized results for their audit committees; recently, however, audit committees have sought an overall opinion from internal audit (as they do from external financial auditors). Internal audit is being asked to express an overall (macro) opinion on governance, risk management, internal controls, the control environment, compliance, and so forth.

- **Your decision to provide such an opinion should be based on considerations of intent, audit coverage, and clarity.** Recent guidance from The Institute of Internal Auditors provides an in-depth discussion of such considerations. In brief, these considerations include the following:
  - The purpose of the macro opinion
  - Whether the audit period and testing timelines support a macro opinion

  **Clarity through Opinions**

  After discussions with the audit committee and executive management, you reach a consensus on whole-report opinions, including a rating system. All stakeholders—audit committee, executive management, and management—are clear about how internal audit will develop the opinion and the rating and how these components will be used by management and the audit committee. You are committed to using this approach to deliver crisper messages to all of these stakeholders. And although your audit committee is not yet asking for a “macro” opinion, you are confident that, if and when they do, you will be able to develop a firm foundation for communicating at that level as well.

Sally F. Cutler is the president of Word-Wrights Incorporated, providing report-writing training and consulting for internal auditing departments worldwide since 1989. She is the author of “Designing and Writing Message-Based Audit Reports,” published by The Institute of Internal Auditors in 2001. Her book “Audit Committee Reporting: A Guide for Internal Audit” will be published in 2009. She may be reached at Sally.Cutler@Word-Wrights.com or at (315)-461-8070.

---

**I do not try to dance better than anyone else. I only try to dance better than myself.**

~Mikhail Baryshnikov
Construction Auditing

Auditing Field Reports and Logs

By Ron Risner

Have you ever looked at a construction project, and observed the on-site field trailers, the materials being delivered, equipment being used, along with workers coming and going, and wondered how all of those “moving parts” work in unison? Or, even better how all of those “moving parts” remain under control? You might be interested in knowing that there are a number of controls—reports and logs—which are maintained in the field to help manage the project. Let’s take a look at some of these reports and logs, to see how they help keep things under control and what you should look for as part of your construction audit. Keep in mind that most large contractors have construction software that help maintain these logs while other smaller contractors might still maintain manual or Excel spreadsheets. Either way it’s good to know from a control standpoint that these logs are in place.

Request for Information (RFI) Log
Commercial projects such as the one your healthcare facility may undergo consist of a set of drawings, plans and specifications. While the architect is responsible for developing these, it is up to the contractor and/or subcontractors to ‘interpret’ them. But what if these documents don’t make sense to the contractor or subcontractors? The answer is a process called a Request for Information or RFI. The contractor completes an RFI form and asks the architect for clarification (i.e. asks for information about some part of the drawings they don’t understand). For control purposes these RFI’s should be sequentially numbered and maintained on an RFI log. Once they have been logged the architect typically responds within several days. Subsequently as the architect’s answer is received the RFI log is updated to reflect that an answer was received. The contractor can now feel comfortable that they will construct the project as per the architect’s or engineer’s design.

Submittal Log
Probably the most commonly used log in the field is the submittal log. Submittals are anything that is “submitted” between the architect, general contractor, owner, subcontractors, engineers and/or other parties involved in the project. Submittals can consist of paint colors, carpet samples, drawings, letters or any other form of correspondence. Why a submittal log? It allows everyone to keep track of what is going on.

Equipment Log
As part of the cost of a construction project the owner typically pays for the equipment that will be used. On a fixed price (lump sum) contract the owner has less administrative concern about which equipment comes and goes since the cost is included in the price. However, on a cost plus or guaranteed maximum price contract the equipment usage will be billed to the owner on a daily, weekly or monthly basis. One way to control the cost is to monitor the movement of equipment to and from the field via an equipment log. This log lists all equipment brought to the site, the number of days it was on site and the day it was removed. When the contractor’s monthly invoice comes each month the equipment costs can be compared to the equipment log to ensure that the billing was correct. Of course, someone independent of the equipment owner should maintain the log for control purposes.

Materials Received Log
Some contractors like to maintain what is known as a materials received log. For instance they maintain a log of all delivery trucks that come and go each day. For example, this could be concrete trucks to trucks that provide lumber or steel beams. As the contractor receives the monthly billing from the material suppliers each month, they can then check receipts to the quantities billed to them.

Backcharge Log
Periodically contractors and subcontractors inadvertently damage each others work. For instance, a plumber might mistakenly damage the drywall that has already been completed by the drywall contractor. Who pays for this damage? Hopefully not the owner. The best way to control these costs is for the contractor to maintain a backcharge log. The log lists the damage that occurred, the date, a description of the damage, who caused the damage, who repaired the damage and who paid for the damage. In the example cited, the backcharge log would show that the plumber paid the drywall contractor to repair the work. For example, if the drywall contractor estimated $300 to repair the damage, the plumber was backcharged—via a change order—for $300 and the drywall contractor was credited an additional $300 for the work performed. The backcharge log helps maintain control over such instances.
Weather Report Logs

Contractors have an obligation to meet the scheduled deadline for completion of the project. If they don’t it is not unusual for them—per the construction agreement—to potentially suffer “liquidated damages”. That is, they have to pay the owner a set amount of money—say $5,000 a day—for not completing the project on time. In that respect, they build into the project schedule a number of “normal” bad weather days for the area. However, since an abnormal amount of poor weather conditions could delay the project the contractor keeps a log of daily weather. If, for instance, the number of rain days exceeds what is normal for the area they may claim—if they are behind schedule at the end of the project—that they were delayed because of excessive rain or flood. The weather log will show abnormal weather and is an acceptable way for the contractor to prove the delay an act of God and therefore potentially forego the liquidated damages. Note: For the owner to validate the weather report log they can refer to websites which track daily weather conditions. They can then compare the log to what is normal for the vicinity.

Daily Activity or Field Log

Many, but not all, general contractors like to maintain a log of daily accomplishments (i.e. the foundation was laid today). Use of this log is manifold. It shows them daily progress but it also shows what activity occurred on what day should there be a disagreement with the owner over cost and/or schedule. Reconstructing daily activity can become important when there is a dispute.

Non-conforming Log

As one might expect there are occasions when a subcontractor does not construct the project according to the plans, specifications or drawings. This is typically called “non-conforming” work and is usually identified or noted by the contractor or architect during routine walk-throughs. Under most construction agreements, the owner has the right to either accept the non-conforming work (i.e. it is not a safety or security issue or, the subcontractor can be forced to re-do their work at their cost). In order to control the non-conforming work some general contractors will maintain a non-conforming log for future reference. To support this log a contractor will typically take a picture of the non-conforming work before it is repaired.

Sign In/Out Sheets

Sometimes projects are so large that it becomes almost impossible to track which laborers showed up for work, went to lunch and never came back or left without anyone knowing. I once worked on a project with over 5,000 laborers on a given day. Since the owner wasn’t sure they would be billed properly for labor costs they requested that all laborers sign in and sign out each day. This way when the payment applications came in each month they could compare the billing to the sign-in and sign-out sheets.

Summary

While a construction site contains many moving parts, there are tried and true ways to maintain controls in the field. We have listed here a number of reports and/or logs which project and construction managers have developed over the years to help maintain control over field activities, including the cost of labor, equipment and materials. In addition to field reports and logs there are other accounting and/or financial logs and reports which are maintained in the field office or back office. We will discuss those in the next column. NP

Ron Risner is founder and president of Risner Consulting Group, Inc. of Orlando, Florida. He was formerly the Vice President of Internal Audit for a large commercial banking firm in Florida where he managed 50 auditors directly and 100 indirectly. Risner Consulting provides domestic and international professional construction consulting and audit services. The firm’s website is found at www.risnerconsulting.com.
Establishing The Foundations: Effectively Monitoring Internal Control Systems

By Sridhar Ramamoorti, Ph.D., ACA, CPA, CITP, CIA, CFE, CFSA, CRP, CGAP, CGFM, CICA, FCPA; Forrest Frazier, CPA & Jessica Dill, CIA

Background and Introduction
Unmonitored internal control systems deteriorate over time. Moreover, the mere existence of internal controls that are ‘stale’ and do not appropriately reflect the organization’s dynamic environment encompassing changes in strategy, risks, technology, people and processes, may give a false sense of security about being ‘in control.’ Former GE CEO Jack Welch remarked that, “when the internal rates of change within an organization fail to keep up with the external rates of change in the organization’s environment, the end is in sight.” In other words, it is critical that organizations track their changing risk profiles and design responsive internal controls that can help mitigate risks to an acceptable level. Such mapping of risks to mitigating controls and the design/re-design of mitigating controls needs to occur continuously so that organizations pre-empt risks from maturing and perhaps becoming material or even catastrophic.

The world of healthcare is in a constant state of flux, so monitoring internal control systems, including the risk assessment and management processes and the design and implementation of responsive controls in a healthcare organization’s context has special relevance for healthcare internal auditors and AHIA members.

Monitoring, as defined in COSO’s 1992 Internal Control-Integrated Framework, is implemented to help ensure that internal control continues to operate effectively. When monitoring is properly designed and executed, a host of benefits typically accrue to a healthcare organization:

- Timely identification and correction of internal control problems.
- More accurate, timely, decision-relevant information is provided through reliable financial reporting (as well as enhanced operational effectiveness and improved compliance activities).
- The ability to furnish periodic certifications or assertions on the effectiveness of internal control, where required.

The original COSO Internal Control-Integrated Framework (1992) had five elements of internal control: control environment, risk assessment, control activities, information and communication, and at the apex, monitoring. Nevertheless, over the years, it became evident that either companies implemented monitoring for which they did not or could not take credit (inefficiency), or they did not implement effective monitoring and simply presumed that well-designed controls continued to operate effectively over time. In either case, the COSO Board determined that it would be useful to provide specific guidance on monitoring so that the internal control framework could be optimally utilized and relied upon. In the U.S., the challenges posed for public companies subject to internal control reporting requirements under the Sarbanes-Oxley Act of 2002 provide an additional impetus to understand and implement effective monitoring activities.

Monitoring, as a re-validation function, provides a critical feedback loop; as such it is an indispensable activity for all organizations. Just as, “an ounce of prevention is worth a pound of cure,” timely and effective monitoring can help ensure that internal controls remain robust and in line with an organization’s constantly changing risk environment, so as to prevent potentially costly and damaging controls failures down the road.

Developing and maintaining a best-class system of monitoring controls is a testament to an organization’s commitment to excellence.

COSO’s Monitoring Guidance (2009) builds on two fundamental principles...
established in COSO’s 2006 Guidance (which reduced all of the COSO 1992 guidance into a set of 20 foundational principles):

1. Ongoing and/or separate evaluations enable management to determine whether the other components of internal control continue to function over time.

2. Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action and to management and the board as appropriate.

Effective monitoring relies on the development of persuasive information—information that is both of suitable quality and in sufficient quantity—about the continued operation of controls or control elements, as evaluated by competent and objective evaluators. Properly designed and executed monitoring not only furnishes persuasive information to evaluators regarding the internal control system’s effectiveness, but also identifies and communicates internal control deficiencies in a timely manner, enabling corrective action. Persuasive information needed for evaluating internal control systems is important to addressing two critical questions: what to monitor, and how to monitor.

Monitoring, to be effective, must be based on three broad elements (see Figure 1):

1. Establishing a foundation for monitoring, including a proper tone from the top, an effective organizational structure, and a starting point or “baseline” of known, well-designed and implemented controls.

2. Designing and executing monitoring procedures focused on persuasive information about the operation of key controls that address meaningful risks to organizational objectives.

3. Assessing and reporting results, including evaluating the severity of any identified deficiencies and reporting the monitoring results to appropriate parties to enable timely corrective action.

Increasingly, in healthcare organizations that are heavily reliant on Information Technology (IT), the persuasive information required for monitoring is highly dependent on automated systems and processes (involving information production or collection, analysis, and/or dissemination). Monitoring activities frequently need to be focused on control processes that have been automated. Moreover, many monitoring tools and techniques, to be truly effective, need to be IT-enabled. Hence information technology can be seen as both a driver as well as an enabler of effective monitoring (Weidenmier & Ramamoorti, 2006). The Board and management’s IT strategy must factor in not only the need for continuous monitoring but also the key role that IT plays in such strategy formulation. IT governance considerations typically would cover matters such as control environment, including tone at the top, data security, privacy and confidentiality, as well as access privilege issues, and the determination of the snapshot of baseline internal controls at a point in time to evaluate changes in people, policies, processes, and technology that may need to be considered as part of monitoring activities. In this regard, evaluator characteristics, such as their competence and objectivity, including the understanding of the “systems environment” are also important considerations.

**Applicability to Healthcare Industry**

Now, more than ever, it is imperative for healthcare organizations to clearly and consistently follow a set of governance practices. Historically, these governance practices may have been less formal and sometimes applied inconsistently. Important healthcare stakeholders, including the IRS, Senate Finance Committee, Catholic Health Association and states’ Attorneys General, are placing increased emphasis on transparency and accountability in the tax-exempt sector. Additionally, bond rating agencies are analyzing the governance practices of healthcare organizations as part of their analysis of an organization’s credit worthiness. Monitoring internal control systems is one aspect of the overall system of good corporate governance practices that organizations are beginning to utilize to support strategic, financial, regulatory and operating objectives. As discussed above, the first aspect of the monitoring process is establishing a foundation for...
monitoring, including tone from the top; organizational structure; and a baseline of effective internal control.

Foundation for Monitoring, Including Tone from the Top
In your organization, how do the executives charged with monitoring finance and compliance get comfortable that the internal control environment is keeping pace with changes that affect your business and operations? We regularly meet with Chief Financial Officers and Compliance and Internal Audit Directors who are asking themselves this question. Typically, their organizations have performed, at some point in the past, various forms of exhaustive internal controls documentation and assessments. After becoming comfortable that the internal control environment is designed and operating effectively, these executives are often distracted as other initiatives take priority, leading the focus on internal controls to wane and the documentation to become dated and stale over time. Internal Audit can serve as a backstop to help prevent this, but the first line of defense should lie with the process and control owners themselves. These executives would be well served by designing, implementing and documenting a comprehensive monitoring controls program to ensure controls change as the underlying business changes, controls failures are brought to the attention of the appropriate individuals, and appropriate focus on internal controls is maintained at the process owner level.

The Board also plays a critical role in establishing tone from the top required for effective monitoring. Most Boards maintain mature compliance and audit oversight activities. To have a best-class monitoring program, it must be ardently championed by the Board and be seen by them as a critical part of an internal control system supporting their oversight activities.

Leading organizations known for providing high-quality healthcare want to continuously improve all aspects of their business practices. Developing and maintaining a best-class system of monitoring controls is a testament to an organization’s commitment to excellence. In this way, these organizations are not only ensuring their continued ability to provide exceptional patient care, but they are also setting an industry benchmark for internal controls and governance standards best-practices.

Organizational Structure
Monitoring involves establishing appropriate roles and responsibilities of management and process owners regarding the design and operation of internal controls and placing evaluators with the appropriate competencies and objectivity in the right positions within the organization. Healthcare organizations inherently have unique challenges with organizational structure. For instance, certain controls that impact the financial statements (e.g., charge capture) are performed by non-financial personnel throughout the organization who may not understand the significance of what they do on the entity’s ability to perform timely and accurate financial reporting. Additionally, healthcare systems often have decentralized operations, with process owners distributed among various geographies and throughout disparate facilities. Many healthcare organizations deal with higher than desired turnover among process owners. Finally, as it should be, process owners in healthcare organizations consider providing the highest priority healthcare to be their top priority and often the execution of internal controls over financial reporting may take a back seat.

Baseline of Effective Internal Control
As former SEC Chairman, William Donaldson remarked, “Internal controls constitute the very DNA of an enterprise.” Hence, at the outset, organizations must recognize that internal controls represent the foundations of a successful enterprise.

For a monitoring program to be effective, it must start with a baseline of effective internal control. As noted above, due to the rapidly changing environment in which healthcare organizations operate, a comprehensive, one-time effort may be needed to refresh controls design and related documentation to establish this baseline. The most effective monitoring program will fail if the underlying controls it evaluates are not designed to address the appropriate risks or are not executed by people appropriately trained and supervised. Once this baseline is established, an effective monitoring program can maintain the effective design and operation of internal controls going forward to ensure timely and accurate identification of controls failures.

Complexities Created by Automated Controls
The extensive use of automated controls and information systems in healthcare creates both a tremendous need and opportunity as it relates to monitoring. As it relates to need, we need look no further than the revenue cycle, including charge capture, claims scrubbing, patient billing and the like to see that automated controls in healthcare are complex and have pervasive impacts on the financial results of the organization and, therefore, should be subject to robust monitoring. Likewise, many of these same systems themselves are in fact evaluators of other automated or manual controls and provide the information needed to conduct such evaluations. So in this sense, because of the tremendous volume and complexity of transactions and the ever-changing reimbursement and other regulations,
Automated and information technology-based controls are a critical element of an entity’s overall monitoring system.

“Internal controls constitute the very DNA of an enterprise.”

Often, automated controls result in the creation of exception reports which, to be useful, must be reviewed and exceptions appropriately investigated and resolved. These reviews are a critical component to any well-designed monitoring program.

Conclusion

Effective monitoring starts with establishing a foundation for monitoring, which, as discussed above, is done with proper tone from the top, an effective organizational structure, and a baseline of well-designed and implemented controls. Monitoring internal control systems is vital to protecting healthcare organizations from unnecessary risks. Effective monitoring allows organizations to gain reasonable assurance that their internal control systems continue to operate effectively over time and that internal control deficiencies are identified and communicated in a timely manner to the appropriate parties, management, or the Board of Directors as appropriate. Monitoring evaluates the internal control system’s ability, in its entirety, to manage or mitigate meaningful risks to an organization’s objectives. Additionally, monitoring can improve the organization’s overall effectiveness and efficiency by providing timely evidence of changes that have occurred, or might need to occur, to the design or operation of internal control. With their often decentralized and highly complicated operations and growing use of information technology, healthcare organizations stand to benefit greatly from a robust monitoring controls program.

In the December issue of New Perspectives, we will discuss designing and executing monitoring control systems and key aspects of that to healthcare entities.

Acknowledgement: We thank Trent Gazzaway, Project Leader on the COSO Monitoring project for his input to this article.

Authors

Sridhar Ramamoorti, Ph.D., ACA, CPA.CITP, CIA, CFE, CFSA, CRP, CGAP, CGFM, CICA, FCPA, is a partner in the National Corporate Governance Group of Grant Thornton LLP in Chicago. He leads the firm’s thought leadership initiatives in corporate governance and accountability, advising on Sarbanes Oxley, professional standards, and other technical matters, contributing to the firm’s professional development programs, promoting university faculty relations, and mentoring younger professionals. A former accountancy faculty member at the University of Illinois, Sri was a member of the Grant Thornton COSO Monitoring Guidance authoring team, and has served on the New Perspectives Editorial Committee since 2004. He may be reached at: sri.ramamoorti@gmail.com, or at (630) 347-9172.

Forrest Frazier, CPA, is a partner in the business advisory services practice of Grant Thornton’s Charlotte office. He coordinates BAS offerings in the southeast region to clients in the healthcare industry. He may be reached at: forrest.frazier@gt.com, or at (704) 632-6801.

Jessica Dill, CIA, is a manager in the business advisory services practice of Grant Thornton’s Charlotte office. She is on the leadership team for Advisory Services offerings in the Carolinas to clients in the healthcare industry. She may be reached at: jessica.dill@gt.com, or at (704) 632-6866.

Introduction
Early 2009, in the scope of one month, there were dozens of cases of healthcare fraud and ethics violations reported. For example, two Texas women pled guilty to theft in connection with fake invoices to a healthcare company. A computer system administrator in New Jersey was charged with computer fraud. Had his scheme been successful, it would have caused widespread financial damages and potential health risks to the company’s clients. And, in California a physician was arrested for dispensing powerful and addictive painkillers directly out of his office without examining ‘patients’. The patients simply paid him cash for pills.

Odd thing is these are not the headlines. They represent only the tip of the iceberg. Frankly, I cannot imagine a more convoluted environment to work in today than healthcare. The issues are complex. Rules and regulations define how, what and when healthcare is provided. More and more the patient feels frustration at a system that is too complex.

In this article I focus on financial ethics and issues of fraud. There are many ethics issues that face healthcare today, but none that have a more direct impact on the healthcare providers than weaving their way through the process of dealing with money. Perhaps the best teacher is looking at what happened and learning from those experiences.

Executive Summary
People make choices every day about many things. Some of those decisions include an ethical aspect, and it is not always black or white as to whether the choice is right or wrong. The more variables there are to consider the greater the odds of a less than desirable ‘correct’ outcome. Healthcare presents one of those difficult environments. Unethical choices share a common thread whether it is a high profile case or your ordinary everyday low level employee. Gray area decisions can put you on a slippery slope that may be difficult if not impossible to get off. When the wrong choice is made did the decision maker deliberately set out to do wrong? We all have our regrets about past decisions and actions. Is your organization doing enough to thwart employees by breaking the thread common to all fraudulent decisions? Every choice has its consequence.

Administrative Choices and Consequences
Jacqueline Nugent, who was known at work as Jacqueline Wilkinson, was sentenced for mail fraud in connection with a fraudulent paycheck scheme at a Washington, DC area hospital. According to the US Attorney’s office, Nugent had a job that allowed her to hire contract employees for the Washington Hospital Center. She was also responsible for submitting the paperwork necessary to ensure that the contract employees were paid for their work. Problem was—Nugent submitted for pay fraudulent paperwork for fictitious employees. Her theft—more than $21,000. (See US Attorney’s News Release: http://www.usdoj.gov/usao/dc/Press_Releases/2009%20Archives/January/09-015.html).

Question—what controls or procedures do you have in place to verify that the payments made to independent contractors represent actual work performed?

Coding/Billing Choices and Consequences
Sentenced to three years in prison, licensed chiropractor Stephen Catterton was found guilty of defrauding insurers of $1.2 million. Between June 2001 and December 2006. Catterton billed in excess of $3 million, and was paid in excess of $1.275 million from various healthcare benefit programs for services he never performed or
provided. The US Attorney’s office reports that in some instances, billing codes for more advanced procedures were used when, in fact, patients only received massages. Catterton modified the billings for the services that were actually performed to maximize his reimbursement from the insurance companies. (See US Attorney News Release—January 13, 2009 - http://www.usdoj.gov/usao/gan/press/index.html).

Here’s an example. As this article is written, I am scheduled for an annual physical in a few months. Meanwhile, I developed a minor problem with my leg—nothing major—but annoying enough that it should be looked at. Go figure, but simple me (the patient) assumes that it would be best to kill two birds with one stone—get the annual physical done and get the leg checked out at the same time. So, I call the doctor’s office only to be told that my insurance will not allow billing for a physical and an acute problem on the same visit. I would have to make it two separate visits.

Is that an ethics issue? No. In and of itself it is not. But, what would have happened if, not knowing the rules as a patient, I had gone in for the annual physical and presented the physician with an acute problem during the visit? Would the physician’s office have billed my visit as a physical only? Would the physician have refused to treat my acute problem? Would the office have coded both issues and taken their chances with the insurance provider? Or, is it possible that the office, knowing that they have to play the insurance game, would have billed both services as if they had occurred on separate days?

With government agencies overseeing the administration of Medicare and Medicaid along with insurance companies putting the financial squeeze on healthcare providers of all sorts, it is easy to see how abuse and fraud could take place. The stakes are high and with eroding margins, this creates and fosters an environment for fraud and abuse. Even good people can find themselves on the wrong end of an overzealous investigator.

Physician Choices and Consequences

In early February this year, Neurometrix, Inc., agreed to a deferred prosecution of illegal payment of kickbacks to physicians. Neurometrix, Inc. also agreed to pay $2,498,337 in civil damages and penalties for their kickback conduct, and for the additional conduct of causing physicians to improperly bill nerve conduction studies to Medicare under a higher code than was actually performed by the physicians. (See US Dept of Justice News Release - http://www.usdoj.gov/usan/ma/Press%20Office%20-%20Press%20Release%20Files/Feb2009/NeurometrixPR.html).

Question—were the physicians involved aware of the billing issue? Perhaps not.

However, there is an ethical component to this case. From August 2004 through October 2006, Neurometrix, Inc. marketed their device through two referral programs where the company paid physicians in the form of free boxes of disposable biosensors to induce them to recommend purchase of the NC-stat System to their colleagues for the purpose of conducting nerve conduction studies that were reimbursed by federal healthcare programs.

Now the ethical question is—is it right to accept ‘gifts’ as an inducement for recommendations to others? In this case physicians were not indicted. However, by the actions of the federal prosecutors, it certainly would appear that Neurometrix, Inc. is deemed to have crossed the line when it comes to ethical marketing practices.

In another case, Destin, FL physician, David W. Webb and his wife and office manager, Bonnie F. Webb were charged with healthcare fraud, the unlawful dispensing of controlled substances, identity theft, conspiracy to commit healthcare and wire fraud, and conspiracy to distribute and dispense controlled substances.

The 131 count indictment involving the distribution and dispensing of oxycodone...
and fentanyl with death resulting from the use of those controlled substances means the defendants face a mandatory minimum term of 20 years’ imprisonment, a maximum of life imprisonment, and a fine of $1,000,000, on each count. (See US Attorney’s News Release - http://www.usdoj.gov/usaofl/press%20releases/2009/jan/webb.html).

Common Threads

Choices and consequences! It is easy to see black and white in many of these examples provided above, but ethics is not black and white nor is it an exact science. Ethics, according to Merriam-Webster is “the discipline dealing with what is good and bad and with moral duty and obligation.” Good and bad is a function of circumstance, not always defined by a clear specific action. Therefore, the more convoluted the environment, the more difficult it is to find the correct ethical choice.

Clearly, many of the examples I am using here are extremes, but there is a common thread that binds most all unethical choices that lead to fraud. It is what I refer to as the ‘three legged stool’ of fraudulent behavior. Whether it is Bernie Madoff or the clerk who is caught, three things are always present.

Need—Opportunity—Rationalization

Unethical behavior that morphs into fraud will always have these three components at their core. People often ask me at seminars I conduct—“How can I prevent fraud?” In many ways that answer is simple—remove one of the three components and the fraud fails or, better still, never materializes. At the risk of being overly simplistic, fraud prevention is really that simple. So let’s examine three simple approaches to reduce unethical behavior.

First, most organizations do not do enough of the right things to discourage rationalization. Oh, sure there are the mandatory boring ethics meetings. Let me repeat …boring ethics meetings. When those meetings are presented in a meaningful way that reinforces the company’s desire for ethical behavior, then the employees will become more conscious of choices and consequences. In its simplest form, if you tell an employee about rationalization and bring the point home, in most cases, it will fire those thought neurons that say, “Maybe I shouldn’t be thinking this way.” When that happens, behavior changes.

Another simple prevention technique is to eliminate opportunity. Now, as a former CPA, I know all too well that you cannot completely eliminate opportunity. But, effective (not burdensome) internal controls can make the possibility of fraud much more difficult. Difficult fraud rarely happens. Some of the examples above show, once we go beneath the surface, that there was a lack of control. If, for example, I get to hire the independent contractors and submit their paperwork for payment, I am given opportunity on a silver platter. Good people will make bad decisions, sometimes disastrous decisions, if there are no controls to the contrary.

Lastly, if there is no need, then there will be no fraud. However, need is the most difficult to identify. Perhaps the need in some of the examples above is purely money. Perhaps the need, like in the case with Bernie Madoff, is more than the obvious. Need can take many forms. Madoff’s, it is speculated, was emotional. Bernie could not admit that he was fallible. His need to be the smartest man in the room was too great and opened the door to effecting what is now the largest Ponzi scheme in history.

One thing that is certainly true in this current economic time is that if your employees are struggling financially—there is need—the first element necessary for fraud. Better in many ways to reduce your work force permanently, than it is to try to keep them on board with less hours or pay and drive up the need factor.

Last Thoughts

In each of my presentations I ask the audience to stand and ask one question. “If the person to your right, left, in front of you or behind you, could see every choice you had made in your life, how many of you would be ashamed or regret one or more of those choices?” I ask them to be seated if they would be ashamed or regret a choice they made. Thus far 100% of the people sit.

We all make mistakes. Sometimes those mistakes can be corrected. Other times those mistakes lead to different choices and as we push those grey areas of ethical behavior the lines can become blurred.

Every choice has a consequence. As a former CPA who became a white-collar fraudster, I know how easy it is to fall into the slippery slope of poor choice. The consequences, well, they are not fun. Now is the time to review what you do, how you do it, and ask yourself and organization if there is anything that can be done to remove the legs from the three legged stool of fraudulent or unethical behavior? The choice is yours!

An international speaker, author, and radio host, Chuck Gallagher is a business ethics and fraud prevention expert. Having risen from convicted felon to Sr. Vice President in a public company, Chuck speaks to companies, associations, and universities. For information about his programs or consulting, visit his web site: www.chuckgallagher.com or e-mail him at chuck@chuckgallagher.com.

Happiness is not a goal, it is a by-product.
~Eleanor Roosevelt
Here Come National Drug Codes, ICD-10, Modifier 25, and RAC Extrapolation

By Duane C. Abbey, Ph.D., CFP

Moving to National Drug Codes and ICD-10

We are finally going to move to NDCs and we have a firm date for implementing ICD-10. Movement to these two code sets is long overdue.

The official date for ICD-10 is October 1, 2013. While the overall impact is yet to be determined, this will herald another set of changes to the MS-DRG payment system. Also, all healthcare providers will need to undertake extensive training programs not only for coding, but also to understand terminology and definitional changes.

The NDCs are embedded in the implementation of the new Pharmacy Claims transaction standard. While the implementation of NDCs will be a significant challenge for information technology personnel, for auditors this is a very welcome change. Perhaps we can even move to billing pharmacy items with the correct number of units and bid farewell to the J-codes.

The ‘-25’ Modifier Moves into the Limelight

The ‘-25’ modifier is attached to E/M (Evaluation and Management) codes to indicate that the E/M service should be paid in addition to payment for a diagnostic or therapeutic service. This modifier is used by both physicians on the professional side under the Medicare Physician Fee Schedule (MPFS) and on the technical side under APCs (Ambulatory Payment Classifications). The CPT description of the ‘-25’ modifier is essentially the same for physicians and hospitals. However, for hospitals we must translate the language somewhat.

The basic language is that a ‘significant, separately identifiable’ E/M service has been provided that goes above and beyond that which would be normally provided with the diagnostic or therapeutic service. Back in 1999 the AMA inserted language indicating that there did not have to be a different condition or different diagnosis in order to use the ‘-25’ modifier. In other words, if the documentation supports E/M services that go beyond the normal services provided with the associated procedure, then there did not have to be a separate reason.

The ‘-25’ modifier has long been a compliance issue for physicians. The OIG has audited the use of the ‘-25’ modifier on the physician side.1 Now the use of this modifier is being challenged on the hospital, technical component side. Unfortunately, CMS has provided very little guidance on the use or non-use of this modifier.

When APCs were officially implemented on August 1, 2000, CMS indicated that E/M codes could be paid separately by using the ‘-25’ modifier. This decision was a distinct departure from the precursor system, APGs (Ambulatory Patient Groups), in which E/M levels were bundled if there was some other service. Additionally, CMS provided no guidance on using the different E/M levels. Instead, CMS in the April 7, 2000 Federal Register2 simply indicated each hospital should develop their own mapping of resources utilized into the different levels.

If this guidance is accurate, the whole landscape of using the ‘-25’ modifier has just dramatically changed.

With the decision to pay separately for E/M levels by using the ‘-25’ modifier, hospitals immediately raised questions about properly using this modifier. If there was some sort of diagnostic or therapeutic procedure performed, there would be some level of resource utilization involving evaluation and management in connection with the associated service. Thus, hospitals needed to know precisely how to separate the general E/M services from the E/M services that were a part of the associated procedure.

CMS did issue minimal guidance on this issue in two program memorandums:

1 See the report at: www.oig.hhs.gov/oei/reports/oei-07-03-00470.pdf.
2 65 FR 18451
Both of these program memorandums indicated that the use of the ‘-25’ modifier depended upon documentation separating the extra E/M resource utilization.

While the healthcare community anticipated that CMS would issue national guidelines on technical component E/M levels, there have been no national guidelines developed. As a result the proper use of the ‘-25’ modifier, which is inextricably related to the E/M levels, has never been further addressed for the past eight years.

Now the ‘-25’ modifier is being moved into the limelight and is being investigated by the OIG. Also, we are now seeing some guidance that is very different from the guidance provided by the two program memorandums referenced above. For instance, from the Medicare Alert Bulletin 2255, February 17, 2009, pages 9–10, issued by Georgia Medicare, there is language to the effect:

“Only in those instances where a medical visit (E&M) on the same date as a diagnostic or therapeutic procedure (‘S’ or ‘T’ APC status indicator code) is separately identifiable service for an unrelated problem should the facility receive separate reimbursement for the evaluation and management service.”

(Emphasis as found in document.)

If this guidance, which was proffered as a reminder, is accurate, then the whole landscape of using the ‘-25’ modifier has just dramatically changed. If this suddenly becomes a clarification in guidance, that is, not a change, then the whole ‘-25’ modifier will become a major RAC audit issue.

Hospital and clinic auditing staff should follow the development of this issue over the coming months and years. Be certain to take a look at your institution’s E/M mapping and documentation support for using the ‘-25’ modifier. Arguably this is a major change in policy, but CMS will probably maintain that it is just a clarification and thus Section 903 of MMA 2003 does not prevent them from applying this clarification retroactively.

The RACs can Extrapolate

Auditors should take careful note that the RACs (Recovery Audit Contractors) are allowed to use the extrapolation process. Also, as the RACs go nationwide, all coding, billing and reimbursement issues for all types of providers will be on the table. RACs address the fee-for-service payment system which is about the only delimitation on their activities. There are three claim RACs and two MSP RACs.

The extrapolation process is a technical statistical process that the auditors can use to determine overpayments, and, theoretically, underpayments, by auditing a statistically valid sample and then extending or extrapolating the results to the entire universe under consideration. This is a formal process that generally requires:

- Identification of a specific issue
- Consultation with a statistical expert to determine the statistical process
- Generally, a probe audit to determine error rate to calculate the sample size
- Selection of the sample
- Audit of the sample
- Analysis of the results to determine the amount of overpayment

Needless to say, this is a very general synopsis of a complex process that uses special statistical software such as the OIG’s RAT-STATS program. The extrapolation process as discussed by the OIG and CMS was not used during the RAC demonstration. However, with the significantly increased RAC activities, at some point the RACs will want to use this process. If for no other reason, with a delimitation on the number of records that can be requested from providers, an issue that is systematic in nature and that affects thousands of cases will lend itself to the extrapolation process.

Auditors, please note that an individual healthcare provider can also use this process and possibly preempt a RAC from this process. If, as an auditor, you identify a problem that is systematic and pervasive, then the organization may want to have a study conducted by an Independent Review Organization (IRO) and make appropriate repayment before a RAC does so. If you perform such a study, these cases can be excluded from consideration by the RAC, at least for the given issue.

There are many questions surrounding this process including the question of what to do if both overpayments and underpayments are encountered. In other words, is it proper to offset overpayments with underpayments? NP

Duane C. Abbey, PhD, CFP is president of Abbey & Abbey Consultants, Inc., specializing in healthcare consulting and related areas. He also teaches workshops and makes presentations to hospital associations and medical societies. He is a leading expert nationally on APGs/APCs. Duane may be contacted at Duane@acciweb.com.
Welcome to this issue of Letters to the Auditor.

As this column is written, we’ve had an early spring here in the Midwest; this usually means that the early robins only use one English sparrow as a parka versus two.

Speaking of our feathered friends, in this issue we hear from one of our readers who wants his team to move together in times of audit stress...

Birds, check out this letter to the auditor...

Dear LTA,

One of the biggest challenges my audit team and I encounter is our client/auditees who are like professional boxers—adept at weaving and bobbing and shifting away from their commitments.

Meanwhile, in the closing meeting, we are giving each other side glances, kicks under the table and clearing our throats.

How do you communicate with your team when under stress and you are finding yourself in confusing circumstances? Someone told me that we need to “Twitter…”

This sounds like it’s for the birds.

Signed,

For the Birds

Dear For the Birds,

It’s the latest trend in social networking, but I am not into “Twittering”, so I’ll leave the decision to “Twitter” or not to “Twitter” up to you, but I can tell you that my son Mike had over 15,000 text messages on our last cell phone bill.

As for your clients that can maneuver like a champion fighter, I recommend that you have a Coherent Motion training session with your audit team.

What is Coherent Motion? We all have seen it hundreds of times in nature. You are at a city plaza and a hundred pigeons get scared and they fly up and down or all bank to the left or right in a collective movement.

This phenomena of Coherent Motion is not solely a bird thing, schools of fish do it, too, as well as bacteria, sheep, wildebeest, etc. Coherent Motion is not a “V” shaped geese flight formation, it is group response thing.

How do they do it? The theory is that each bird makes its own adjustments based on their immediate neighbor. In 2001, scientists (Potts) measured the length of time it took birds to react to a flash of light. The birds startle reaction was 38 milliseconds but it took less than 15 milliseconds for the immediate neighbor to react. Potts later called this the “chorus line hypothesis” comparing it to the Rockettes at Radio City Music Hall who can see and anticipate an approaching high leg kick when it is well down the line. Films of human chorus lines show that rehearsed maneuvers, initiated without warning, propagate down the line at less than 108 milliseconds, almost twice as fast as the human visual reaction time of 194 milliseconds.

So the next time, you have a meeting that turns into a bobbing and weaving session; have your Coherent Motion session set and ready to go.

1. Keep the Main Thing as the Main Thing. Don’t allow the topic of discussion to be distracted.
2. Organize your major audit recommendations into themes, messages, and mantras and return to them often when you find yourself getting distracted by the client.
3. Maybe you can initiate a non-verbal cue to your team like crossing your arms at the same time. (No leg kicking allowed in closing meetings!)

And in the meantime, if you figure out this Twitter thing, let me know....

Well, that’s it for this issue of Letters to the Auditor. Please keep those letters, calls, cards and emails coming. You can send your questions and comments to Letters to the Auditor, c/o John Landreth, 1810 W. Birch Lane, Park Ridge, Illinois 60068, via email at jlandreth999@aol.com, or phone 847-525-6529.

John Landreth leads a Healthcare Internal Audit, Compliance, and Consulting practice (Atoll~Compliance and Control) and was former Corporate Integrity Executive / Director, Internal Audit for Northwestern Memorial Hospital in Chicago, Illinois. This is his 20th year as founder and columnist of Letters to the Auditor. He was the AHIA’s Founder’s Award recipient in 2000 and recipient of the 2009 APEX Award of Excellence for his Letters to the Auditor column.

By John Landreth, CPA, CFE, CHC

Birds of a Feather…and How Their Behavior can Help an Auditor
Interview with AHIA Chair Mark Eddy

New Perspectives recently had the opportunity to interview Mark Eddy, CPA, Vice President, HCA Internal Audit and the 2009 Chair of the AHIA Board of Directors about the progress the Association is making, opportunities for personal growth through leadership, as well as obtaining some personal insights on the person our members elected to head the Association this year.

NP: Mark, you are more than half way through your term as AHIA Chair. How is AHIA progressing against the goals you set for this year?

Eddy: I am very pleased with our progress to-date. We have new, energetic Board members and our returning members have stayed focused on strategic goal achievement. This Board understands the importance of meeting our teammates’ needs. We are always brainstorming as to how we can provide new or better services for the membership. The Education and Technology Committees have pursued webinars as a new, cost-effective benefit for members. The Annual Conference Committee continues to do a bang-up job designing our national conference. The Education Committee is expanding opportunities through Chief Audit Executive Roundtables and regional seminars. The Technology Committee continues to market the web library, updating and expanding content through contests. Through the Editorial Committee, we publish this professionally recognized New Perspectives quarterly journal. Plus, the Finance Committee is watching closely during these challenging economic times to keep our Association fiscally strong.

The area I’d like to see us improve upon is to get more of our teammates involved in the AHIA. I’d like to gain access to their ideas to improve the organization today and train them for the leadership positions of tomorrow.

NP: Within the past year the AHIA Board held a planning meeting to consider its strategic plans. What parts of those plans are underway at this time and when will members see the results?

Eddy: At the January Board of Directors meeting, we revisited and challenged our strategic plan. The plan, when written, was intended to direct efforts for approximately 5 years and we believe it remains relevant for that purpose. We did not propose any changes to the plan but discussed each component to ensure we stay focused.

NP: Finish this sentence: If I could start my life over again I would....

Eddy: I haven’t finished what I set out to accomplish but I wouldn’t make any significant changes in the road I’ve traveled thus far. I am lucky to have experienced what I have but “I have miles to go before I sleep.”

NP: Mark, what would you do if you won the lottery?

Eddy: It depends how large of a payout. Winning anything less than the “Powerball” would likely be invested for retirement. If I won the “Powerball,” I would retire. I never thought I would retire, but I have a few more years under my belt now and the “Powerball” pay-off would provide enough to live comfortably. Wendy and I want to travel throughout Europe when we retire and doing it while we are young would be nice.

NP: Everyone is working under constrained budgets these days. As the Chair, can you speak to how AHIA provides value for the dollars expended?

Eddy: Our annual membership fee is a great value when compared to other organizations/associations. $200 (or less) per year gets you access to the website audit library, a very active list serve accessible to over 1,200 members, the professionally recognized New Perspectives quarterly journal, and discounted fees for educational offerings. The cost per hour for CPE offered by AHIA is as cost-effective as you’ll find, plus it is focused on issues associated with our industry and profession.

NP: What plans does AHIA have or is it considering for extending new value to its members?

Eddy: In 2009, we have begun offering webinars. These provide inexpensive CPE on a variety of topics for which no travel is required, further keeping costs down. The Library continues to be updated and expanded by our members who’ve taken AHIA’s motto to heart: “Excellence through Sharing.” Through our strategic partnering, our members may attend AAMAS conferences at their member rates, ACL courses are offered at AHIA educational sessions at excellent rates, and we continue to seek common ground with other potential partners.

NP: Mark, what organizations outside of work and AHIA do you belong to?

Eddy: Regarding professional organizations, I am a member of the American Institute of CPAs, the Tennessee Society of CPAs, the American Management Association, and the Healthcare Compliance Association.

Regarding professional work and AHIA do you belong to?

Eddy: I am a member of the American Institute of CPAs, the Tennessee Society of CPAs, the American Management Association, and the Healthcare Compliance Association.
Regarding charitable organizations, I recently completed a 6-year term on the Special Olympics Tennessee Board of Directors where I served as Treasurer, Chair-elect, Chairman (2 years), and Past-chair; also, I am a mason.

**NP:** What would you say is the best way for someone to begin to make a professional commitment to AHIA, or to another professional organization?

**Eddy:** Take the first step. Volunteer to help with something small at first, then progress from there. Time management is so important. I’ve seen many people spread themselves too thin, they get tired, and drop-out. Remember your family (and work to support them) should be your first priority. The excess time and resources are what you have to give back. Prioritize and choose wisely where you share.

**NP:** What encouragement would you offer to those of our members who may be considering becoming involved in AHIA leadership endeavors?

**Eddy:** At some point in everyone’s life, they will come to believe they need to give back. We’ve been helped along the way by many people, often not realizing it at the time. Obtaining a leadership position in church/synagogue/mosque, at work, in a professional organization, or in a charitable organization provides the greatest opportunity to give back to our society. However, no one starts in a leadership position. It has to be earned. So get involved. From AHIA’s standpoint, that means volunteering for a task force or committee, depending how much time you have. Get to know the people, learn how the organization functions. The leadership position will come if you want it and maintain your energy and commitment. There are plenty of associates, including each Board member, who will help you if you express an interest. We are all looking to be better teammates.

**NP:** Where did you go to college, what was your major? When you graduated did you see internal auditing as being your career?

**Eddy:** I started out wanting to be a lawyer and received a congressional appointment to West Point; however, I discovered pursuing the law was not likely so I left to attend the University of Michigan. I spent two years in Ann Arbor. My older brother talked me into pursuing an undergraduate accounting degree as a basis for becoming a corporate lawyer. I was admitted to the U-M business school, but transferred to Eastern Michigan University due to their accounting program reputation. I received my BBA with an accounting major from EMU in 1980. I interned for a public accounting firm in Detroit during the summer and winter recess of 1979. I loved the audit work but felt I could make a bigger difference as an internal auditor than as an external auditor. So, I pursued my career in internal audit. It’s funny, I never made it to Law School but have the opportunity to work with lawyers almost daily.

**NP:** Tell us about your time with HCA. How long have you been with them and what led to you signing on with HCA?

**Eddy:** I joined HCA Internal Audit in 1980. My older brother worked here in the mid-1970s before transferring as a hospital Controller. I’d met the HCA Vice President of Internal Audit at my older brother’s Nashville wedding and was invited to interview with HCA when I graduated. I interned in public accounting in 1979 and learned I loved auditing but realized I wanted to work in industry rather than with a firm. I also wanted to move to a warmer southern state. In 1987, HCA spun-off 104 hospitals to a new company: HealthTrust, Inc. I was invited by the Internal Audit Director to help him start the Internal Audit Department at HTI. In 1995, HealthTrust, Inc. was acquired by Columbia/HCA which subsequently resumed the name HCA.

The nice thing about my movements via divestitures and acquisitions is that all my work counts as one employer regarding retirement—not a bad deal. In my 29 years, I’ve never been bored because something new has popped-up every few years that has allowed me to learn new aspects of business, auditing and regulations.

**NP:** Mark, what famous person—living or dead—would you like to meet and why?

**Eddy:** Thomas Jefferson. He was a true renaissance man. He appreciated different cultures (serving as Ambassador to France), was an architect and inventor (visit Monticello if you’ve never been), a farmer, a man of letters (Declaration of Independence), an educator (founder of University of Virginia), a politician (House of Burgesses, Vice President, President), and a visionary (the Louisiana Purchase). He also had interesting disagreements with John Adams and Alexander Hamilton. It would be a fascinating discussion!

**NP:** Tell us about your family, Mark.

**Eddy:** I’ve been married to Wendy for 29 years. She is an accountant, too, but has focused her career more on the manufacturing industry. She is a Certified Management Accountant. We have one son, Matthew. He is twenty-five and got married this last spring. He and his wife live in Knoxville, Tennessee.

**NP:** Where did you grow up, Mark, and what is your favorite childhood memory?

**Eddy:** I grew up in Detroit, Michigan. My mother was a school teacher and my father was a Detroit policeman. Since my mother had “summer vacation” with the students, my father would schedule his work hours so he had the end of one month and the beginning of the next month off. Thus, for one month each summer we would camp and sightsee a new area of the country. I’d been to 44 states before I got out of school. American history classes were a breeze because I had seen and experienced so much of what we were studying.

**NP:** What are the titles of last two books you read?

**Eddy:** The Snowball: Warren Buffett and the Business of Life by Alice Schroeder and Master of the Big Board: The Life, Times, and Business of Jack Massey by Bill Carey. I highly recommend both books.

**NP:** Mark, thanks for taking the time to chat with us about yourself, your views and our association.

**Eddy:** You are welcome. It has been my pleasure.
The reality of healthcare operations today includes oversight of an increasing volume of personal health information which must be protected. Although the protection of sensitive and personal data has always been good business strategy, implementation has often been tactical and opaque managed by IT departments. New laws, rules, and contractual obligations are changing all of this and management needs to be more involved. Even as information privacy and protection objectives grow more critical and complex, they are also increasingly subject to scrutiny by both internal and external auditors.

Responding to the commercial threat of fraud and the private threat of identity theft, most economically advanced nations have now passed national privacy laws that govern the collection, use, and disclosure of personally identifiable information (PII).

**Consider physically reviewing the standard information and information requests that are sent to patients and other entities either by mail, electronically, fax, etc. These are so part of the normal routine paper “shuffling game” that people can totally ignore what PII actually appears on the forms.**

Privacy is about the Protection of Confidential Information

Simply put, privacy is the confidential preservation of personal and proprietary information that would not be readily available to use without the data subject’s explicit permission or entitlement. Although companies often limit privacy practices to customer data, the same usage and protection principles can, and often should, also apply to other kinds of sensitive information, such as employee and business-partner information, proprietary business data, sensitive financial information, and other types of information that should not be indiscriminately accessed or shared.

Especially given the broad scope of sensitive data, companies need to take a deep and critical look at the many business needs and legal requirements that impact the ways they collect, use, transmit, and store various types of information. Companies should always apply due care based on business needs and legal requirements. In general, four basic categories of control are involved:

1. What data may be collected and under what conditions
2. How data may be stored, managed, used, and transferred
3. How data must be protected from unauthorized and inappropriate access
4. How companies should interact with the individuals whose data they control

Although the realm of prudent privacy controls is very seldom limited to the mandates of law; the fundamental restrictions intrinsic to consumer-oriented privacy laws can be considered baseline control considerations for all types of sensitive data. The company should define the scope and nature of protected information, help in establishing policies and procedures for information protection, and align technologies and resources to ongoing privacy assurance efforts. A company’s specific policies and procedures for data breach notifications, collection limitations, consumer control over data, and other controls depend on industry, business practices, customer expectations, and other factors.

Management and internal auditors should look at all standard customer/patient requests with ‘fresh eyes’ to see what information is supplied as a routine matter of business.

**Why Should We Care if Data Protection and Privacy Efforts are working well?**

Its good business practice! Personal identity theft, intellectual property (IP) leakage, bank fraud, and payment-card data theft are serious concerns with significant financial ramifications.
To respond to the increasing number and level of threats, companies must provide concrete assurance of strategic and comprehensive privacy programs that incorporate managerial, operational, and technical controls. What many think of as information protection—primarily technical controls such as account access management, encryption, and secure software development protocols, and antivirus software—is just one piece of this complex puzzle.

Organizations also need to implement and regularly assess other, generally non-technical controls. Managerial attitudes and risk postures, espoused through information security policies, standards, procedures and guidelines are particularly important as is an ongoing investment and commitment to staff awareness and training programs. The development of privacy and communication/disclosure procedures and identity and access management programs (including routine managerial review of access entitlements) are needed. Vendor and contractor access rights and controls should also get a high priority. Overall, the organizational risk management program should identify, evaluate, and monitor key privacy risks. So, as you can see, the information companies must protect goes well beyond customer information and you need to track and manage all critical information maintained by the organization.

Roles and Responsibilities for Privacy and Data Protection Must be Assigned

Responsibilities for data protection are as pervasive as data itself and are part of almost every manager’s duty. The actions and attitudes of company directors, managers, office workers, contractors, business partners, and internal auditors all impact privacy and data protection control objectives.

The commitment to privacy assurance must start at the top, that is, with the organization’s leadership. Executive management in particular must provide constant, consistent leadership on privacy and data protection principles and demonstrate by example the necessity of policy compliance. Executive management must also ensure that business and IT departments have the budget and staff to effectively enact controls.

Executive technical managers—including chief technology, information security, and privacy officers—should take a more granular interest in privacy and data protection programs. They should contribute high-level strategic insight into business projects and initiatives that ensures information privacy and protection controls are planned and embedded throughout technology implementation lifecycles. Finally, your CIO, CTO, CISO, and CSO should all understand the privacy legislation affecting the organization.

Improve Privacy and Data Protection through Assurance

Although companies often conceptually and procedurally segregate privacy and information security, assigning administrative responsibilities to two different persons, the practices are two sides of the same coin and neither can be effectively evaluated in a vacuum. Privacy objectives and obligations provide direction, scope, relevance, and priority for information security controls. Information security provides the confidentiality, availability, and integrity of sensitive information that underpins privacy assurance.

Accordingly, privacy audits tend to focus on organizational processes: how information is used; whether those uses are legal, ethical, and supportable from the perspective of the company’s relationship with its customers; and how the organization communicates with customers and other entities about its privacy practices.

Resources Taking Privacy to the Next Level

1. IT Audit Checklist: Information Security
http://www.t2pa.com/

2. IT Audit Checklist: Privacy & Data Protection
http://www.t2pa.com/

3. AICPA-CICA Privacy Framework, Including the AICPA/CICA Trust Services

4. Health and Human Services (HHS) Centers for Medicare & Medicaid Services
   a) US HIPAA Security Educational Paper Series
   b) US HIPAA Privacy Rule
      http://www.hhs.gov/ocr/hipaa/finalreg.html

5. US Financial Modernization Act (Gramm-Leach-Bliley)
   http://www.ftc.gov/privacy/glbact/glbsub1.htm

6. Payment Card Industry (PCI) Data Security Standard (DSS)
   https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

   https://www.isfsecuritystandard.com/SOGP07/index.htm
Information security assessments evaluate managerial oversight and operational practices. Auditors should look at automated processes for user authentication, systems access, technology configuration, and other security measures within information systems; and management must support this evaluation with periodic performance of functional tests, evidencing of system performance, and maintaining complete and current technical documentation. (See my column titled: Improve IT Security: Educate Staff—New Perspectives June, 2009 Volume 28 Number 2).

A typical audit scope for internal auditors to consider includes: policies, procedures, and the organization’s plans for data protection, incident response, and customer consent management; employees’ roles, responsibilities, and accountability related to privacy and data protection; data collection and use in relation to intended purposes, legal constraints, and customer consent directives; employee awareness and education programs as well as employee hiring, transfer, and termination controls; control monitoring and reporting; and existing practices benchmarked against good practices for information security.

Privacy and security audits should be performed regularly, and over time cover the entire enterprise. Privacy assessments should be conducted on all new projects and on major enhancements to existing systems.

Within the scope mentioned above, auditors will generally evaluate controls under three major groupings:

Management controls
Management controls encompass the managerial programs, support, and foundations for effective, efficient privacy and data protection programs. In general, management control audits assess whether: privacy and security policies and procedures have been established; performance metrics are documented and performance is measured; controls are supported by adequate budgets, staff, and other resources; and a continuous improvement program is in place and operates effectively.

Key question: Has the organization required personnel to confirm their understanding of privacy policies and procedures before authorizing access to sensitive information?

Operational controls
Operational controls encompass operational processes in which privacy and data protection are a factor, how the organization overseas privacy and data protection, and the measurement of control effectiveness. In general, operational control audits assess whether: rules and requirements exist and are documented, controls exist, employee and managerial actions are in alignment with regulatory requirements, operational processes support privacy and security objectives, and appropriate managers regularly review key performance reports and operating results.

Key question: Does the organization perform risk assessments to determine the potential material impact and harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization? The risk assessment should include possible impacts on:

- brand value
- stock value and investor relationships
- legal liability and regulatory sanctions
- customer and class action litigation
- customer and employee loyalty and trust

- revenue from customers, business partners, and other relationships

The risk assessment considers and documents a worst-case scenario for the compromise, corruption, or misuse of the entire set of data subject to the assessment.

While management should lead the above risk assessments I believe internal audit should participate, although each organization’s approach could be different.

Technical controls
Technical controls encompass systems and automated functions that support privacy and data protection goals. Technical controls address risk inherent in system design, access, and operation, as well as risks inherent in the business processes facilitated by organizational technologies.

Be Proactive—Evaluate Privacy and Security Efforts Now
The bottom line—internal auditors should: 1) be like the organizational doctor who completes regular physicals that assess the health of the organization’s vital organs and verifies that the organization is taking the necessary steps to stay healthy and secure; and 2) encourage management and the board to invest in privacy and information protection practices that contribute to sustainable performance and ensure the reliable protection of the organization’s information.

While many will indicate “We’ve put HIPAA in place, identified a privacy officer, educated staff, what else needs
It’s time we confirm things are as they say, and more importantly, identify what the key improvement opportunities are.

In closing, as in all audits, it must be stressed that managers, not auditors, are responsible for defining and implementing solutions to issues found in the audit. Auditors can help management to understand identified risks, best practices, and common privacy and data protection frameworks; however, auditors cannot—and should not attempt to—dictate management’s response to known deficiencies. Such an effort would undermine auditor independence and degrade the value of the audit process itself.

Finally, the two IT audit checklists cited this month (see sidebar) provide extensive commentary and guidance regarding tackling the evaluation of your organization’s privacy and information security programs. As always, I welcome hearing about your successes and “lessons learned”, please contact me at dswanson_2008@yahoo.ca.

Dan Swanson, CIA, CISSP is a 26-year internal audit veteran, who recently was the director of professional practices at the Institute of Internal Auditors. The author of more than 100 articles on internal auditing, Swanson is currently a freelance writer and management consultant. He can be reached via email at dswanson_2008@yahoo.com.

To be done?”
Moving to the Next Level: Consulting Skills for Internal Auditors

By John J. Hall, CPA

Executive Summary

Management’s audit team expectations are higher than ever. The traditional auditor roles of compliance assurance, information verification, and control testing must be supplemented by value enhancing ideas for operational and technical improvement.

This article suggests several skills that are required for auditors seeking to provide measurable value on every audit project by including an ‘internal consultant’ approach to their work. Readers are encouraged to examine their current levels of mastery in each skill discussed and to seek proactive solutions to enhancing their existing abilities to meet fully the growing expectations of organization leaders.

Introduction

Let’s start by describing where internal auditing intersects consultative auditing. In his book Flawless Consulting, author Peter Block provides the roadmap for anyone providing consultative service to organizations. Block does an excellent job of providing definition and focus to any internal auditor seeking to incorporate a consultative approach as part of their work. On the first page of his book Block states, “A consultant is a person in a position to have some influence over an individual, a group, or an organization, but who has no direct power to make changes or implement programs. A manager is someone who has direct control over the action. The moment you take direct control, you are acting as a manager.”

With no direct line control over management actions, internal auditors fall under the umbrella of internal consultants. We want to improve our employer’s condition but our ideas and suggestions must first be sold to management for them to implement. Ideas sell best to management when consulting skills are employed. Since eliciting management action to undertake needed change is a core aspect of an audit, we need focus on developing consulting skills as a competency.

Consultants can naturally be broken down into two categories: internal and external. Keep one critical point in mind when functioning in an internal consultant mode: our assignment is not to fix the problem but rather to move management toward taking effective action. The skills discussed below are all designed for internal auditors to help well-intentioned managers identify and implement actions that will effectively and efficiently address problems and opportunities in their work environment.

Level One: Technical Skills

Before anyone can act in a consultative manner, a solid foundation built on technical skills must be in place. Among the technical skills foundation are the following:

- Internal auditing standards and practices adherence.
- Audit test design, execution, and documentation knowledge.
- Audit report and other document writing skills.
- Industry and employer organization expertise.
- Accounting, information technology, logistics, engineering, manufacturing, or other relevant expertise.
- Internal audit administration, planning, supervision, and project leadership competency.

Mastery of these internal auditing technical skill areas is required in order to perform internal consulting tasks. But before you are invited into internal consulting opportunities, your technical skills must clearly exceed the foundational skills mentioned above. Again from Peter Block, “Either in college or in our first job, we were trained in a specific field or function. This might be engineering; sales; accounting; counseling; or any of the thousands of ways people make a living. This is our basic training. It is only after acquiring technical expertise that we start consulting. If we didn’t have some expertise, then people wouldn’t ask for our advice.”
Ask yourself: What areas of legitimate expertise do I have? On what subject areas relevant to my company do I have expertise to take to my management team? Does management perceive me as having this expertise? In short, what do I know that they would be willing to pay for?

Level Two: Behavior and Communications Skills

Once we have a solid foundation of technical and auditing skills, we are ready to master the behavior and communications skills needed for full implementation of a consultative approach to our work. While there are many specific skill areas to be mastered by the consultative auditor approach, here are four to consider.

Establishing and Building Rapport

Many audit projects for auditees are not optional exercises. Rather, the audit is our process burdened upon them. It is an imposition on their daily work responsibilities. If given some say in the matter, many managers and staff of the organizations we audit would probably just as soon have us ignore them and go audit elsewhere. Some managers may have a lingering feeling from past audit experiences that their needs were not fully met and their opinions were not adequately respected or communicated. We must master the skill of establishing and maintaining legitimate rapport with those we audit. Rapport is the level of trust that exists between two people. It is normally built over a period of time as individuals work together. Our challenge is that we often simply do not have the time for this process to develop on its own. Audit projects may run only a few weeks and we often start day one with no prior experience with or working knowledge of the people and departments we audit.

We must, however, take specific proactive steps to create and maintain a relationship of trust with the managers and staff we are auditing. We must show our audit clients that we understand their priorities and performance measurement variables. We must look for opportunities to demonstrate our interest in improving their work performance, quality of results, and how well their goals are being met.

When blending consulting skills into an internal audit assignment, we need to balance traditional audit project objectives with building a collaborative working relationship based on mutual trust. We need to take the initiative in building that relationship starting with our first contact and continuing throughout every phase of the audit work, and continuing on afterward.

Creating a Positive Relationship

- Show people they are important
- Frame issues as mutual problems
- Listen first, talk second
- Find common ground
- Share a vision
- Don’t compete
- Be cooperative
- Be empathetic
- Be receptive
- Be sensitive
- Be honest
- Keep your word
- Keep in touch

We must master the skill of establishing and maintaining legitimate rapport with those we audit.

To counteract any barriers that may exist, we must master the skill of establishing and maintaining legitimate rapport with those we audit. Rapport is the level of trust that exists between two people. It is normally built over a period of time as individuals work together. Our challenge is that we often simply do not have the time for this process to develop on its own. Audit projects may run only a few weeks and we often start day one with no prior experience with or working knowledge of the people and departments we audit.

We must, however, take specific proactive steps to create and maintain a relationship of trust with the managers and staff we are auditing. We must show our audit clients that we understand their priorities and performance measurement variables. We must look for opportunities to demonstrate our interest in improving their work performance, quality of results, and how well their goals are being met.

When blending consulting skills into an internal audit assignment, we need to balance traditional audit project objectives with building a collaborative working relationship based on mutual trust. We need to take the initiative in building that relationship starting with our first contact and continuing throughout every phase of the audit work, and continuing on afterward.

Ask yourself: How effective are you at establishing rapport with those you audit—especially when there is observable resistance to the audit? What specific steps can you take on an upcoming project to build rapport during each interaction?

Listening and Interviewing

One of the places where traditional auditing and the consultative approach will intersect is the collection and analysis of relevant data. While much of the data used by an auditor comes from transaction records and other documents, much can also come from human sources during project interviews and ongoing discussions. This human source information gathering is the forte of a consultative approach while the former can be achieved via the old ‘gottcha’ style of auditing.

Gathering audit information through interviews is a core skill that all auditors must begin to develop early in their audit careers. But the interviewing skills necessary for consultative auditing go much further. The internal auditor consultant must become a master of interview to:

- Collect and organize data in a manner leading to the root causes of problems and missed opportunities
- Test possible solution scenarios
- Motivate managers toward action where action is needed
- Identify organization and personal resistance that may not surface in other data collection

Consultative interviews offer a number of challenges for the auditor. All information comes to us through the interviewee’s filters. Relevant information may need to be confirmed for accuracy and applicability. Some information collected will be irrelevant. There may be a mismatch in business or technical experience levels between interviewer and those being interviewed. The consultative auditor should take proactive steps to recognize and react to these challenges.

Consultative auditors must take their interviewing and listening skills to a high level. We must be sensitive to the spoken responses to our inquiries and to the subtleties of the interviewee’s style, words, and non-verbal messages. Consultative interviewing relies quite heavily on open-ended questions. And it seeks a higher level of open discussion of issues, causes and ‘what if’ scenarios than might normally be the case in compliance-based audits.
**Ask yourself:** How effective are you at planning, conducting and summarizing consultative interviews? What specific actions could you take to improve your performance in this critical area?

**Speaking and Presenting** Throughout all phases of consultative audit projects, we must be able to stand and competently present our process, our findings and observations, our conclusions, and other relevant information. We must also be able to handle questions, resistance and outright disagreements. Murphy’s Law is in full effect during presentations: anything that can go wrong probably will.

All audit professionals, regardless of level, can and should master speaking and presenting skills. It is a skill where we can all make great strides with instruction, mentoring, coaching, constructive feedback, and especially practice and repetition. Consultative auditors must be able to present in situations including one-on-one, small groups (kick-off meetings, project status meetings, closing conferences), and large group settings (training, board meetings, department conferences).

**Ask yourself:** How effective are you at standing and speaking in front of others? How could you improve?

Who is the best speaker in your group? What do they physically do in planning, delivering and analyzing their presentations that you could copy in your presentations? How could you get effective supportive feedback on your own presentations?

Don’t kill your ideas through ineffective presentations. Get better. Much better.

**Selling Audit Ideas** It was once said that, “if auditors were in the used car business they’d all be on welfare.” Whether we like it or not, auditors are all in the sales business. Not selling products. But selling ideas that can help those we audit be more effective, fully comply by standards, and improve individual and group performance. All of our planning, testing, interviewing, analyzing, concluding, summarizing and reporting are of minimal value if no action occurs. Getting management to act where action is appropriate is critical to the success of a consultative auditor. While independent external consultants theoretically have no vested interest in whether the client organization takes action in response to a consulting project, consultative internal auditors very much care if their organizations adopt improvement ideas generated through the audit process.

**Ask yourself:** How effective are you at motivating those you audit to take effective action? Do they recognize the inherent value for them in your ideas? Do your ideas have the potential to truly improve their results? And when managers do not act on ideas generated during audits, do you analyze why no action occurred and adjust your approach?

As with the other consultative skills mentioned in this article, selling audit ideas and getting people to act is a skill that must be mastered. For most of us it is not naturally ingrained in us. Training and mentoring are a great help. But for this skill, so is reading. Here are a few suggestions to get you started:

- **The One Minute Sales Person** by Spencer Johnson is a quick read that provides the basics for anyone involved in motivating others over whom we have no direct control. Written in a story form, it chronicles the search by a seasoned sales professional to improve their existing skill set. The book translates perfectly to the auditor consultant’s daily responsibilities, and it provides specific action steps to improve our audit/sales effectiveness.

- **Selling the Invisible** by Harry Beckwith focuses on the role of concept marketing in getting others to act. It is helpful for the auditor consultant in setting the right tone with those we audit, and provides specific suggestions for getting managers to be receptive to the audit and our ideas.

- **Nudge** by Richard Thaler and Cass Sunstein was my favorite book of 2008. The authors are experts in the field of choice architecture. The book highlights how susceptible we all are to various often irrational biases in our decisions and resulting behavior. The book describes the “groundbreaking discussion of how we can apply the new science of decision architecture to nudge people toward decisions that will improve their lives…” Very useful information for nudging management teams toward action. Extremely useful for nudging our own behavior toward greater effectiveness.

**Level Three: Auditor Internal Consulting Skills**

Let’s assume that we are well on the way to mastering our core Level One: Technical Skills and our Level Two: Behavior and Communications skills. We are now ready to utilize these skills in internal audit consultative situations.

In **Flawless Consulting**, Peter Block methodically leads the reader through five phases of a formal consulting project. These phases match nicely the normal work approach internal auditors use on traditional audit projects. In the brief description of the five phases below, look for the opportunities to utilize the Level One and Level Two skills.

*In Phase 1—Entry and Contracting,* the auditor consultant and the auditee client come to agreement on a need that exists, match the auditor consultant’s expertise to that need, and define the auditor consultant’s role in addressing the need. It is during this phase that the who, what, where, and how questions of the work approach are defined.

*In Phase 2—Data Collection and Diagnosis,* the auditor consultant should feel right at home with this one. After all, this is what we do in our audit work. But using the consultative approach, the auditor should consider going beyond the normal audit data sources. Depending
on the scope of the assignment and the complexity of the issue, we might consider interviews of a broader range of sources, original research, questionnaires and surveys, competitor research, and other information not generally utilized on compliance-based internal audits.

**Phase 3—Feedback and Decision to Act**, is where our conclusions are presented and an action commitment by management is sought. During this phase, the Level Two skills of speaking, presenting and selling audit ideas are critical. The techniques highlighted in the suggested books *The One Minute Sales Person* and *Nudge* are especially useful during Phase 3.

**During Phase 4—Implementation**, managers either do or do not take the steps agreed to in Phase 3. The internal auditor consultant may have minimal if any responsibilities during this phase with the exception of monitoring management activities.

**During Phase 5—Extension, Recycle, or Termination**, in this phase we evaluate the results of the entire process and make decisions with management about whether to extend, renew or end the consultative efforts. At a minimum, internal auditor consultants should review their own results with the goal of adjusting their approach when the next consultative audit opportunity comes along.

Obviously, the short description just presented cannot do proper justice to the process of internal consulting or to Peter Block’s specific recommendations. But if your curiosity is aroused, perhaps you will invest in *Flawless Consulting* with the goal of selecting from its many ideas those specific action steps you can take to provide a consultative approach on every audit project you undertake.

**Summary**

We find ourselves and our organizations in a time of tremendous economic pressure and uncertainty. Our managers need and want our help. By making the changes needed for a consultative approach to our internal audit work, we may just find that the time has never been better to help management deal effectively with business challenges, gain acceptance of our work approach and results, and enhance the perception of internal auditing as a legitimate expertise-based resource for future opportunity. Examine your current skills. Take steps to shore up weaknesses. Look for opportunities to utilize a consultative approach in regular audit assignments. And make sure your management team knows about your interest and expertise.

John Hall is the president of Hall Consulting, Inc. located in Vail Colorado. He specializes in auditor effectiveness and fraud risk management training programs and presentations. He is a frequent speaker at conferences and company seminars. John’s e-mail address is jhall@hallconsulting.biz.
Economic Stimulus: Major Implications for Privacy and Security of Electronic Health Records

By Jan Hertzberg, CISA, CISSP, and Jim St. Clair, CISM, PMP

President Obama signed a $787 billion stimulus package into law on February 17, 2009—the American Recovery and Reinvestment Act of 2009 (ARRA). The ARRA creates the Health Information Technology for Economic and Clinical Health (HITECH) Act which establishes some $19 billion in incentives for the adoption of health information technology (HIT) by hospitals and physicians and helps drives forward one of the President’s major objectives: adopting electronic health records (EHR).

The paramount importance of safeguarding privacy and security, including new standards for encryption and breach notification, are critical aspects of many of the new standards. ARRA strengthens enforcement of federal privacy and security laws by increasing penalties for violations, and provides greater resources for enforcement and oversight activities. Given the sizeable incentives and stiff penalties, healthcare organizations and their vendors need to understand how the HITECH Act will affect them. Moreover, now more than ever, they need to assess and take steps to minimize their organization’s exposure and vulnerability to potential security and privacy breaches by putting in place an effective information program to mitigate these risks.

Expansion of HIPAA Definitions

As healthcare organizations begin to implement electronic health records, the Health Insurance Portability and Accountability Act’s (HIPAA) privacy and security rules will no longer be sufficient for managing these records. While ARRA does not abolish current HIPAA standards, it broadens the definition of breaches of confidentiality and establishes penalties for loss of personal health information (PHI) and record information.

Some of the other noteworthy expansions of HIPAA definitions under ARRA include the following: Business associates are now held to the same standards as covered entities regarding safeguarding, use and disclosure of PHI, and are subject to the same civil and criminal penalties for noncompliance. Certain types of entities are defined explicitly as business associates, including health information exchange organizations, regional health information organizations, e-prescribing gateways, and personal health vendors contracting with covered entities. Also, the Department of Health and Human Services (HHS) is authorized to conduct audits of both covered entities and business associates.

New Data Privacy Requirement: Establishes Standard for ‘Minimum Necessary’

Under HITECH, the new rules create a temporary presumption that ‘minimum necessary’ data is equivalent to the ‘limited data set.’ This means organizations will be treated as being in compliance with the minimum necessary standard only if it limits disclosure to a limited data set as defined under the Privacy Rule; or, if necessary, to the minimum necessary data required to accomplish the intended purpose of the disclosure.
Establishes Rules for Vendors and EHR

The term electronic health record (EHR) means an electronic record of identifiable health information that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. Vendors of EHR refer to entities, other than covered entities, that offer or maintain EHR. EHR identifiable health information includes information that is provided by or on behalf of the individual and that identifies the individual or could be used to identify the individual. EHR vendors are business associates when they contract with covered entities to allow a covered entity to offer a personal health record to patients as part of its electronic health record.

New Breach Notification Standards

ARRA also launches a new federal mandate regarding privacy of personally identifiable information (PII). Under the new rules governing PII, anyone processing PII will have to report to authorities on any breach if that breach impacts more than 500 individuals in a single jurisdiction. Vendors of EHR and their third-party service providers are subject to notification requirements in the event that security or privacy is compromised, regardless of whether the vendors are covered entities. Failure to provide this required notice will be deemed to be an unfair and deceptive trade practice under the Federal Trade Commission Act.

In the event of a breach, covered entities or business associates must notify individuals affected within 60 calendar days after discovery of breach, unless law enforcement requires a delay. The clock on the 60 days starts ticking when the first employee either knew or should have known about the breach. If the breach is by a business associate, that organization must notify the covered entity within the 60-day period.

The HITECH Act breach provisions are effective 30 days after the Secretary of HHS publishes interim final regulations—180 days after the date of enactment. As such, the effective date will be approximately September 15, 2009.

Developing an Effective Information Security Program

Healthcare providers, administrators and third-party service providers must take the time now to define their security procedures, and review insurance coverage and contract risk allocations. They must determine which databases, systems and files contain sensitive, personal information to ensure that controls are functioning properly.

This information security program should include an annual risk assessment process addressing the protection of personal information, security policies related to records retention, data access and transmission, training of employees in the handling and use of personal information, and controls and certifications over third-party service providers.

Under the new provisions of the HITECH Act, the penalties for mishandling personal information are substantial. An effective information security program can give organizations the tools they need to effectively protect their most precious business asset: customer information.

Authors

Jan Hertzberg, CISA, CISSP, leads the Chicago Business Advisory Services Information Technology (BAS IT) Group. Jan has over 25 years of experience helping multinational companies in healthcare, financial services and telecommunications develop infrastructure, systems and internal IT controls for enhanced reliability and regulatory compliance. He may be reached at (312) 602-8312 or at Jan.Hertzberg@gt.com.

James St. Clair, CISM, PMP is a Senior Manager and leader of Grant Thornton’s Global Public Sector Risk Management, Controls, and Security (RMCS) practice, which focuses on Enterprise Risk Management (ERM), IT Security and Internal Controls. He has thirteen years’ combined experience in technology risk management, controls assessments and security for public utilities, government agencies and private industry. Prior to joining the private sector, Jim was an Officer in the United States Navy. He may be reached at (703) 637-3078 or at jim.stclair@gt.com.

The world of achievement has always belonged to the optimist.

~Harold Wilkins
The celebratory fireworks came a few days early for AHIA. Communication Concepts notified Association Headquarters on June 30 that *New Perspectives* was selected for two 2009 APEX Awards for Publication Excellence.

*New Perspectives*, Kenneth Spence, CFE, Editor, received the award for Most Improved Magazines & Journals.

The *Letters to the Auditor Column*, authored by John Landreth, CPA, CHC, CFE received the award for Regular Departments & Columns.

“It is particularly gratifying to have been selected from the thousands in this competition for communication professionals,” said Ken Spence, Editor. “The goal of the Editorial Committee has been to take *New Perspectives* to the ‘next level’ and as such that has been my primary charge. Receiving these awards, the second consecutive year *New Perspectives* has received national recognition, is solid evidence that we are moving in the right direction. This is really made possible only because of the outstanding authors and columnists who have so graciously given of their knowledge, skills and time. I am especially heartened that John Landreth has been singled out for this significant award. He is our ‘dean’ of columnists in that 2009 marks his 20th year of *Letters to the Auditor*, an idea he originated.”

Upon learning of the awards, Mark Eddy, 2009 AHIA Chair, extended his congratulations the entire Editorial Committee, and all our authors. “You’ve done a great job raising AHIA’s profile and standing in the profession.”

We look forward to continuing to improve *New Perspectives* by featuring the most relevant and meaningful information of importance to our readers. To learn more about the APEX awards, visit http://www.apexawards.com/.
AHIA Mission Statement
The Association of Healthcare Internal Auditors (AHIA) is an international organization dedicated to the advancement of the healthcare internal auditing profession, which includes auditing disciplines such as operational, compliance, clinical/medical, financial and information technology. AHIA is committed to:

- Providing healthcare auditors with specialized education and networking opportunities
- Providing leadership to the healthcare audit profession

AHIA Vision Statement
Healthcare leadership and the healthcare internal auditing profession recognize AHIA as the catalyst for continually elevating the quality of healthcare internal auditing and advancing the profession and its members. AHIA embodies ‘excellence through sharing’ and is the healthcare auditors first choice for education and leadership specific to this multi-disciplined profession and for information on best practices and industry and professional trends. AHIA is a leader in partnering with other organizations to expand professional resources.
Please provide your primary contact information below: I was referred to AHIA by:

Dr. / Mr. / Ms. _____________________ Degree/Suffix _____________________

Affiliation: ________________________

Title: ______________________________ Office: ( ) _______________________

Address: __________________________ Fax: ( ) _________________________

Address: __________________________ Home: ( ) _______________________

City: ___________________ State: _______ Zip: _______ Country: _________

E-mail: ____________________________ Web: _________________________

The address above is a: [ ] Business [ ] Home [ ] Both

Membership includes a $65.00 per year subscription to the New Perspectives Journal, both printed and electronic versions.

AHIA Individual Membership Levels:
- [ ] 1 Year Membership = $200
- [ ] 3 Year Membership = $555
- [ ] 1 Year Faculty Membership = $75
- [ ] 3 Year Faculty Membership = $210
- [ ] 1 Year Student Membership = $40
- [ ] 3 Year Student Membership = $105

Membership Total

AHIA Group Membership Levels:
Please provide additional names and contact information on back for group members or provide additional sheet. All Prices below are Per Member.
- [ ] 2-5 Members:
  - 1 Year = $180/member
  - 3 Year = $510/member
- [ ] 6-20 Members:
  - 1 Year = $155/member
  - 3 Year = $435/member
- [ ] 21-50 Members:
  - 1 Year = $125/member
  - 3 Year = $345/member
- [ ] 51+ Members:
  - 1 Year = $90/member
  - 3 Year = $255/member

Total Number of Members: _______ X $ _______ = _______ Membership Total

Additional Information:
1. Highest Education Degree ________________________ 7. Position (Check the box that most accurately describes your job position; check one box only.)
   - Executive: ________________________________ Staff:
   - Chief Audit Executive or VP Audit Services
   - Chief Compliance or VP Compliance
   - Director:
   - Audit Director (Internal/Medical)
   - IT Audit Director
   - Compliance Manager
   - IT Audit Manager
   - Compliance Manager
   - Manager:
   - Audit Manager (Internal/Medical)
   - Other:
   - External Public Accountant
   - Corporate Management
   - Educator
   - Audit Committee Member
   - Management Consultant
   - Other

Your name, address, and email address will automatically appear in our online membership directory available only to members, and your email address will be used to send you information regarding AHIA. Opt out options are available online.

Payment Information:
- [ ] Check/Money Order [ ] Visa [ ] MasterCard [ ] American Express

Card Number: ____________________________ Exp. Date: _______

Name on Card: __________________________ Signature: __________________________

Make your check or money order (in U.S. funds) payable to AHIA.

Please FAX or MAIL your form to: 10200 West 44th Avenue, Suite 304
Wheat Ridge, Colorado 80033-2840, USA
FAX: 303-422-8894
Association of Healthcare Internal Auditors
Membership Application
www.ahia.org

Additional Organizational Members:
Name: Dr. / Mr. / Ms. ________________________________
Affiliation: ______________________________________
Title: ___________________________ Wphone: ________
Address: ________________________ Fax: ______________
City: ___________________________ State: _______ Zip: ________ Country: ______________
E-mail: _________________________ Web: ______________

Name: Dr. / Mr. / Ms. ________________________________
Affiliation: ______________________________________
Title: ___________________________ Wphone: ________
Address: ________________________ Fax: ______________
City: ___________________________ State: _______ Zip: ________ Country: ______________
E-mail: _________________________ Web: ______________

Name: Dr. / Mr. / Ms. ________________________________
Affiliation: ______________________________________
Title: ___________________________ Wphone: ________
Address: ________________________ Fax: ______________
City: ___________________________ State: _______ Zip: ________ Country: ______________
E-mail: _________________________ Web: ______________

Membership Categories
All categories include a subscription to the New Perspectives Journal both printed and electronic versions.
Individual Member: Any individual is eligible to join AHIA as long as they are interested in the healthcare auditing profession.
Group Memberships: Individuals are eligible to join as a group at discounted rates. Members will be enrolled based on employment under one organization name, with one source of payment. Discounts vary based on the number of individual members joining or renewing from the same organization.
Faculty Membership: To be eligible for a faculty membership, a member must be an active faculty member or professor (adjunct or full) at a junior college, college or university. Proof of your faculty status must accompany your membership application or at each renewal period. The proof of status can be either a letter from the Department Chair or Human Resources Department.
Student Membership: To be eligible for student membership, a member must be enrolled as a full-time undergraduate student in a junior college, college or university. Full-time status is defined as 12 hours/semester, trimester or quarter. Proof of your undergraduate status must accompany your membership application or at each renewal period. Student memberships will expire after five consecutive years.