



Are Your Audit Priorities Aligned with the Organization's Needs?

By Dan Swanson, CIA, CISA, CISSP

Internal audit efforts must be risk-based and contribute to the long-term assurance needs of the organization and its board. A formal audit risk assessment should be completed at least annually and the results of that assessment should direct internal audit priorities.

As the summer approaches it is an excellent time to refocus your sights on the long-term horizon. For example, what does the organization want to achieve over the next three to five years, and what does it need to do to get there? Certainly, each organization will have different goals, objectives, issues, and challenges; and no single "standard" long-term internal audit plan will work; however one option is presented below.

The Top 12 Internal Audit Priorities

Over the next few years, internal audit departments should evaluate their organizations' efforts in the following areas and provide their "opinions" to management and the board.

1. *The Top Three (to Five) Most Significant Business Initiatives.* We should be auditing the most significant business initiatives. Internal audit should also complete a very robust analysis of the IT component for each of these initiatives. Internal audit can also play an advisory role where beneficial. The bottom line—internal audit should be assessing the critical business initiatives that the organization is implementing as part of its long-term strategic plan.
2. *The Enterprise Risk-Management (ERM) Program.* ERM is a silver bullet for improving governance and organizational results because it identifies key objectives—and managing risks that accompany those objectives is effective governance. Whether your organization is a proponent of COSO's risk-management framework; the Australian risk-management standard; the governance, risk, and compliance guidelines from the Open Compliance and Ethics Group (OCEG); or other standards, it is time for organizations to take ERM to the next level. Completing an internal audit of the organization's ERM efforts will provide a baseline assessment report that will reveal gaps in risk management. Risk management is one of the key management activities in achieving cost-effective health operations over the long term. For example, Community Benefit spending has been the tax-exempt justification for the not-for-profit status of most of the hospitals in the U.S. The federal government and many states are examining the degree that hospitals are meeting their obligations regarding community benefit spending with the goal of removing the tax-exemption for some hospitals. The auditor can assist the organization by evaluating the annual 990 form and the Community Benefit report, and reporting process, and other contractual obligations to determine if the organization is at risk. And for many (most?) organizations the risk of fraud needs to be closely monitored and regularly evaluated.
3. *The Business-Continuity Program and the Disaster-Recovery Program.* BCP and DRP are on most lists of top-10 priorities; the problem is that they often rank in the bottom half. It is now time to ensure that the organization's resiliency efforts are truly operational. Establishing a robust preparedness capability is also one of the best investments an organization can make; auditing BCP and DRP efforts will assist the organization in ensuring that the proper attention is given. An effective business-continuity capability is essential, although being able to recover IT is critical. Operational resiliency is becoming an overarching organizational priority and auditing BCP and DRP efforts will help ensure the organization is better prepared for business interruptions (because they will happen). Also, consider auditing the organization's Emergency/Pandemic Preparedness Plan.
4. *The Information-Security and Privacy Program Efforts.* Protection of an organization's assets is a critical activity; for some organizations it is the most critical activity. While other industries have increased their focus in this arena, healthcare providers have not made the same level of commitment thereby increasing the risk to the industry and the organization. Auditing an information-security program is also a long-term effort involving many audits over many years, and it is time to start this long-term assurance effort. A very simple starting test: Has the effectiveness of your security efforts been discussed at the board level this year? As organizations roll out electronic health records systems, information security and information privacy will become ever more critical. Finally, the privacy of our information has moved to the very forefront of organizational risks. Most security is all about protecting data that has to be kept private. But not enough auditing of privacy efforts is being done.
5. *The Overall Governance Regime.* Corporate governance; organizational

governance; performance accountability; governance, risk, and compliance—governance goes by many names. Internal auditing provides assurances to management and the board regarding an organization's governance, risk-management, and controls processes. Therefore, fundamentally, internal audit should provide an opinion regarding the overall governance "regime," regardless of the exact term your organization uses to describe its efforts. Does your health organization take governance seriously? Sarbanes-like requirements for not-for-profits in healthcare is on the horizon and Internal Audit can assist the organization by moving the organization toward management's examination and documentation of entity-level controls, especially in regard to financial and regulatory reporting. Internal Audit can also play a key role in governance awareness and identification of key training areas.

6. *The Compliance and Ethics Program Efforts.* Compliance and ethics efforts have received significant attention (and funding) in the last ten years, and this will continue. Depending on the internal audit department's past efforts, audits of the compliance and ethics programs should either drill down into specific areas or become much more high-level to provide the board and senior management an overall assessment of improvement priorities. Typically lower priority, qui-tam litigation, coding, impending DRG Model change, medical necessity, and HIPAA regulations require increased focus for Internal Audit departments. Assessments of effective compliance programs should be considered as well. Audit and Board levels of risk have increased with regard to oversight. Also, what has impacted most organizations in the past few years? In government circles, (and I suspect in the private sector as well) there were numerous examples of 'failure to comply with regulations'. Granted, this can often be linked back to things like tone at the top, ethics, and governance, but a good ethics and compliance audit should identify the problem and the root cause.
7. *Records Management.* If your organization has not started upgrading its records-management

program to reflect today's regulatory requirements and technological capabilities, then the organization is "at risk." An audit of the records-management program will assist in the determination of what opportunities for improvement exist. Having a policy and not following it poses additional significant risk. The sea-change of moving to electronic medical records provides additional challenges and opportunities.

Establishing a robust preparedness capability is also one of the best investments an organization can make.

8. *The Quality of the Enterprise Information for Decision Making.* Information is critical to every organizational effort. The quality of the organization's information will directly affect organizational results and, therefore, should be assessed regularly—by management and internal audit. In my view, information management will become more critical every year. Quality of care initiatives should also be a focus area. Medicare and Medicaid are jointly moving to outcomes-based performance-measures which will affect reimbursement. CMS (Medicare) has already announced initiatives that will evaluate episodes of care and reimburse based upon the quality of care, necessity of care, and outcome. Hospitals will need to become more closely aligned with the physician community, and outcomes will no longer be measured separately but jointly.
9. *The IT Function's Efforts to Meet Business Needs.* This audit priority is very diverse. The IT function performs a broad range of services that has a substantial impact on business results. As a result, the IT audit priorities require a more detailed risk assessment to determine the audit priorities. Fundamentally, evaluating the IT function's efforts to meet business needs is a core

audit requirement. Assessing IT's effectiveness, efficiency, and "customer service" are the three main components of an effective IT shop. Deciding on further IT audit "focus" beyond these areas needs to be based on a more formal IT risk-assessment process. For example, movement to a true, comprehensive electronic medical record system is a trend in the industry that will warrant the attention of Internal Audit in the upcoming years. This trend will require greater focus on IT Auditing in the areas of security, HIPAA and Payment Card Industry (PCI) compliance, disaster recovery, business continuity planning, data integrity, data management, data access, system replacements, data center operations and systems integration, etc. I'd also recommend studying the 18th Annual HIMSS Leadership Survey (see resource sidebar).

10. *Board and Executive Management Service Requests (Consulting and Assurance Projects).* This audit activity is an important catch-all to assist with the specific or unique needs of the organization. It is also included in my top dozen to highlight the need for a customer service philosophy by the internal audit function. The percentage of the audit budget allocated to this important activity will differ widely, but it lets the board and management know that internal audit is responsive to the board's assurance and consulting needs. Of course, these special audit projects should be of significant value to the organization, and they should not distract from the delivery of the overall audit commitment. Auditors could be involved in initiatives to reduce operating and non-operating costs, improve the use of capital and capital planning, and debt management. Examination of service lines and service line productivity, reimbursement and cost gaps will also be essential to identify areas where programs can/should be scaled back or even eliminated if the community need is met elsewhere. Efficiency and effectiveness of operations will be essential, as will supply utilization, clinical staff scheduling, procedure scheduling, etc.
11. *Process Management, Including Continuous Process Improvement.*

The second-to-last audit priority relates to improving organizational performance. I label the audit priority “process management”; your organization might call it a Six Sigma or LEAN program, while others might call it a corporate quality-management initiative. This audit priority is focused on encouraging and confirming that there is an organization process-improvement program in place, whatever the title. If the organization has not established an organizational program to improve its performance on a sustainable basis, it is at risk. Further Medicare/Medicaid program revenue reductions are almost a certainty, creating more cost shifting to commercial and private payors, thereby impacting operating income. This in turn will put pressures on reimbursement and cash flow. As a result there will be a need to focus on revenue cycle processes and controls to shorten days in A/R, accelerate cash flow from payors, and improve point of service collection of co-pay and deductibles, improve non-operating income through better cash management and investment performance, etc.

12. *The Internal Audit Quality Assurance and Improvement Program.* This last priority relates to ensuring you have the capability to deliver on your client’s needs (all the other priorities), i.e. internal audit should assess its performance and identify key improvement opportunities. Meaning, we should practice what we preach! The board and senior management need to know that internal audit meets audit standards and applies best practice to its own work. Issues to be explored include managing people, talent and skill sets (including evaluating the need for co-sourcing) for the internal audit function, devising accountability metrics to demonstrate “value-addedness” to the organization, and finally, managing internal audit operating costs. It is also time for us to think about where we are, where we should be, and how we are going to get there. For example, we should be thinking about: moving to a risk assurance model; re-assessing the services provided to our stakeholders, interviewing them and thinking about

how effective we really are; whether we are positioned to understand and contribute to management of emerging business risks, and providing timely controls consulting; and the strategic development of our staff. Have you implemented the IIA’s QAR requirements?

Auditing an information-security program is also a long-term effort involving many audits over many years.

Define a Long-Term Balanced Audit Plan

As I mentioned previously, each organization is different, and its internal audit priorities will be different, too. Still, for any organization, internal audit’s priorities should be risk-based and should focus on the organization’s governance, risk-management, and control processes. Corporate-wide themes of cost efficiency, cost effectiveness, strategic management and control, quality management, process improvement, and so forth will (and should) influence your internal audit efforts over the coming years.

In general, IT auditing will become more important. For example, many clinical devices are now connected through networks to hospital information systems. Security, patch management, change control at the clinical device and application/systems levels will be new territory but will affect the quality of care and clinical outcomes (not to mention medical records as previously stated).

You also should ensure that the internal audit plan has a strong linkage with the organization’s strategic and compliance plans. The audit plan cannot cover everything but it should complete a balanced assessment of the strategic, financial, operational, and regulatory risks facing the organization. Finally, delivering on a comprehensive audit plan will be the one of the most difficult challenges for internal audit, but without agreement on

what needs to be done internal audit will not receive the resources it requires. **NP**

Dan Swanson, CIA, CISA, CISSP is a 26-year internal audit veteran, who recently was the director of professional practices at the Institute of Internal Auditors. Swanson has completed audit projects for more than 30 different organizations, spending almost 10 years in government auditing, at the federal, provincial, and municipal levels, and the rest in the financial services, transportation, and health sectors.

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_2005@yahoo.com.

Guidance

How to Establish an Internal-Audit Shop: <http://www.theiia.org/guidance/standards-and-practices/additional-resources/establishing-an-audit-shop/>

20 Questions Directors Should Ask About Internal Audit:

http://www.theiia.org/bookstore.cfm?fuseaction=product_detail&order_num=519

Key FAQs about the Internal Audit Profession:

<http://www.theiia.org/theiia/about-the-profession/faqs/>

The Path to Quality—a comprehensive step-by-step guide to world-class internal auditing:

<http://www.theiia.org/guidance/quality/the-external-quality-assessment-process/path-to-quality/>

The audit committee briefing “Internal Audit Standards: Why They Matter” provides executive guidance on the practice of internal auditing and the assurance internal audit can provide the audit committee.

<http://www.theiia.org/download.cfm?file=83632>

Other Resources:

18th Annual HIMSS Leadership Survey:

<http://www.himss.org/2007Survey/DOCS/18thAnnualLeadershipSurvey.pdf>

PwC: *Top Eight Health Industry Issues in 2008*