

IT Audit Basics

Due Professional Care

By Frederick Gallegos

Due professional care can be defined several ways. Some describe it as the respect shown an auditee and how an auditor conducts himself during an audit. Others might say it is the professional image expected of an auditor towards the auditee. Still others believe that due professional care denotes the expectation of adding value to the client by providing solutions instead of problems.

During an audit, some view the auditor as the cop and the auditee as the suspect. Auditors make inquiries, and investigate and test their conclusions. At the end, they indicate who is guilty of doing what, and the punishment is the recommendations made to the client. This may be a harsh way to look at an audit, but to the auditee it may be real life. The auditee has to answer to upper management and in some cases jobs may be affected based by the auditor's report.

No classes exist on the process of due professional care, but there are factors that contribute to the formation of due professional care in audit departments, including:

- Peer review
- Auditor conduct
- Communication
- Technical competence
- Judgment
- Business knowledge
- Training
- Certification
- Standards
- Independence
- Continuous reassessment
- High ethical standards

Several pages could be spent discussing each of these areas as well as delving into timeliness and client review. However, in 1996, the Orange County and Los Angeles (California, USA) chapters of ISACA® funded the development of a videotape, "Best Practices in IS Audit Management." One of the major areas addressed in this video is the subject of due professional care and its importance. According to this resource, there are seven areas that are the foundation of the subject of due professional care. These areas are peer review, auditor conduct, judgment, technical competence, business knowledge, certification and standards. They will be the focus of this article.

Peer Review

The audit profession relies heavily on peer review. Peer review shows IS auditors how they are perceived within the IS audit community. Peer reviews also help auditors develop good professional relationships with their peers. Someone within their own department, organization or external entity can perform these reviews. An external entity could be a public accounting firm reviewing the work of a client's internal audit department. Peer reviews are supported by ISACA, the US General Accounting Office (GAO), American Institute of Certified Public Accountants (AICPA) and Institute of Internal Auditors (IIA).

High-quality peer reviews should be performed on a regular basis and help reach the desired goals of management. The reviews should be given to assign criticism and praise where needed. During the first couple of years, IS auditors go through a transformation as they acquire the skills instrumental to their careers. The IS auditor should be reassessed continuously through these reviews to verify the adequacy of newly acquired skills.

The peer review also indirectly assures the client that the auditor is capable of performing the job duties as required by the guidelines of the audit. Areas to examine include the auditor's technical knowledge, communication, analytical skills and time management skills. Consequently, the peer review process ensures that the auditor possesses all the skills needed to perform the job duties and that the client receives a high-quality audit.

Peer reviews also provide a way of conducting continuous reassessment of audit goals. Continuous reassessment is necessary to stay on track in audits lasting longer than two to four weeks. They verify that the auditor has not lost sight of the audit's original intentions and that the scope remains the same. Auditors can easily lose themselves in other areas or go off on tangents during seemingly unending audits. The client is not paying for a jumbled mess of information or information on areas not previously agreed upon.

For this reason, the auditor needs to step back and reassess the situation. The auditor should make sure the goal of the audit has not changed. If the goal has changed and the audit is encompassing more information than previously thought necessary to support its conclusions, then a reevaluation of the audit scope is necessary. In this case, it is possible that the scope of the audit may need to be expanded.

Technical Competence

Auditees always want auditors to possess more technical competence. But because of the number of diverse platforms in common use, it is not realistic for an IS auditor to be an expert in them all. When staffing a technical review, most audit departments will partner individuals with the necessary expertise with auditors who need to gain the knowledge. Development plans for experienced auditors should always include the training of new auditors. In addition, the team should be provided the needed tools to effectively perform their audit steps.

If an audit department does not have the expertise to perform a review, two things can be done. First, an expert can be borrowed from another part of the organization to teach the audit group what is needed for the review. This way, the audit group retains the experience. Second, an experienced outsider can be hired to perform the audit steps in these areas. If outside experts are used, audit staff should learn from them what needs to be done for the next time a review is scheduled. Thus the audit department can share in the expert's knowledge.

Training is a key subcomponent of maintaining technical competence. There are many sources of training available. Management must support continuous training of the audit staff to meet the technical competence needed to perform today's complex IT audits.

Auditor Conduct

Auditor conduct is important because it sets the tone for the audit. If the auditor has a "gotcha" mentality, the auditees will not be open to discussing issues or receptive to audit recommendations. The auditor needs to work with the auditee to develop reasonable recommendations that either will eliminate the exposure or minimize the exposure to an acceptable degree. Most internal audit reports today include comments indicating that the recommendations have been discussed with the auditees and whether the recommendations have been implemented.

Another critical component to an audit function adding value to the organization is audit independence. This means the audit report and opinion must be free of any bias if the integrity of the audit process is to be valued and recognized for its contribution to the organization's goals and objectives. The auditor's conduct must reflect audit independence.

Judgment

Judgment is a key factor to ensure due professional care and perhaps the most difficult to develop. During each audit step, the auditor needs to determine whether a control exists and evaluate whether it functions as intended. Experience, business knowledge and risk exposure play a part in the evaluation. The client's exposure should be quantified to determine what the total impact to the business would be if the control were not working. The auditor's past experience would help provide recommendations to eliminate or minimize the exposure.

Typically, audit judgment is gained through experience and professional development. One of the earliest ways to develop audit judgment was writing audit steps. This guidance was developed by an audit manager or supervisor who was experienced in the organization's culture and processes. Historical audit records also were used as a basis to develop the audit steps to be performed by the auditor.

Today, this experience is captured through automated support systems for auditors, which allow them to assess past patterns and audit findings. From such audit support systems, records and experiences collected via the audit, workpapers can be retrieved and used as guidance. The auditors must exercise their judgment in accepting recommendations or suggestions from such support systems.

Professional development activities such as involvement in professional associations can help develop an auditor's judgment through learning about the experiences of others. Certainly, the Internet has helped in this area by allowing auditors to share their experiences and audit programs through listservs and web sites. Professional associations must be commended for their activities, which provide the best level of training and experience-sharing events for today's audit professionals. For example, best practices sharing can be used to aid auditors in similar situations, especially through the sharing of what worked and what did not work.

Business Knowledge

Auditors are fortunate in that they see how an entire company operates. They see a product being made, orders being taken, product being shipped to the customer, the customer being billed and receipt of payment. In addition, auditors are exposed to the management processes in place to ensure a smoothly operating environment. Gaining business knowledge can be time consuming, but it is necessary for audit reviews. At the 1995 ISACA International Conference, Carol Hyzer said the following about due professional care:

Due professional care is not just reporting findings to management, but it is also ensuring them that the issue or issues have been addressed. The only way this can be accomplished is if you are working with the auditee to ensure that it is being addressed before you bring this to management's attention. You are not there to be just a "tattle tale," you are there to make sure whatever is wrong gets fixed.

Effective IS auditors possess a variety of skills that enable them to add value to their organizations and clients. Technical training does not fully prepare IS auditors with the communication and negotiation skills required for success. These additional skills may be referred to as business knowledge skills. The IS auditor must fully understand the business, its goals, objectives, culture and operational requirements. Exposure to these skills can come only through experience and training.

An understanding of the client and its environment should be evident in the auditor's evaluation. Also, the auditor should possess an understanding of the cost of doing business, how controls impact that cost and how controls represent a deterrent to business loss or profitability if not maintained and monitored. This knowledge would help to identify the organization's high-risk/high-loss areas. Once the high-risk areas have been identified, the auditor can define the objectives and scope of the review. IS auditors must examine, gather and interpret information from automated and manual systems with the business objectives and goals in mind. Many of the nontechnical or supplemental

business knowledge skills are concerned with gathering information and, of comparable importance, presenting information. As such, these supplemental skills are readily transferable to other disciplines, such as finance, management and marketing.

When control exposures are identified, the auditor also must identify the associated risks and discuss them with management. The discussion will ensure that the auditor's evaluation of the risk is correct, and it will help with the development of a recommendation that will adequately address the exposure and add value to the organization. The final product IS auditors create is the information in their audit reports. If this information is not effectively and efficiently delivered with an understanding of the business, via solid oral and written communication skills, all value accruing from the audit process could potentially be lost.

Certification

An IS auditor's goal should be to attain the Certified Information Systems Auditor (CISA) designation. The CISA designation shows dedication to the profession and is an indicator of the high-quality work the client would receive. To achieve the certification, the IS auditor is expected to successfully pass the CISA exam, have a minimum of five years of professional IS auditing experience, subscribe to the *Code of Professional Ethics* and gain continued education.

Standards

Those who act as auditors must have a high standard of ethics. The term "auditor" is Latin for someone who hears complaints and makes decisions or acts like a judge. To act as a judge, a person must be ethical. If the auditor loses favor in this area it is almost impossible to regain trust from audit management and auditees.

Trust is thrust upon all auditors as they enter into the position. Whether an auditor is ethical in the beginning or not, each begins with the same amount of trust and good favor from the client or auditee. If the bond is not broken, the auditor establishes a good name as someone who can be trusted with sensitive material.

In today's world economy, trust is an unheard-of word. For this reason, it is imperative that ethics be at the top of a manager's list of topics to cover with new staff. Times are changing and so are the clients requesting services. Most managers will say they cherish ethics because they distinguish one person from the next.

For example, if a budget calls for numerous hours, it is unethical to put down hours not worked. It also is unethical to overlook something during the audit because the client says it is not important.

Speaking of ethics, Carol Hyzer, said:

One has to be objective, one has to be fair, and one has to be ethical. If I have to stress one thing above all with respect to due professional care, it's ethics. Sometimes our wants and desires to succeed and produce the best profit margin for our company get in the way of our ethical standing. I think at times we use gray areas with ethics. It's black, it's white, it's right or it's wrong. So, if there is one message I can give, it's have a high standard of ethics.

A fine line exists between what is ethical and what is legal. Something can be ethically wrong but still legal. However, with that being said, some things initially thought to be unethical become illegal over time. Often, if there is a large enough group opposed to something ethically, legislation may be introduced to make it illegal.

IS auditors who attain the CISA certification must subscribe to the *Code of Professional Ethics*, which requires, in both one's professional and personal conduct, that the ISACA standards are adhered to, confidentiality is maintained, any illegal or improper activities are reported, the auditor's competency is maintained, due care is used in the course of the audit, the results of audit work are communicated, and high standards of conduct and character are maintained.

Certified or not, IS auditors should adhere to the standards and guidelines issued by ISACA. Besides ISACA, there are several professional associations that have issued standards and guidance that may directly or indirectly affect the IS audit professional. For example, IS auditors in the US Department of Justice are required to meet the Government Auditing Standards issued by the US General Accounting Office as their primary audit standards criteria.

Legal Implications

The establishment of limited liability partnerships came as a result of a Big 5 organization that was taken to court by a client. Based on the firm's recommendation, the client selected a support system that failed to perform in the manner recommended and caused the company financial loss. The courts held the Big 5 firm liable for not exercising due professional care in the conduct of the work performed. The guidance the courts used to evaluate the issues of this case was the guidance issued by the AICPA. Since the firm held itself and its professionals compliant with AICPA's governing standards and guidance, the courts used this guidance as a basis for evaluating the evidence of the case. To date, an audit group has not been taken to court for a lack of due professional care, however, it does not say that the liability does not exist.

Conclusion

Due professional care is a necessary component of the audit process. A number of best practices successfully used by audit management, supervisors and staff to instill due professional care have been discussed. Ultimately, due professional care serves as a foundation to ensure that the client receives a high-quality review. Audit departments

should hire people who care about what they do. By caring, they put in the high-quality work.

References

Arthur Andersen LLP, *Control Self-assessment: Experience, Current Thinking, and Best Practice*, Institute of Internal Auditors Research Foundation, Altamonte Springs, Florida, USA, 1996

Hudoba, Steven; Carol Hyzer; Tom Truglio, "Best Practices of IS Management," ISACA International Conference, Orlando, Florida, USA, 1995

Gallegos, Frederick and Anna Carlin, "Best Practices in Due Professional Care," *EDP Auditing Series*, Auerbach/CRC Press, 1999

Goldblatt, Joe Jeff, *Special Events: Best Practices in Modern Event Management*, Van Nostrand Reinhold, New York City, New York, USA, 1997

ISACA®, www.isaca.org

ISACA Los Angeles Chapter and Orange County Chapter, "Best Practices in IS Audit Management," California State Polytechnic University, Pomona, California, USA, 1997

Roth, James, *Control Model Implementation: Best Practices*, Institute of Internal Auditors Research Foundation, Altamonte Springs, Florida, USA, 1997

Toney, Frank, *Best Practices of Project Management Groups in Large Functional Organizations*, Project Management Institute, Upper Darby, Pennsylvania, USA, 1997

Using the Best Practices of Information Technology in Government, Project Management Institute, Upper Darby, Pennsylvania, USA, 1997