IT Audit
Solutions Manual

Chapter One

Discussion Questions

1-1. Describe the two objectives of IT Governance. Which do you think is more important?

The two objectives of IT governance are to: (1) use IT to promote an organization's objectives and enable business processes and (2) to manage and control IT-related risks. As with many discussion questions, there is no "right" answer here. Both objectives are important. The answer could vary by industry and organization type as IT-related risks could be greater for some businesses than for others. Similarly, the use of IT for strategic business purposes could mean the difference between business failure and success.

1-2. Describe the various types of transactions that an IS might process in the course of acquiring raw materials for production.

Acquiring raw materials for production involves ordering the materials, receiving the materials, and paying the vendor. The information system would record each of these transactions and the data associated with them. For example, data entered in the system would include the supplier name, the terms of payment, shipping data, the name of the person making the purchase, and so on.

1-3. This chapter described several types of work done by IT auditors. Using the Internet, can you identify any other types of work these auditors might do?

Several Internet sites provide information about the work of IT auditors. Professional organization sites such as www.isaca.org and www.iia.org provide insight. The web sites for various auditing firms, such as www.ey.com or www.kpmg.com are also helpful. Auditing firms typically post services or solutions as a menu item at their web site. Selecting assurance services will provide you with information about the various assurance service lines offered by the company.

1-4. IT auditors often have technical skills related to specific software. One such software specialization area is enterprise resource planning (ERP) applications. Explain how an IT auditor could acquire and maintain knowledge about one of these software packages.

Knowledge about specialized software, including enterprise systems, is most often obtained through work experience. Auditors working for large professional service firms will "apprentice"

on job assignments that involve technologies new to them. A company may send the IT auditor to formal training or provide them with time to take online courses. Still, practical experience is always needed to master these systems. IT auditors wishing to learn how to audit a specialized technology may request working on engagements where clients use these IT systems. Internal IT auditors are limited in their experience to the technologies used by their firms.

1-5. CISA is the most common credential obtained by IT auditors. Discuss how this certification would add value for someone practicing IT auditing.

The CISA credential, like any other widely respected certification provides an IT auditor with credibility. An auditor with this certification will have a competitive advantage in the market place. Professional service firms encourage their employees to acquire certifications as they cite them when proposing work to clients. Someone purchasing services from an IT auditor is assured that if the professional has the CISA certification, they have passed a knowledge test and are up-to-date on current practices.

1-6. The AICPA recently created a new credential for CPA's who have specialized training and experience in IT. Discuss whether or not you think the CITP is likely to be a sought after credential by both IT audit practitioners and those contracting with IT audit professionals.

An example of an individual who has the CITP credential is Kevin Martin, of Kevin Martin and Associates, an accounting/consulting firm specializing in implementing mid-level accounting information systems. Kevin is a CPA who has personally obtained many specialized technology-related certifications. He felt that the CITP would provide him with a competitive advantage. The CITP allows a practicing accountant to differentiate him or herself with respect to knowledge of IT. It is difficult to say how widely this will be received but it makes some sense to have a specialized “add on” to the CPA, which remains the most widely recognized and respected professional certification for accounting professionals.

1-7. How do IT audit guidelines, such as those issued by ISACA, help an IT auditor to do their work?

IT auditors need frameworks and guidance in order to make sure that they have reviewed information systems risks and controls sufficiently to have an opinion about them and to offer management suggestions. Risks and controls vary with different technologies. As a result, no one auditor can hope to have sufficient knowledge to recognize all the risks associated with each, nor can the IT auditor be knowledgeable about the controls or sets of controls best able to mitigate risks. Auditing standards help lend structure to IT audits.

1-8. ISACA recently made their standards, guidelines, and procedures "open." This means that they share them at no cost - anyone can download them from the ISACA web site. Discuss the value of such a strategy.

While a professional organization might wish to profit in some way by keeping standards private and charging for them, if the aim of a profession is to help develop and improve the profession, then open distribution of the standards is imperative. Open distribution will assure that a maximum number of IT audit professionals will have the benefit of these standards and guidance. It should serve to increase the quality of work that IT auditors do. Enhancing the professionalism of IT auditors in the long run will increase the stature of the professional organization to which they belong.

EXERCISES

1-9. In 2001, the Auditing Standards Board of the AICPA issued Statement on Auditing Standards No. 94 - *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit.* This standard is likely to increase the involvement of an IT auditor on a financial audit engagement. The standard requires auditors to consider how an organization's use of IT might affect internal controls. The standard explains that auditors may determine that it is more effective and efficient to assess control risk than to perform detailed testing of account balances and transactions (i.e., substantive testing).

Required:

Explain how SAS No. 94 is likely to impact the work of both the financial and IT auditor.

Both financial and IT auditors are likely to increase the amount of attention they pay to internal controls as a result of both SAS No. 94 and the Sarbanes Oxley Act of 2002. Since almost all AIS today are computerized, financial auditors are likely to rely more on IT auditors in their evaluation of internal controls, particularly application controls. In talking with some Big Four IT audit practitioners, it appears that IT auditors are increasing the time they spend on financial audit engagements. They're doing internal control evaluations up front in the engagements, and their work is increasing from about 5 to 10% of the engagement time and cost budget, to 20% or more.

1-10. Many large business, government, and not-for-profit organizations have adopted CobiT® as a framework for IT governance, including the U.S. House of Representatives. IT governance has two primary components: (1) acquisition and deployment of IT to promote an organization's objectives and enable business processes and (2) management and control of IT-related risks.

Required:

Assume that you have been asked to consult a Fortune 1000 business enterprise about implementing IT governance. Using the framework shown in Figure 1-1, identify an implementation plan with six or more specific activities you would recommend.

The ISACA web site has several examples and case studies of implementations using CobiT, e.g., implementation at Charles Schwab. The following is an example of how the IT governance framework might be used for a Fortune 1000 company.

1) The process begins with management setting objectives for IT. Specific activities might include, surveying competitive use of IT, analyzing the current organization's use of IT (maps and flowcharts would be useful here), inviting IT vendors to discuss new products on the horizon, and doing a high level IT risk assessment.

2) Management needs to compare where they want to be (strategic objectives) with where they currently are (current performance). This will require several meetings that will include some or all of these groups: IT management, internal audit, external auditors and consultants, the board, and general management.

3) The results of the comparison of objectives with current performance will lead to identification of specific IT activities. These activities might include: implementing an enterprise-wide software solution, adopting customer relationship management or other e-business software, creating a data warehouse, implementing a plan for systems reliability assurance, improving the return on investment for IT resources, creating a knowledge management system, or improving automation in business processes, such as manufacturing or procurement.