Stepping Through the IS Audit

Second Edition

PREFACE

Stepping Through the IS Audit speaks directly to Information Technology (IT) Professionals who are undergoing information systems (IS) audits.

ACKNOWLEDGEMENTS

A recurring theme of this book is that sharing of ideas with respect to control practices between Information Systems Auditors and Information Technology (IT) Professionals results not only in clean audits, but also in management control over IT. I owe this perspective to a combination of influences. These include the AT&T network operations experts whose reasoning I modeled as an expert system developer, the Information Systems Risk Management partners of Price Waterhouse - especially my coach, Mike Donahue, and the diligent Chief Financial Officers I have encountered over the years as information security officer, auditor, consultant, and practitioner. This second edition also attempts to incorporate the considerable information systems control experience and expertise of ISACA reviewers Michael Parkinson and Michael Hines. Their constructive review and perceptive insights enable this edition to answer the educational needs of an audience far removed from my range of experience.

1. Foundation

IS audit is an activity that can only be understood in the context of its root cause. The root cause of IS Audit is a concerned individual or group. The individual or group seeks assurance concerning some state of affairs. In general, those who seek such assurance are often also responsible for managing the given state of affairs. So this book about IS Audit begins by providing an overview of managment concerns with respect to information systems. This *Foundation* chapter also provides context for understanding audit activity in response to those concerns. It includes a brief history of the IS audit profession as well as an overview of types of IS audit services.

The remainder of the book concentrates on IS Audit activity itself. Audit activity is divided into two parts, planning and execution. These activities are in turn reduced to sub-activities. These are actual actions performed by auditors that, in sum, provide assurance that management concerns are addressed. A description of audit planning and execution is followed by a case study that ties these activities together with concrete examples and dialogue. For those interested only the the mechanics of the information systems audit process, both this Foundations chapter and the Case Study chapter may be skipped without loss of continuity.

Each chapter is divided into subsections that contain distinct lessons on the Information Systems Audit. As this book is targeted at an information systems professional seeking to understand the audit process, each subsection ends with some recommendations spoken directly to the auditee at the corresponding stage of the audit process. The overall content of *Stepping Through the IS Audit* is summarized in the figure below. You are about to take the first step.

1.1 Management Concerns

1.1.1 IT Governance

An audit is a process by which something is verified. The purpose of the audit is that the verifier be able to attest. Audits are commissioned because something needs to be verified. Auditors verify and attest to that which they verified. For the most part, auditors report on the way something is being handled, or *managed*. By that fact, auditors are checking up on management. So it is entirely appropriate for management to be concerned about the activities of auditors.

The managers that are concerned about a given audit may not always be the same as those who actually manage whatever is being examined or verified. Where that is the case, management is concerned with its own Governance process. Governance is the structure of relationships and processes used to plan, organize, staff, and control the organization in order to achieve goals. In the context of an audit, Governance is comprised of the frameworks and methods management has established for maintaining control over the thing being audited.

In the case of an Information Systems (IS) audit, management is concerned about computerized information systems. Management's concern may be the computers themselves as assets, the operational integrity, the data confidentiality, the assets controlled by the computers' software, or any combination of the above. These all reflect the quality of management's Information Technology (IT) Governance. IT Governance refers to the people and processes that govern IT. Those who manage these processes, IT Governors, are expected to maintain goals, policies, procedures, and practices to ensure that all IT managers:

- Align IT with the enterprise and realization of promised benefits
- Use IT to enable the enterprise by exploiting opportunities and maximizing benefits
- Responsibly manage IT resources
- Appropriately manage IT-related risks.[1]

When an IS audit is commissioned, the "auditee" is not the technology itself. The auditee is instead the IT manager delegated the responsibility for addressing concerns with respect to the technology. Note the distinction made between the IT Governor and the IT manager. The terms are used to clearly differentiate the person with ultimate decision-making authority on how IT is managed from the person who handles day-to- day management. It may be the same person, in the form of the Chief Information Officer (CIO), Chief Technology Officer (CTO), or other high level executives with the ultimate responsibility for systems operations.[2] In companies with very distributed leadership, it may be that any manager who has any aspect of IT Governance within his or her organization is by that fact also an IT Governor. By extension, this makes the ultimate IT Governor the highest ranking executive in the company.

Where audit reports identify technology control weaknesses, both the IT Governor and corresponding IT managers are expected to eliminate the weaknesses. If they do not, they can expect pressure to do so. In public companies, the pressure will usually come from the Audit Committee of the Board of Directors. The more familiar the Board of Directors becomes with the extent of the company's reliance on computer

---

1 Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, Rolling Meadows, IL, ISBN 1-893209-64-4 2003.

2 Though these titles may not be interchangeable at any given organization, the top IT executive will be hereafter generically referred to as the CIO.

systems, the more obvious it becomes that vulnerabilities seen in audit reports represent significant business risk. It is commonly acknowledged among IT Governors that it is helpful to the company when there is some IT experience at Board level to ensure that the analysis of individual audit results is tempered by an overall understanding of the technology issues. Where there is none, Board-level decisions on IT management issues are often based on audit results. This means that it is in the best interests of IT managers to ensure that the overall understanding of technology issues is reflected in the auditor's report. This book will focus on the audit process itself, and speak to the IT manager directly involved in, and directly responding to a given audit.

1.1.2 Chronology of Concerns

IT management precedes the advent of computers. During World War II, a group of scientists in Los Alamos, New Mexico, were assigned to build an atomic bomb. This required an extensive number of calculus calculations. The only calculating machines available could perform only arithmetic. The physicist Richard Feynman managed information technology by directing a roomful of people to perform separate arithmetic operations on mechanical machines.[3] Each person recorded the result of a calculation on an index card to feed to the next human calculator. Every error had to be isolated to a subset of the original set of cards. To recover from the error, a new set of color-coded cards was set into circulation in parallel to the first. The product of the new set would be fed into the first set at the point that would establish error recovery. Watching three different color-coded card sets being passed simultaneously around the room, Feynman was painfully conscious of the opportunity for human error to slip into the calculations. The design of the atomic bomb would be based on the results.

Early managers of automated computer systems were likewise acutely aware of the potential for system malfunction. The human potential for making technical mistakes has always been evident in computer operations, as well as development, acquisition and implementation. Software folklore provides numerous examples of development, acquisition and implementation decisions being made for monetary, political, criminal, and even personality reasons.[4] Even supposing that the human factor was eliminated from IT decisions, system malfunction can occur with no one to blame. Since one of the first actual bugs was discovered among the vacuum tubes in a computer system, IT management has been aware that a certain level of paranoia is justified.[5] In spite of the increasing sophistication in planning, delivery, support, and monitoring processes, IT managers have always recognized that even ideal organizational process flow can be foiled by unanticipated events.

Like any other management discipline, IT managers have explored the gamut of best practices, both trendy and timeless. They have won friends and influenced people, sought total quality management, gotten to *yes*, thrived on chaos, adopted seven habits, reengineered their processes, and measured down their defects.[6] In

---

3 Feynman, Richard, *Surely You're Joking, Mr. Feynman*, W.W. Norton & Company, 1985, p.126-132.

4 Glass, Robert L., "Software Folklore," *Computing Trends, 1990.*

5 Slater, Robert, *Portraits in Silicon*, the MIT Press, 1987, p.223.

6 These catch phrases come from the popular management handbooks: Carnegie, Dale, *How to Win Friends and Influence People*, Simon and Schuster, 1936, Walton, Mary, *The Deming Management Method*, Dodd, Mead, 1986, Fisher and Ury, *Getting to Yes*, Houghton Mifflin, 1981, Peters, Tom, *Thriving on Chaos*, Alfred A. Knopf, 1987, Covey, Stephen, *Seven Habits of Highly Effective People*, Simon and Schuster, 1990, Hammer and Champy, *Reengineering the Corporation*, HarperBusiness, 1993, and Pande, et al, *What is Six Sigma?*, McGraw-Hill, 2002.

addition, there have been several information-technology-specific management books that have been particularly influential on IT Governance.

For example, there is *The Mythical Man Month.*[7] *When computers moved from Feynman-variety mathematical calculations to business problem-solving, the divide-and-conquer approach became an art of reducing rote tasks to discrete programs where the output of one became the expected input of another. Success such as Feynman's in lining up human calculators had given IT managers the false impression that computer problem-solving was a linear process.* *The Mythical Man Month* showed that the amount of communication between project team members necessarily increased in proportion to the number of programmers working on the project. It pointed out that increasing the number of people assigned to create a computer program did not get it done proportionally faster, instead they spent a larger proportion of their time in communicating with each other.

Though it seems common sense today, in 1974 this was an unexpected revelation. Programs needed to be modularized so that individual contributors could be productive without all of them needing to learn every aspect of the complete system. The value of such structured programming had long been known to academia,[8] but had not till *The Mythical Man Month* been embraced by IT managers. Over the next decade, structured programming became the theme by which IT managers modeled their programs for software planning and acquisition.[9] Its basic tenants were echoed in the delivery and support processes for distributed systems, which at that time were seen as an extension of the program delivery process. IT management became the art of deploying and monitoring multiple concurrent and sequential processes across diverse platforms. Throughout the 1980s, and later fueled by the advent of object oriented programming in the 1990s, programs continued to become more modularized and distributed. IT Governance grew proportionally more challenging and complex.

Despite this growing management attention to technology controls in the 1980s, at that time, most technology control activity was focused heavily on financial systems. This changed in 1988, when an Internet worm caused performance problems on approximately 6,000 computers and $15 million in productivity loss.[10] The catastrophic nature of this event was significant because it predated the general public's reliance on the Internet service industry. It was in 1989 that Microsoft released its first Office Suite. It was in 1990 that the first version of hypertext-markup-language (html) brought Internet browsing to the general public. The threat of information corruption and theft from online sources motivated IT managers to implement a wide variety of controls aimed not just at protecting financial statement accuracy, but at restricting the ability of the general public to tamper with information delivery services.

Increasing awareness of Internet vulnerabilities prompted concern with respect to the storage and transfer of personal sensitive information. As more and more types of data with respect to individuals were kept in corporate computer systems, privacy advocates world-wide have lobbied their governments to keep this data secure. In the 1980s and early 1990s, several countries passed their own privacy and computer crime

---

7 Brooks, Frederick P., *The Mythical Man Month*, Addison-Wesley, 1975, Anniversary Edition, 1995.

8 See the 1960s papers of Edsgar Dijkstra on object and structure in programs, available from World Wide Web: <http://www.cs.utexas.edu/users/EWD>.

9 Yourdon, Edward, *How to Manage Structured Programming*, Prentice Hall, 1976. This was the first widely read book by Yourdan. It success prompted subsequent books on the same topic.

10 Littman, Jonathan, "Shockwave Rider," *PC Computing*, June 1990.

laws.11 Even so, throughout the 1990s, this corporate use of personal data increased. Personal data was bought and sold as a commodity in the advertising industry. Theft of individual personal data directly led to theft of identity itself, prevalently in the form of credit card fraud. These revelations led to a host of other personal privacy laws and corresponding data protection requirements.12 Organizational strategies emerged for protection of trade secrets and intellectual property as well as for personal information.

As IT management struggled to contain what seemed a rapidly expanding chaos,13 the 1990s brought an epistle of common sense: organizations that follow well-defined processes to produce and deploy computer programs have fewer errors in both programming and delivery than organizations that do not. This measure of software delivery capability, developed by the Software Engineering Institute in 1995, was referred to as the Capability Maturity Model (CMM).14 It instructed managers to:

- define processes
- determine how to tell if they are effective
- set them in motion
- evaluate the results

These principles were followed not just in the software development process. The management philosophy was also directly reflected in operation of software once it was developed or acquired. Throughout the 1990s, tools and techniques devised for monitoring individual modules within large-scale system support processes became increasingly sophisticated. Best practices continue to evolve around the notion that deployment, support, and monitoring of computer systems is modular and containable as long as well-defined processes are followed and those processes have measurable results.15

Measurable results are auditable results. Hence, most IT Governance methodologies use some form of audit as the primary method of determining compliance with one's own management procedures. Examples of simple but effective audit steps that IT management uses to determine compliance with its own procedures are:

---

11 Icove, David, et.al., *Computer Crime*, O'Reilly & Associates, Inc., 1995.

12 For example, the European Union Data Protection Directive and Privacy and Electronic Communications Directive; the United Kingdom Data Protection Act 1998; the Spanish, German, and Swedish Personal Data Acts; in the US: the Health Insurance Portability and Accountability Act of 1996; US Public Law 104-191; California Civil Code 1798; and the Gramm-Leach-Bliley Act of 1999, US Public Law 106-102.

13 See *The Chaos Report*, a 1994 publication of the Standish Group International, available from World Wide Web: <http://www.standishgroup.com>.

14 Paulk, Weber, Curtis, and Chrissis, *The Capability Maturity Model*, Addison-Wesley, 1995. For more information on Carnegie Mellon's Software Engineering Institute CMM project, see World Wide Web: <http://www.sei.cmu.edu/cmm/cmm.html>

15 The most comprehensive collection of these best practices is the IT Infrastructure Library, available from World Wide Web: <http://www.itil.org>.

- verifying expected system performance characteristics
- listing of overdue program deliveries
- comparing actual dollars spent to projected system deployment costs
- reviewing records of outstanding maintenance requests
- counting service disruptions and measuring their duration
- transactions are executed with management approval.

The 1990s also brought appreciation to one of the more poignant epistles of *The Mythical Man Month*, "The project manager's best friend is his daily adversary, the independent product-testing organization….In the last analysis, the customer is the independent Auditor. In the merciless light of real use, every flaw will show."16 IS Audit has become an integral part of IT management.

1.1.3 Internal Control Structures

By the end of the 1990s, all major companies and most small ones had converted their books and records and Generally Accepted Accounting Practices (GAAP) to computerized systems. Before the advent of computers, these books and records had only been verified in the course of a financial audit. It became obvious to those auditing financial statements that all legislation and regulation that applied to books and record keeping practices now applied to IT. For example, the Foreign Corrupt Practices Act (FCPA) requires companies whose shares trade on public exchanges in the U.S. to have methods to verify that their financial statements are accurately stated in compliance with GAAP or other authoritative source, and thus computerized system were by U.S. law a focus for the Audit Committee.17 The extent to which an Audit Committee has the ability to assure integrity in financial statements and other organizational objectives is the extent to which an organization has established "internal control." A organization's *internal control structure* (ICS) is the method by which operational and performance goals are achieved in an efficient and effective manner that is transparent to management.

Though usually described in the context of business or financial processes, the integrity of an ICS is often reflected in its technology operations. Consider that the ability to measure progress in organization goals often depends on the reliability of financial statements. View this consideration in the context of the role of IT in the production of financial statements. A financial statement audit will be designed to ensure that, if a lapse in internal control exists, it can be safely assumed to not significantly, or materially, affect the reliability of the financial statements. That is, a financial audit should provide assurance that the judgement of a reasonable person relying on the financial statement would not be changed or influenced by any financial misstatement not caught in the course of the audit. A misstatement is not necessarily a booking error like a simple error in a bank account balance. A misstatement could be in a revenue projection that relies on the continuous operation of a critical system. Materiality may be affected by failures of systems integrity due to lack of confidentiality, integrity, or availability. If an auditor does identify a gap in the ICS that materially affects financial statements, both the financial statements and the ICS should be changed before the auditor will attest to the adequacy of the financial statement generation process. Technology considerations are an integral part of most internal control structures.

---

16 Ibid, Brooks, p. 69.

17 Vanasco, Rocco, *The Audit Committee: An International Perspective*, The Institute of Internal Auditors Research Foundation (No. 893), 1995.

Throughout the advent of distributed systems, client server, and Internet access, Audit Committees have been hearing about technology control weaknesses and associated risks to the business. For example, some IT concerns may present a risk of inaccurate revenue projections. These may include:

- major systems initiatives show weak returns on investment
- over-reliance on fragile legacy systems or unstable open networks
- incomplete recovery plans for critical systems.

Others may present a risk of legal or regulatory violations. For example:

- white collar crime made easier by loose controls on computer security or
- lack of computer security on private personal related data.

In response to these and other concerns, the Audit Committee expects to see IT management implement "technology controls." The objective of a technology control is to prevent, detect, or correct undesired events in information systems processes.

In the late 1980s, a national committee was formed to involve corporate management in designing and developing ICSs, i.e., the Committee of Sponsoring Organizations of the Treadway Commission (COSO).18 In 1992, this private-sector task force published an influential guide to creating internal control processes, the COSO Framework.19 It emphasized five interrelated components of internal control: control environment, risk assessment, control activities, information/communication, and monitoring. Audit committees and public accounting firms almost immediately adopted it. The dominant theme of the COSO Framework is its representation of *control environment*, a long description of good management behavior that quickly became synonymous with the succinct phrase: *the tone is set at the top.*

IT Governors following a COSO-like management methodology will frequently use audit as a form of independent feedback. They will use this feedback to identify weaknesses in the internal control structure and correct them. To a casual observer, it may seem that IT organizations that are audited frequently have achieved more consistent implementation of these IT controls than those that are audited infrequently. But this is a constant correlation, not a causal one. Effective IT Governors did not earn their position by managing risk in response to IS Audits. They manage risk using a strong ICS and use audit as a tool to monitor their own objectives. A *tone at the top* emphasizing strong IT controls tends also to emphasize the necessity of audit.

1.1.4 To the Auditee:

Feynman's calculation activity was in support of the designers of the atomic bomb. Today's IT managers are supporting shareholders and investors. In both cases, there is significant pressure to make the IT Governance process work. The difference between Feynman's job and yours is that the level of complexity inherent in IT processes has grown exponentially over the intervening 60 years. The attention to IT controls has grown correspondingly. You are expected to support strategic plans, define policies, document

---

18 Members include: American Accounting Association, American Institute of Certified Public Accountants, Financial Executive Institute, Institute of Internal Auditors, Institute of Management Accountants, more information on the role of these organizations is available from World Wide Web: <http://www.coso.org>.

19 The Treadway Commission, *Internal Control, an Integrated Framework*, AICPA, 1992.

procedures, segregate job functions, schedule changes, measure performance, control costs, manage quality, and plan for disaster recovery in support of an ICS.

Though IS Audit has not traditionally been viewed as a contributor to IT quality assurance, it is one of many by-products of a push for quality on the executive management level. Where your architecture and productivity goals have been strategically aligned with the goals of the ICS, IS Audit control testing can provide you with some insight into whether the goals are being met. An internal auditor will have common goals and can help communicate struggles to senior management. An external auditor can be used as a sanity check on new controls, and for ideas on how other organizations have implemented controls similar to yours. To see how this is possible, you must understand the purpose of the audit, know the rules governing the process, participate in the audit process, and welcome the opportunity.

The rest of this book will lead you through the current practices of IS auditors to help you understand how this management assurance tool may be used to your advantage. It will introduce you to the IS Audit profession. It will describe the audit process in such a way that highlights the differing perspectives of auditors and IT Governors with respect to IS management control practices. The lessons which follow will enable you to take a proactive approach to ensure a positive outcome for an IS Audit.

1.2 The Audit Profession

1.2.1 History

In the same way that management tools and techniques have evolved over time, audit tools, techniques, and procedures have evolved. One significant difference is that trendy new tools for problem-solving are not as attractive to auditors as they can be to IT management. Because an auditor must always be in a position to attest to results, the time commitment required to completely understand how an IT components works before applying it is larger for an IS auditor than for a typical IT professional. Auditors thus tend to stick to tried and true audit techniques. The answer to the old joke, "Why did the X cross the road?," where X=Auditor is, "Because he crossed it last year."[20] Hence, to understand what is happening during an IS Audit, it helps to understand how the profession of audit has evolved over time.

Long before the term IT was coined, the computer field was generally known as Electronic Data Processing (EDP). Auditors were brought in to verify the integrity of company financial statements generated by a computer.[21] Most were volunteers from the ranks of financial audit and approached the "EDP Audit" in the same way as the financial audit. In performing a financial audit, an auditor would compare actual financial transactions to the summary version that appeared on financial statements. In the EDP, an auditor would collect batch data-entry sheets ("data in"), manually compute financial statements, then compare their version of the financial statements with those produced by the computer ("data out").

It soon became clear that even if the "data in" perfectly correlated to the "data out," there was still a material risk in computer usage. For example, it was typical to find that the accounts payable clerks were granted access to menus that allowed them to update vendor name and address records as well as print checks. This was not an issue before computerization because bank reconciliations were done using the handwritten paper checks as source transactions, and the handwriting part was performed by another department. Any error in the vendor name on the check would be caught when the checks came back from the bank to the reconciliation department. However, in the computerized environment, bank reconciliation was performed automatically using numeric data feeds from the bank. No one looked anymore at the return check. The new computerized process would not detect a change in the check recipient. It would not challenge a technically savvy criminal to simply change the name and address on a vendor record before a check was sent the printer, and after the check was printed, to change it back. Accounting managers might not question ten computer-generated checks to a reliable supplier. IT management thus became aware that material computer risks lay in a user's ability to escape detection through data manipulation. EDP Audits expanded to include data-entry procedures, access control, audit trail logging, and system support processes.

Unfortunately, only a small percentage of these and other types of unforeseen consequences of the conversion to computerization were caught. Many organizations in all industries experienced fiascoes due to poorly conceived and implemented systems.[22] The "data in/data out" method was soon condescendingly dismissed as "auditing *around* the computer." Auditors were encouraged to learn about

---

20 Powers, William, "*The Role of the IT Professional in Sarbanes-Oxley Compliance*," ISACA Sarbanes-Oxley IT Controls Symposium, April 2004.

21 For a history of the audit profession prior to the advent of EDP, see Flesher, Dale, "A History of Accounting and Auditing Before EDP," EDP Auditor's Journal, Volume III, 1993, pp. 38- 47.

22 Weiss, Harold, "Standing the Test of Time," EDP Auditor's Journal, Volume III, 1993, pp. 10- 13.

programming and computer operations so they could assess and potentially avert these disasters going forward. Yet despite the intense technical training, most financial auditors were not prepared for the challenge of validating technical access control mechanisms. Audit organizations were gradually forced to supplement their financial audit teams with technical staff members.

EDP Audit thus gained respect not just as a confirmation of financial system number-processing integrity, but in its own right as asset-protection insurance. EDP Audit became routine in large data processing organizations to ensure that organizations complied with laws and addressed security risks. Thus the introduction of *EDP Auditor* as a job title.

By 1968, practicing EDP Auditors were reverently aware of their role in verifying computerized records. They were hungry for tools and techniques with which to execute their charter. In that year, an entrepreneurial company called the Automation Training Institute held a conference specifically to address the special concerns of EDP Auditors, the Computer Audit, Control, and Security (CACS) Conference.[23] Some attendees joined with others similarly engaged to start the EDP Auditors Association (EDPAA) in 1969. The CACS conference became an annual event. By 1973, the demand for information sharing with respect to audit tools and techniques led the Automation Training Institute to supplement CACS with a monthly publication, the EDP Audit, Control, and Security Newsletter (EDPACS).

Increased activity within the profession of EDP Audit had become a major topic for the already well established Institute of Internal Auditors (IIA)[24], as well as many accounting firms. Established in 1941, the IIA was a recognized independent and reliable source of standards and guidance for audit professionals. In1977, it established a global committee of accounting firms, government entities, and virtually every professional organization involved in EDP Auditing to produced the *Systems Auditability and Control Report* (SAC).[25] SAC was a "how-to" document that laid out step by step what IS auditors should look for to mitigate risk. Later that year, the EDPAA complimented SAC with a primer called *Control Objectives*.[26] It defined *Control Objective* as *a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity*, and provided a comprehensive list of control objectives that address most situations encountered in the course of an IS Audit.

Both publications were immediately well received.[27] As a key contributor to one and the publisher of the other, the EDPAA assumed a leading role in the education and professional development of information systems control professionals. In 1978, the EDPAA introduced a certification to attract more qualified professionals to the field, the Certified Information Systems Auditors (CISA) designation. Approximately 3,000 EDP Audit professionals were awarded the designation of CISA in the first year of its existence, a number that has since grown exponentially.

EDP auditing has become a highly specialized skill that requires years of experience and training. CISAs must have a minimum of five years of IS auditing, control, and security work experience. They must pass a test that covers technical knowledge and deductive analysis on these topics:

---

23 op. cit.

24 See <http://www.theiia.org>.

25 Institute of Internal Auditors (IIA), *Systems Auditability and Control Report*, IIA, 1977.

26 EDP Auditors Association (EDPAA), *Control Objectives* (Handbook), EDPAA, 1977.

27 Singleton and Flesher, "The Evolution of EDP Auditing in North America," *IS Audit and Control Journal*, Volume IV, 1994, pp. 38-48.

- Management, Planning, and Organization of IS
- Technical Infrastructure and Operational Practices
- Protection of Information Assets
- Disaster Recovery and Business Continuity
- Business Application System Development, Acquisition, Implementation, and Maintenance
- Business Process Evaluation and Risk Management
- The IS Audit Process

The test is currently given annually in 11 languages, in 78 countries, at approximately 200 locations worldwide. Potential questions are vetted through several layers of experienced professionals. The test itself is held under lock and key until released as simultaneously as time zones allow to all takers on the day of the exam. In addition, a CISA must submit evidence of IS control experience, as well as continuing education annually in order to maintain certification. These requirements are designed to ensure that a CISA will continue to operate effectively, that is, to know enough about alternative control practices to be able to recognize whether or not a given control objective is met.

To keep up with the demand for continuing education, the EDPAA negotiated the purchase of the CACS in 1985, then the EDPACS newsletter in 1988, as the founders of the Automation Training Institute retired. The IIA committees continued to revise the SAC publication in the early 1990s. Recognizing that IT managers would need a framework with which to define controls that would pass audits using SAC-specified techniques, the EDP Auditor's Association revised its *Control Objectives* primer to speak more directly to IT Governors, subsequent revisions continue to produce a variety of publications under the heading *Control Objectives for Information Technology* (COBIT).28

By 1994, the EDPAA had about 15,000 members, more than half outside of the U.S. It had seen its first non- U.S. international president (a resident of Thailand). It continued to grow by an average of approximately 1,500 members per year, reaching approximately 30,000 at the time of this publication. With the advent of the Internet came auditor recognition that vulnerabilities in infrastructure itself were as significant as issues related to traditional data processing. The term EDP had become too narrow to fully describe the profession of IS audit. The EDPAA announced a name change to the *Information Systems Audit and Control Association* (ISACA). Professionals no longer referred to themselves as EDP Auditors but as IS Auditors.

---

28 *Control Objectives for Information and Related Technology Framework (COBIT),* Information Systems Audit and Control Association (ISACA), see World Wide Web: <http://www.isaca.org>.

1.2.2 Independent Outsiders

The opinion of an IS auditor has become valuable input to IT Governors largely because IS auditors usually (i) are information systems control experts and (ii) do not report to IT management. It is one thing for IT management to establish goals and demonstrate how they have met them. It is quite another for an independent outsider to take a list of established goals and *attest* that IT management has met them. Independent attestation is much more credible.

Thus, many large organizations maintain an *internal audit* department to verify and attest that managers meet their goals. Such organization should have a charter established and approved at the highest level of company management, for example, by the Board of Directors. The charter includes the purpose and responsibilities of the organization, which is normally covers the organization's whole ICS. It normally also includes provisions for a reporting structure for internal auditors that guarantees independence in attitude and appearance from any potential auditee.

When an audit is performed by a completely different corporate entity, it is referred to as *external audit*. The term "external auditor" normally refers to a firm hired to perform an attestation as to the validity of published financial statements and overall ICS. However, there are many other type of external attestation services. The charter of an external audit will normally be created by a contract sometimes referred to as an "engagement letter." The document will outline the scope and intent of the engagement. It will includes the expected services, deliverables, and terms of payment. As the scope is the subject of contractual negotiation and not organizational mission, the fact that an external audit was performed and the audit report showed no control weakness does not necessarily mean the auditee's ICS is reasonably sound. The engagement letter may describe an attestation services that does not cover all aspects of an organization that could result in material deficiencies.

The *internal auditor* versus *external auditor* versus *consultant* distinction has been a recurring theme in the history of the audit profession, and is repeatedly examined in the context of debates concerning *auditor independence*. In 1989, the ISACA members agreed that it made sense to come together on Information Systems Auditing Standards for professional practice.29 Yet even with the consensus that the independence issue must be uniformly addressed, this was by no means an easy task. Though some standards, such as those on *Illegal Acts*, gained ready acceptance, vigorous debates ensued on the topic of *Auditor Independence*.30

The most conscientious Audit Committees had by then established an *internal audit* department, and had required that a company's head of internal audit report directly to the Audit Committee without fear of management reprisal. This gave internal auditors freedom to give unqualified opinions on executive management. But internal auditors still were employees of the firm to which they belonged. Many internal auditors considered themselves to be surrogates of the Board of Directors, seeing nothing inconsistent about consulting on operational processes, or even dictating them. Others saw their roles as independent outsiders by necessity, where even a consulting role in a process would affect their ability to produce an unbiased assessment of it. The standards then adopted continue to be refined, but it is generally agreed that there is a core distinction between an IT controls professional that works directly for a manager in charge of control implementation and an independent or objective auditor that audits or advises the same manager. The former is more appropriately called a IT risk manager than an auditor.

---

29 See World Wide Web: <http://www.isaca.org> for current standards for Information Systems Control Professionals.

30 Ibid. Singleton, and also Weiss.

Audit professional practice standards acknowledge that close working relationships between IT staff and IS auditors have a positive effect on implemented controls. However, they also maintain that these close working relationships must not include management responsibility or otherwise interfere with impartiality.[31] Just as an arbitration judge must step down from a case in which he or she has a business relationship with one of the litigants, an auditor is obliged to disclose potential conflicts of interest and be prepared to step down from an audit in which he or she has responsibility for any aspect of the system under review. Though some internal audit organizations have been pursuing partnerships with IT management, a professional auditor is still an independent outsider. Auditors are independent in that their organizational reporting chain of command does not merge with those they audit. They are outsiders in that they are not responsible for maintaining any aspect of the processes that they audit. As a condition for maintaining certification, a CISA must adhere to the current standards for objectivity, due diligence, and professional care in accordance with professional standards.[32]

1.2.2.1 External Audit and Scope

It is of course difficult for an independent outsider to come into a modern technology environment of any significant proportion and fully understand where all the risks may be. This is why *scope* is so important. Scope is a technical term in audit that refers to the business purpose of the review. Without a well-defined scope, an IS audit would at best be an after-the-fact confirmation that IT processes seem to be working. At worst, it would be a too-late indication that earlier decisions on the part of IT management may not have been the best. With a well-defined scope (along with a well-timed review), there is some room for the auditors to proffer their experience with IT controls to actually assess the impact to the business of a control environment surrounding a specified IT or business process.

An external audit for a typical US corporation provides a good example of how the term scope is used. In these engagements, the external audit firm's charter is to attest that financial statement are accurate and in compliance with GAAP. The external audit firm will assign a statutory auditor[33] to accept responsibility for the overall audit engagement. Once that responsibility is accepted, the scope of that statutory auditor's assignment is to detect material misstatements in the financial statements. He or she is called the *Lead,* and will, at the end of the review, affix his or her signature to the report that attests that the financial statements are correct. Generally Accepted Auditing Standards (GAAS) require that the Lead allocate sufficient staff and resources to achieve assurance that the judgement of a reasonable person would not be influenced by any financial misstatement not caught in the course of the audit.[34] To accomplish this staff allocation for a large corporation, the Lead may break the audit down into a series of smaller projects, and provide each with its own scope.

---

31 See World Wide Web: <http://www.theiia.org> for professional practice standards for internal auditors versus consultants.

32 See World Wide Web: <http:// www.isaca.org> for the CISA Code of Professional Ethics.

33 *Statutory auditor* is a generic term used to describe a person licensed in a given environment to perform independent audits. A more correct term for a given country may be *Certified Public Accountant (CPA), Chartered Accountant,* or *Independent Auditor.*

34 American Institute of Certified Public Accountants (AICPA) Auditing Standards Board (ASB), *AICPA Professional Standards,* AICPA, June 2003. These standards govern the conduct of external audits conducted by CPAs.

For example, if the audit is for a company with three subdivisions individually represented in financial statements, the lead statutory auditor may assign other statutory auditor to audit each subdivision and work with them to consolidate the results into an overall assessment of the parent company's financials. Each assignee may in turn create assignments of a smaller scope. It is through this process that IS Audits are done in support of Financial Statement Audits. At some point, as the delegation progresses, an individual computer system will be identified as the source of information upon which the financial statements are heavily dependent. The statutory auditor whose scope includes the system may have gotten the system name while interviewing the company's Chief Accountant.35 An audit of that system will be assigned to an IS auditor. The system itself becomes the IS audit scope.

That is a good example of how scope is decided for a typical IS Audit. Minor scope adjustments are expected to arise, and in most cases, are made throughout the duration of an audit. *Scope creep* is a technical term that refers to the tendency of previously unidentified components of the IT environment making their way into an IS Audit scope. It is the responsibility of those who identify the original scope and assign resources to ensure that scope creep does not spread the assigned resources so thin that the quality of the overall engagement suffers.

To see how this works in the context of the previous example, suppose that the Chief Accountant tells the statutory auditor that the asset calculations in the financial statements have their origin in a specific system; call it FINSYS. To assign resources adequate to detect a material misstatement of finances, the statutory auditor would have to gain enough information about the technology comprising FINSYS to assign an auditor with the right skill set. The statutory auditor might ask the Chief Accountant to identify the hardware and software that runs FINSYS. Suppose that the Chief Accountant tells the statutory auditor that FINSYS is an Oracle-based application running under UNIX.

Suppose further that the statutory auditor must select an IS auditor from a resource pool of that includes former IT administrators, programmers, or engineers from a variety of technical environments. The assignment of resources must leave the Lead fully confident that unimpeachable independent testing and evaluation is performed on the full scope of the FINSYS audit. An auditor who has direct experience in UNIX and Oracle would be chosen for the job. Yet as is often the case, upon arrival, the auditor might find that FINSYS is not performing all asset calculations at the firm, but that another system called ASCALC calculates assets for a small business unit and that business unit uses FINSYS merely as a pass-through mechanism to feed the general ledger. Suppose that ASCALC runs on NT. As the scope of the statutory auditor's the point of view is not defined as the FINSYS, but as asset calculations, the IS auditor reports the existence of ASCALC to the statutory auditor. The statutory auditor analyzes the financial statements of the business unit that provides asset data from ASCALC, decides that ASCALC should be part of the systems review. The NT system would then come in scope. The scope from the point of the of the statutory auditor remains the same, but scope creep has occurred in the context of the IS audit and a minor adjustment in the audit plan would be required.

One way this example might play out is to proceed with the assumption that the FINSYS auditor knows enough about controls and systems in general to identify a "best practice" document that covers the NT environment. The auditor uses that document to perform a basic NT audit using step-by-step instructions. Results are recorded in *workpapers*, a technical term in audit referring to an organized set of papers, or evidence, collected in the course of doing the work. The auditor's findings are detailed and thorough for the UNIX and Oracle systems, but academic for the NT component. Recognizing the risk of inadequate staffing, the statutory auditor responsible for the scope definition then makes the auditor's workpapers available to a more experienced NT auditor, who accepts those results because (i) the controls were

---

35 *Chief Accountant* is a generic term used to describe a person that has primary responsibility for the production of an organization's financial statements. A more correct term for a given country may be *Chief Financial Officer or Comptroller.*

adequately reviewed and (ii) because of the low risk associated with the NT component. On the basis of the completeness of the workpapers and the independent peer review, the Lead statutory auditor may sign the consolidated audit report.

1.2.2.2. Other Attestation Services

The scope in a normal external IS Audit must be flexible enough to serve the overall goal of financial statement and ICS verification. But there are many audit-like attestation services that are not subject to scope creep. For example, the first non-audit-variety IT attestation services were performed in the 1970s. Companies that marketed accounting software began to contract EDP Audits from reputable accounting firms. The accounting firms performed "data in/data out" audits on the contracting company's software. This saved customers the expense of an individual IS audit. Moreover, if the software passed the audit, the company could use the accountant's seal of approval in its advertising.

This two-pronged motivation for attestation services, assurance and advertisement, has led to a wide variety of attestation services as marketing tools. The growth of IT outsourcing and Application Service Providers is fueling the fire for attestation services. Like the accounting software firms of the late 1970s, many information services companies contract independent technology audits of themselves. A successful audit is a positive advertising statement. It also saves the time their own staff would have to spend if all of their customers sent separate teams of auditors to their site. At one end of the spectrum of these services is independent control testing; at the other, plain consulting.

1.2.2.3 Independent Control Testing

Where a company outsources a materially significant transaction processing function like benefits or payroll, it requires assurance that the service provider is fully capable of processing transactions. Independent control testing can provide assurance that the processing of the transactions is controlled to the extent that the service provider asserts. An auditor is presented with a document describing the service provider's control objectives and associated control practices. This is not necessarily the entire company ICS, but the subset of it that provides the specific service under review. The auditor will review and test controls that correspond to the stated control objectives. The audit report will reflect whether the controls are adequate to achieve the control objectives, whether they have been implemented, and if their implementation meets control objectives. This type of independent control testing is a common component of verification of controls in a wide variety of outsourced IT operations, from insurance processors to internet service providers. However, avid readers of these reports on service providers include not only service processing clients, but shareholders, vendors, business partners, and investment analysts.

One example of this type of attestation is based on the AICPA's Statement on Auditing Standards No. 70 (SAS 70).36 These guidelines were specifically developed to provide guidance to auditors of companies that outsource transaction processing to IT service providers. As such, SAS 70 provides a convenient illustration of the distinction between control objectives in themselves, their implementation by management, and the auditor's testing of them. There are two types of audits described in the SAS 70 guideline: (i) an audit of the financial statements of the user of the service and (ii) and audit of the services provided. The SAS 70 service provider attestations are directed at the second type, that is, the activities of the service organization and the service auditor. Within this second type of audit, the service organization audit, there are two subtypes: (i) an assessment of management-identified controls and (ii) an assessment of management-identified controls plus tests of these controls. The two subtypes of a SAS 70 service organization audit are colloquially referred to by IS auditors as SAS70-Type-1 or SAS70-Type-2 audits.

---

36 See AICPA Auditing Practice Release No. 021056: Implementing SAS No.#70 Reports on the Processing of Transactions by Service Organizations.

In both types of SAS 70 service organization audits, the service auditor is presented with a document describing management's control objectives and associated control practices. This is not necessarily the entire company ICS, but the subset of it that provides the specific service under review. The auditor will review controls with respect to the control objectives. In a SAS70-Type-1 audit, the audit report will reflect whether the controls are adequate to achieve the control objectives and whether they have been implemented. In a SAS70-Type-2 audit, the audit report will in addition *identify weaknesses in control implementation*. The SAS70-Type-2 audit clearly provides more valuable information than the SAS70-Type-1. But neither type of SAS 70 provides independent verification that the control objectives themselves are appropriate for the processing environment.

This omission and lack of scrutiny on scope is common to all attestation services where the customer provides the list of things to test. Independent control testing projects are defined by IT management to highlight a specific aspect of the control structure they have put in place. The extent to which their audit reports can be trusted by clients, shareholders, vendors, business partners, and investment analysts interested in the company is the extent to which those performing the work are objective in its performance. Questions one may ask to determine the extent of an auditor's objectivity are:

- Reporting hierarchy - does the auditor report to a person that is responsible for maintaining the controls being audited?

- Financial independence - does the auditor's salary or fee in any way depend on the favorable opinion of a person that is responsible for maintaining the controls being audited?

- Participation in system design - does the auditor work for an organization that helped design or implement controls that are under review, or did the auditor participate in these activities?

Where these questions are answered negatively, those assigned to the project may be more appropriately called *assessors*, a term used to distinguish them from auditors, as the work is not covered by the standards of professional practice that apply to auditors.37

1.2.2.4 Consulting Services

Where IT attestation services are not based on independently defined professional practices for those who will attest, they fall into the general category of information system risk management consulting. Assessors determine whether IT management has actually implemented the control structure as described in the scope of the project's statement of work. The statement of work may refer to a document written by management, an assessment methodology developed by the consulting firm, or a "best practice" document published by a third party. Depending on the agreement between the consultant and the organization, the report produced by the assessor may or may not include all control weaknesses uncovered in the course of the review.

Consulting attestation services and the reports produced by them are thus wholly controlled by the IT manager or the IT Governor that commissioned the review. Thus, the common caveat with respect to attestation services is that controls can be modeled on best practices but the fact that they meet the requirements of the review never means that they will thereby meet the control objectives specified in any given audit, even in the same domain. For example, there is a popular IT security standard that specifies a set of IS processes that should be in place to achieve security.38 There are many consulting standards that

---

37 For example of these standards, see World Wide Web: <http://www.isaca.org>, <http://www.theiia.org>, <http://www.aicpa.org>.

38 ISO/IEC 17799:2000, or BS 7799-2:2002, available from World Wide Web: <http://www.iso.org>.

follow a specific methodology in assessing compliance with that standards. Given those methods, an IT organization can staff and execute every process prescribed by the IT security standard and be certified as fully compliant with it without actually having chosen the correct systems configuration that would protect its data. An ICS auditor, by contrast, will take standard compliance into consideration, and even cite the standard as a reference for how a system should be managed, but even full standard compliance will not guarantee that an organization will pass an ICS audit. To pass an ICS audit, the organization must in addition show that the organization meets all the control objectives that management defined as its purpose for complying with the standard.

Thus, in order to make best use of attestation services, an IT Governor should have control over scope and direct access to the assessor's findings. In addition, a healthy skepticism may be called for in areas where attestation is performed without reference to best practices. For example, in the domain of IT security, several IT consulting services provide "penetration studies." These are attempts to break security controls that IT management has put in place. Penetration study reports are often offered as attestations that control objectives are met. Many application service providers hand them out in lieu of Independent Control Testing Reports. An IT Governor should be wary of the claims that systems cannot be penetrated when the reports neither identify the controls management has put in place nor the methodology used to maintain the control environment. The scope of the review will often have been limited to a set of systems that management is confident it protects, and the scope may have been changed in mid-review.

In contrast, an auditor is held, but rarely limited, to the predetermined scope of the current audit. For example, even in the case of an external audit where the scope is a specific regulatory requirement in the domain of privacy, if the auditor stumbles upon a financial misstatement, he or she will not look the other way. In the case of internal audit, if the auditor sees a potential for control weakness in a previously unidentified risk area, a new audit scope may be created on the spot.

1.2.3 To the Auditee:

The professional practice of information systems audit has a history as rich as the practice of information technology itself. The auditor who shows up at your door may know nothing about your operations and little about your technology, and the approach he or she takes in discerning them may be very different than what you would expect. But there is always a purpose and method to the approach. By the time an IT manager gets an email, letter, or phone call from an auditor, the audit process is well underway, complete with a defined objective and scope.

If your ICS is supported by well-understood policies and procedures, you will have little trouble identifying those that correspond to the audit, as well as assimilating any additional controls recommended in the course of the audit. Nonetheless, there may be audit recommendations that you will need to research before you can to devise a plan to implement. Although IS auditors are knowledgeable and can provide insight into IT control practices, the IS audit is not an IT consulting assignment. Audits do not increase the integrity level of an IT operation. That can be done only by the IT organization itself. The audit is an independent examination with reference to industry standards. It is a management-monitoring tool.

1.3 External Influences

1.3.1 Regulatory Environment

Most IT managers are content to leave regulatory compliance worries to their legal and finance departments, but in many industries, this is simply no longer possible. More and more regulatory agencies are interested in safeguarding data, completeness in accounting for transactions, and accurate results in calculations. Therefore, regulatory compliance audits often include technology control reviews. Moreover, regulatory agencies often are armed with enforcement divisions that have their own professional audit staff and their own sets of audit procedures. IT management is host not only to their own company's internal and external auditors, and their IT Governor's risk management consultants, but also to audit organizations from a variety of regulatory agencies, depending on the organization's regulatory environment.

Regulatory environment refers to the set of regulatory agencies that have jurisdiction over a given set of organizations. A *regulatory requirement* is a rule established by a regulatory agency which must be followed by organizations defined to be in its scope. *Regulatory compliance* refers to an organizational operation that meets all applicable regulatory requirements. When the scope of an audit is a regulation, the audit is called a compliance audit. But auditors will also use the term *compliance* in a completely different context that may be confusing to those who hear it for the first time. Note that *compliant* is not a state in itself, but only a state achieved with respect to something else. Auditors will use the term compliance audit colloquially to refer to any audit wherein the majority of audit tests are tests for compliance with the organization's ICS.

1.3.1.1 Compliance versus Substantive Testing

A comprehensive and properly documented ICS allows an IS auditor to quickly assess whether a given IT process meets a stated objective. That is because a comprehensive ICS will detail which processes and procedures are designed to meet objectives and these will map to the associated systems that are operated in compliance with the overall ICS. In any type of audit, an IS auditor's task is simplified if IT managers have already determined that their own ICS is compliant with control objectives established by the audit scope. They may achieve this demonstration by outlining the set of control practices within the ICS that pertains to the control objectives. If these control practices are listed in a policy document, an auditor may simply review the document for adequacy in meeting the objective, then design tests that demonstrate that the policy is followed. This is called a *compliance testing*. Compliance is modified not by the control objective itself, but by the *procedures predetermined to meet the control objective*. A *compliance test* verifies whether a process is followed.

For example, assume that a regulation requires that access to a certain kind of data should be limited to only those employees whose job function requires access. To complete a compliance test, an auditor may:

- observe that management has a policy in place that covers the regulatory requirement, and assess whether the regulatory requirement would be met if the policy were followed;
- ask IT management how the policy is followed, and assess whether the underlying control practices address risks of non-compliance;
- examine the integrity of the processes that comprise the control practices identified by the IT manager; and
- view the system processing logs and other evidence of the control practices to verify that the processes are indeed followed.

Where the organization does not have its regulatory compliance strategy documented, or the documented policy is not judged adequate to mitigate known risks, an auditor will be forced instead to perform a *substantive* test. A substantive test will disregard management controls and instead check for underlying evidence that a regulation had been followed. To contrast the substantive test with the compliance test of the previous example, assume that some regulation requires that only those employees whose job function requires access should have access to view a certain kind of data. To complete a substantive audit, the auditor may:

- review all job functions at the organization and determine which require access to the data;
- identify where the data was created or otherwise introduced into the firm, follow the systems processing stream through to where it was archived, transmitted, or otherwise stored;
- based on the data flow analysis, yield a list of systems which potentially could be used to grant access to the data;
- identify all input/output capabilities for all systems of the list and verify that they are all protected according to the minimum required for system operation;
- list the users of the systems on the list and cross reference the users lists with the job function list created in the first step.

Note that the use of the word *compliance* in reference to audit testing is not the same as its use in the term *regulatory compliance*. Both *compliance testing* and *substantive testing* may demonstrate *regulatory compliance*. The former demonstrates regulatory compliance in the course of demonstrating compliance with its own ICS. The latter demonstrates regulatory compliance by direct and substantive verification. Compliance testing places much more emphasis on reviewing the process by which IT management mapped a control objective onto an existing ICS. Substantive testing relies on the auditor to do that mapping.

For certain legal or regulatory requirements, substantive tests cannot be avoided. They sometimes serve to identify errors or omissions in policies or procedures. If the substantive test does reveal a previously unknown vulnerability, the IT organization that already has an effective ICS in place will more easily rise to the challenge and eliminate the vulnerability. The compliance versus substantive distinction is of the utmost importance in the case of a regulatory compliance audit because compliance with any individual regulation can be achieved in a myriad of ways. If a substantive audit reveals that a chosen compliance strategy is faulty, it can certainly be changed. That change is without risk to the business because the control objectives of the process are invariable.

Typical types of common compliance audits are listed below. They are listed alphabetically and include a brief description of the regulation. Frankly, any catalog of regulatory audits that affect IT is bound to be immediately outdated. Nevertheless, the following list serves to give an idea of the types of regulatory requirements that have surfaced and their impact on the IT community.

1.3.1.2 Anti-Terror

As the 21st century brings increasing focus on terrorist threats, there have recently been literally hundreds of anti-terrorist regulations world-wide.39 A major focus of anti-terrorism regulation is to limit the ability of criminals to use financial services. To this end, several international Financial Anti-Terrorism Task Forces have been established in order to ensure that all countries adopt legislation to counter the use of financial systems by criminals.40 IT management must be concerned with these regulations because many of them require financial institutions to implement anti-money-laundering processes. These practices have been folded into existing information systems that process certain types of financial transactions. Every transaction that meets certain criteria may be examined for compliance.

Another type of anti-terrorism legislation that affects IT are those emphasizing information sharing as a tool of law enforcement. For example, the U.S. Department of Homeland Security has established Information Sharing and Analysis Centers (ISACs) in many industry sectors.41 These organizations are meant to organize industries into cohesive national assets that allow critical infrastructure within the U.S. to operate throughout national crisis. While is it is not yet a regulatory requirement to participate, U.S. companies are under increasing pressure to share the burden of national security by contributing to these efforts, and this means adopting control objectives with respect to incident detection and response with management teams in other organizations. Other countries may be expected to have similar requirements.42

1.3.1.4 Data Protection

Legislation addressing individual privacy concerns dates back to the early 1970s, when the concerns over personal data in computer systems first became a topic for international media and prompted computer privacy laws.43 The concern has grown more widespread as information is more easily accessible. More recently, the European Union Data Protection Directive has provided a broad set of criteria for the legitimate use of personal information.44 It describes the types of data that may be collected relative to the purpose of the collection, accountability for use of the data, and rights of the data subject. It imposes conditions on personal data storage, processing, and transfer. Of particular concern to IT management are

---

39 For examples, see the anti-terrorist activity reports of various countries to the United Nations Security Council, available from World Wide Web: <http://www.un.org>.

40 See the Financial Anti-Terrorism Task Force web page, currently hosted by the Organization for Economic Cooperation and Development at World Wide Web: <http://www1.oecd.org/fatf/ index.htm>.

41 Industries where ISACs are currently active are: Chemical Industry, Electric Power, Energy(Oil & gas), Financial Services, Food Industry, Information, Technology, Public Health, Research and Education Network, Real Estate, Surface Transportation, Telecommunications, Water, more information on the ISACs is available from World Wide Web: <http:// www.dhs.gov>.

42 See, for example, Canada's Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) and Australia's Critical Infrastructure Advisory Council (CIAC).

43 For example, the Privacy Act of 1974, US Public Law 93-579.

44 European Parliament and the Council of 24, "Directive 94/46/EC," *Official Journal of the European Communities*, No L. 281, 1995, p. 31.

the provisions establishing the legal responsibility of the person who controls or processes the data. The Directive imposes requirements on its member states to make it a crime to violate confidentiality and security with respect to personal data processing.

The EU Privacy Directive is notable for its widespread reach as well as its status as a standard on which future laws in other countries may be expected to be based. It shares this influence with the U.S. Gramm-Leach-Bliley Act of 1999 (GLBA), which provides protection for personal financial information.45 GLBA requires banks, securities firms, and insurance companies to secure personal financial information, advise customers of their policies with respect to sharing the information, and to provide procedures for customers to "opt-out" of processes that share their personal data unless they are necessary to provide expected financial services to the customer. In 2001, a group of U.S. banking regulators adopted interagency guidelines that further outlined compliance with GLBA in their own domain. The domains of those institutions are global. These guidelines require any regulated financial institution to, among other things, implement an information security program to safeguard personal data.46

A similarly influential regulation in the domain of personal medical information is the Health Insurance Portability and Accountability Act of 1996 (HIPPA). HIPPA requires the U.S. Department of Health and Human Services (HHS) to address the security of personal health information.47 The HHS responded with the HIPPA Security Rule.48 The rule requires health-care providers to establish information security programs within their IT organizations. It specifies administrative, physical and technical standards in the form of specifications for safeguarding personal health information. Regulated entities must either address each specification as documented, or demonstrate why they do not apply to the organization.

1.3.1.5 Internal Control

Although an ICS is primarily a tool for organization's management to run its own operations, the integrity and stability of an ICS is becoming increasingly important to external stakeholders like customers, business partners, and governments. In the 1990s, failures in internal control not only put several public companies in bankruptcy, but also forced a world-wide public accounting firm out of business.49 Executives, bankers, and auditors were charged with money-laundering, securities fraud, wire fraud, mail fraud, and conspiring to inflate profit and obstruct justice. The negative consequences for stakeholders prompted a variety of legislation aimed at making regulated entities accountable for maintaining operational integrity in a manner transparent to regulators. The two most influential of these regulations are known as Basel and SOX. Basel refers to directives of the Basel Committee on Banking Supervision, a committee of central-bank

---

45 Gramm-Leach-Bliley Act of 1999, US Public Law 106-102.

46 Interagency Guidelines Establishing Standards For Safeguarding Customer Information, *Federal Register*, Vol. 66, No. 8615, Feb. 1, 2001. The regulators participating in the interagency guidelines are the Office of the Comptroller of the Currency, Office of Thrift Supervision, Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation.

47 Health Insurance Portability and Accountability Act of 1996; US Public Law 104-191.

48 US Department of Health and Human Services Security Rule, *Federal Register*, Vol. 68, No. 8334, February 20, 2003.

49 Berenson, Alex, *The Number, How the Drive for Quarterly Earnings Corrupted Wall Street and Corporate America*, Random House, 2003.

governors.50 SOX is shorthand for a legislative quest for an elimination of material deficiencies in financial statements by two U.S. Senators, Paul Sarbanes and Michael Oxley.51

In the case of Basel, the scope of the internal control requirement is the entire operational integrity of the regulated organization. Several of its directives are targeted at ensuring that regulated entities have a sound strategy for closely aligning IT requirements with risk management practices. These directives require IT Governors to closely align their ICSs with their risk management strategies as well as their financial statement support. Moreover, these risk management strategies are viewed as applicable world-wide.52

SOX introduced a requirement for ICS transparency as part of the process for responding to Securities and Exchange Commission (SEC) compliance audits.53 SOX applies to IT controls insofar as corporate management relies on IT to produce financials or track material components of the financials. ICS dependency on computerized financial statement generating processes must be visible and verifiable to its auditors. Management must document their control objectives and show audit how they comply with them. SOX further requires that auditors of publicly-held companies be registered as such, and in the registration process, provide evidence that the auditor assignments are appropriate and the audit results have peer review. As with BASEL, the trend in this type of regulation is toward worldwide standardization.

1.3.2 Best Practices

Attestation consultants often present standards as a means of guaranteeing regulatory compliance. This is true only if IT can effectively map the standard onto actual control objectives that are required for operating in compliance with the regulation. For example, the auditor in our scope example was able to perform an NT audit because the control objective was clear and there were step-by-step instructions available to follow. NT is a common technology and therefore an auditor has many "best practice" documents to choose from. Yet mapping from control objectives to best practice technology controls requires familiarity with control theory, something the auditor in our example was experienced enough to do. This section will describe what best practices are and how they can be useful in meeting control objectives.

Because technology review areas are expanding and changing at a rapid pace, it is often the case that auditors face technology for which no instructions are readily available. In this case, auditors often need to have some experience in the uses of the technology before they can identify the potential for risk. For example, before the advent of relational databases, IS auditors were sometimes comfortable auditing database applications by testing access controls only at the operating system level and/or application user-interface screens. Auditors with some experience in relational databases have since raised awareness that auditing an application without also testing controls at the database level can be as ineffectual "auditing around the computer" is now known to be. In this manner, new areas of best practice are born.

---

50 Basel Directives No. 82, *Risk Management Principles for Electronic Banking*, 2001, No. 86, *Sound Practices for the Management and Supervision of Operational Risk*, 2001, No. 91, *Risk Management Principles for Electronic Banking, 2002*. More information on Basel directives is available from World Wide Web: <http:// www.bis.org>.

51 Public Company Accounting and Investor Protection Act of 2002, US Public Law 107-204.

52 The Basel Committee on Banking Supervision, *Overview of the New Basel Capital Accord*, Consultative Document Issued for Comment July 31, 2003, p.2.

53 Public Company Accounting and Investor Protection Act of 2002, US Public Law 107-204, Section 404.

Best practices publications run the gamut of focus and format. Auditors are not the only audience for best practice. Whenever a new technology management issue arises, one of the first questions IT managers at all levels seem to have is, "*How do other people deal with this?*" Thus, best practices have spawned a full range of consulting activities and publications. They are usually published in checklist or tabular format so that an implementor or auditor can easily implement or check for compliance, respectively. However, it is sometimes hard to figure out how to implement, much less verify, the contents of the lists. This is because the lists can be written as different types of items, which include but are not limited to:

- Control Objectives Statements of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.
- Control Practices Key control procedures that support the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business.
- Policies Technology agnostic specifications for system configuration or personnel behavior to ensure a management requirement is met.
- Standards Technology specific specifications for systems configuration to meet a control requirement.

Different standards publications focus on one or more of these types of items. Here is a sample, starting at the most comprehensive in scope, followed by those whose scope narrows into specific technology domains:

- COBIT Control Objectives for Information Technology lists control objectives, and for each control objective, a list of control practices.54
- ITIL The IT Infrastructure Library is a set of documents covering different aspects of IT planning, delivery, and support. It lists control practices for the various domains.55
- SANS The SysAdmin, Audit, Network, Security Institute identifies issues that present problems for system administrators, and lists policies that will help address them.56
- BS7799 This British Standard, and a corresponding International Standards Organization Security document, lists control practices in the domain of IT Security, followed by an appendix listing security-related control objectives, and for each control objective, a list of control practices.57

---

54 IT Governance Institute, *Control Objectives*, one of the many COBIT documents available from World Wide Web: <http://www.isaca.org>

55 More information on ITIL available from World Wide Web: <http://www.itil.org>

56 More information on SANS available from World Wide Web: <http://www.sans.org>

57 See BS 7799-2:2002 and ISO/IEC 17799:2000. More information available from World Wide Web: <http://www.iso.org>

- CIS The Center for Internet Security (CIS) selects popular operating systems and lists configuration variables with associated standard IT security requirements.[58]

While all of these types of best practices are valuable in helping an IT organization to design controls, none actually specify controls as audit defines them. From the point of view of audit, controls are very specific policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. While best practices may have similar methods of documenting the relationship between controls and control objectives, none prescribe the exact controls that are in place at a given organization. Even those that specify what variables on operating systems should be set in a given way do not also specify how access to set the operating system variables should be controlled. Controls in themselves are by definition specific to an organization. The description of an actual control will refer to real department names and document locations within an organization.

Though it is possible to map most technology requirements of the ICS to some aspect of best practices, most technology is not standard enough in itself to allow well defined audit and control requirements that completely address all possible configurations. As companies tend to use the same technology in different ways, as well as keep data in different formats and schemas, a single technology best practice will always have exceptions. That is, there will be alternative practices to those it proscribes that still meet basic audit and control requirements. Where IT management has set its own standard, the only constraint on the method of configuring a given technology is that it serve the business purpose while maintaining the ICS.

Nonetheless, the existence of readily available *standards* or *best practices* is thus a good measure of the ability to rely on the results of any given IS Audit. These publications generally provide a suggested method of configuring a given technology to meet most frequently encountered audit and control requirements. While multiple versions of best practices will be in circulation among the audit community, they will be more likely to correspond to audit requirements when they are targeted at members of a specific community. For example, the Financial Services Roundtable Banking Information Technology Standards (BITS), the National Institute for Standards and Technology (NIST) standards for government agencies, and the Federal Financial Institutions Examination Council (FFIEC), all have documents that have a faithful following in the auditors, as well as the IT management, in those industries.[59]

---

58 More information on CIS available from World Wide Web: <http://www.cisecurity.com>

59 More information on these organizations standards is available from World Wide Web: <http:// www.bitsinfo.org>, <http://csrc.ncsl.nist.gov>, <http://www.ffiec.gov>.

1.3.3 To the Auditee:

Though targeted at accountability at a higher management level, the bottom line effect of most legislation is ever more strict IT controls. On the positive side, regulations serve to create a well-defined scope for control practices and associated review processes. When audits are commissioned for reasons of regulatory compliance, the auditors represent the concerns of the regulators. Though regulatory agencies may focus on different levels of detail in their requirements, audits always begin at the ICS level. If you have in advance determined a method of complying with a regulation, then the regulatory compliance audit will probably be composed of compliance tests, that is, tests of your own controls. Your role as an IT manager is to reflect regulatory requirements in your procedures, and that starts with your ICS. However, if you have not in advance determined your regulatory compliance strategy, then the audit will be substantive with respect to all transactions covered by the regulation. You may still pass the audit, but it will be more work for everyone involved, both the auditors and the staff you assign to work with them.

Authentication mechanisms, recovery timeframes, version controls, and numerous other configuration options are invariably tailored for a given environment. Nevertheless, an auditor will normally compare them to industry standards. If these do not match your environment, you may have to justify to the auditor why the industry standard does not apply to your operation. This is done via documented policies, research or analysis results, meeting minutes, or any other evidence that you have analyzed the risk-reward trade-offs of your options and established a configuration that meets the requirements of your ICS.

2. Audit Planning

Audits, like any other IT project, require schedules and resources to execute. Also like any other IT project, for schedules to be drafted and resources to be estimated, a full statement of work must be created. This chapter describes how information systems control theory is understood and communicated within an audit organization. Control theory and communication techniques have evolved within the audit profession over time, and continue to evolve. Nevertheless, systematic application of these techniques will generally result in audit programs that meet management expectations for addressing risk. They will also help ensure that individual audits of information systems control practices are properly designed in a methodical and efficient manner.

2.1 Risk Assessment

2.1.1 Risk Identification

This chapter describes how auditors get their assignments. The idea is that the processes that pose the most risk to the business should be examined to verify that management is controlling risk. In most large organizations, there is an internal risk management professional assigned to create an audit plan. This position may be called the Chief Audit Executive, Director of Internal Audit, General Auditor, Director of Business Controls, or some other title with a similar connotation.[60] The Chief Audit Executive is responsible for planning and executing audits of the organization's ICS for all risk areas. Chief Audit Executives will start with what they know about risks and industry standards, add in what they learn about a particular organization, analyze and frame the organization's control issues, then develop a high level audit plan. On a periodic basis, usually annually, they will review risk profiles, analyze operational processes, conduct surveys, carry out interviews, visit remote sites, and consolidate these observations into a high level checklist of risk areas to be presented at an executive level audit planning meeting. This chapter will focus on the risk assessment activity that is specific to IT.

In the course of this risk assessment, it is common for the Chief Audit Executive to interview the company CIO. If this is the case, the CIO may be able to influence audit planning by identifying risks to the business introduced by specific technologies or technology-related processes. However, unless the company is in the technology services industry, the influence of the CIO may not be as compelling as that of management in the profit centers of the company.

For companies that are required by some law or regulation to have an *independent* audit of financial statements, there will also be an *external* organization conducting an audit planning process. Laws and regulations typically require that the external auditor be an audit firm.[61] Audit firms will usually delegate audit planning representation to a specific statutory auditor, often a firm Partner. The work performed by Internal Auditors and External Auditors is very different, but the principles remain the same. External Audit has a financial statements risk perspective and may rely upon internal audit. Internal Audit has an operational risk perspective and may perform work that assists the external auditor. The External Audit Partner, like the Chief Audit Executive, will review financial statements and other documents to perform a rick assessment in relation to their areas of interest. Each will develop a high-level checklist of risk areas.

In publicly held companies, the Chief Audit Executive and External Audit Partner will both provide audit plans to the Board of Directors Audit Committee. Often, they will team in the preparation of their respective checklists in order to minimize the potential for controversy and conflict in respective presentations to the Audit Committee. As appropriate, given its status as the principal evidence of executive-level due diligence, the Audit Committee must read everything it receives from the Chief Audit Executive and External Audit Partner and be prepared to discuss it. Presumably, the Audit Committee will also have done some independent research prior to the meeting. Then, after reviewing the presentations of the Chief Audit Executive and External Audit Partner, they may follow up with some interviews or financial analysis. In

---

60 Though these titles may not be interchangeable at any given organization, the top Internal Auditor will be hereafter generically referred to as the Chief Audit Executive.

61 The most well known audit firms are referred to as the "Big 4": PriceWaterhouseCoopers, Deloitte & Touche, Ernst & Young, and KPMG. These companies all have audit divisions staffed mostly by accountants but also significant numbers of information technology specialists. There is no requirement that a publicly held company use a Big 4 firm as their independent auditor, but the depth and variety of resources these companies bring to the independent audit task makes them a convenient choice for most large global firms.

companies with no Audit Committee, this function, if it exists, might be assumed by the Board itself, or delegated at an appropriately high level to senior executives.

The point of all this analysis is to make sure that the list of suggested audits is sufficient to uncover significant risk exposures such as serious operational failures, financial and other report misstatements, fraud, criminal activity, misuse of assets, and any other material ICS weaknesses. However, no audit plan will ever be 100% guaranteed to uncover all possible ICS weaknesses. While choosing between suggested audits, the Audit Committee is aware that any decision will carry some form of risk. They weigh the pros and cons of suggested audit activity against three kinds of risk:

- Inherent risk - risk derived from the level of complexity of an activity as well as its materiality with respect to organizational objectives.

- Control risk - risk that internal controls are inadequate.

- Detection risk - risk that the audit process fails to identify policy violations according to plan.

The Audit Committee is charged with reducing the overall risk to the organization by approving an audit plan that takes into account the inherent, control, and detection risk factors.

In very large organizations, audit planning is an impossible task for one person, and the internal audit department may be broken down into teams that allow a divide-and-conquer approach. The breakdown may focus on financial statement composition, operational process, organizational structure, or any other partitioning scheme the Chief Audit Executive may impose upon the business. Within a partition, business processes are often sorted by inherent risk expressed in monetary terms, and this may result in more emphasis on requirements for audits of high risk areas. Some audit directors view information technology as a separate risk area, others provide for an information technology component in every business risk area.

Though IT planning is not as often locked into an annual cycle as audit planning, they are both budgeted processes and so tend to occur around the same time of year. The budget process tends to force IT Governors to place a “stake in the ground” on expectations for the fiscal year. They are being asked to make decisions on technology improvements and projects schedules just about the time the Chief Audit Executive is starting to gathering the information required to put together an audit plan. Whatever decisions are set at the time of Audit Planning form the basis of the risk assessment. For the rest, the Chief Audit Executive is left to independently assess the probability that technology changes will impact the list of potential audits.

An annual meeting of the Audit Committee usually results in the audit plan of record for the fiscal year. It will produce a list of risk areas that will be targeted that year for a “management controls” audits. Some of those may be exclusively “technology control” audits. The Internal and External Auditors will be assigned the work according to their respective levels of ability and fiduciary responsibility. Sometimes their audits will overlap, in which case they will decide to perform them separately or jointly.

Some audit organizations will have separate staff dedicated to IS audit, who will then review the schedules of IT projects and business processes that fall into the scope of the approved audit plan. If the associated business dependencies allow, the high risk areas will be first on the schedule. This order is followed because the audit plan produced by the annual planning process is subject to change at any time. A merger or acquisition may siphon audit resources away from an audit department, and the low risk reviews may drop from the schedule by year-end.

2.1.2 Risk Assessment Example

There are so many ways an IT risk assessment can proceed, it is more easily explained by example. This example assumes that an Chief Audit Executive has decided to consult the CIO in the course of preparing the annual audit plan. It illustrates that the technology audit planning process requires a cooperative effort

between the technology planners and the audit planners. The needs of the business drive the IT planning process. The interests of the shareholders and investors, as represented by the Chief Audit Executive, drive the audit process.

Just as the CIO is concentrating on ways to minimize development and deployment cost fluctuations, a letter arrives from the Chief Audit Executive. “Dear CIO,” it says, “I will soon be contacting your administrative assistant to schedule a meeting to discuss information technology risk. In order to prepare for that meeting, I respectfully request that you forward any documents you have that will give me up-to-date metrics on the company’s most critical computer systems, the status of the systems that were scheduled to be deployed in the previous fiscal year, and a list of new projects proposed for the new fiscal year....”

Though under tight deadlines to deliver the budget, the CIO agrees to the meeting. Administrative staff is directed to send the information on the critical systems and on last year’s deployments. But the CIO decides that the new project listing is not ready for critical review.

The Chief Audit Executive receives the information, forwards it to an audit manager dedicated to IS issues. The IS audit manager reviews the information sent by the CIO, identifies significant changes in critical systems, compares last year's results with last year's plans, analyzes prior year technology audits, and conducts interviews with technical project managers.

The IS audit manager identifies metrics that indicate business reliance on the associated systems. Example items to be measured may be the number of customer records held, the value of the assets tracked by a system, or the criticality of a system to maintain a guaranteed service level. Once systems are ranked by business risk, the IS audit manager identifies measurable components of the technology environment that indicate technology risk. The values for these metrics are researched and recorded for systems or categories of systems. This work results in a draft analysis of the company's most significant risks related to the use of technology. The analysis is labeled, “Technology Risk Model.” It is illustrated in Figure 2.1-1.

The Chief Audit Executive reviews the analysis, asks questions to clarify key control issues, supplements the analyses with financial information and insight into the company's systems requirements, and make suggestions for further research to improve the analysis. The IS audit manager schedules the meeting. The revisions and review process continues until the meeting itself.

At the meeting, the CIO is presented with the risk model. In return, the Chief Audit Executive receives the CIO's plan for the new fiscal year. It shows that the Decision Support system is being replaced by System Q, so they agree that the Decision Support system will be replaced by System Q in the draft risk model. The CIO asks a few questions about the extent of the IS audit manager’s analysis, and the method of determining values for metrics. Some changes are made to the draft plan based on the answers.

The Chief Audit Executive then asks the CIO for a general overview of the technology control processes. The CIO moves to the white board and draws the diagram in Figure 2.1-2. The CIO classifies each IT process into one of four categories: design, development, deployment, and production; then explains the categories. System design is performed by a small team of core engineers who may require a consultant or test equipment on occasion. They are well established but have unpredictable results and costs. Development results tend to fluctuate as unexpected customer demands and unexpected technology limitations are encountered during the course of the year. Deployment processes may also vary from expectation as unexpected performance and high availability issues may be encountered in the transfer from development to production. However, results do not change as much as they do in development. Production processes are well established and have predictable results and costs.

The Chief Audit Executive then asks the IS audit manager for a point of view on the industry standard control objectives for Information Technology. The IS audit manager erases the CIO’s diagram, and draws the diagram in Figure 2.1-3. The IS audit manager explains that the overall business objectives and IT Governance process can be loosely referred to as the overall IT strategy. Given that strategy, actual IT

activities will fall into one of four basic categories: planning & organization, acquisition & implementation, delivery & support, or monitoring.62 Planning & organization processes directly reflect the IT strategy, the people that make it work, and the communications processes. Acquisition & implementation is the process of building or buying systems, and covers everything from selection criteria to installation. Delivery & support includes all IT operations processes, including security to business recovery. Monitoring is the way IT Governors know it is all working. The IS audit manager explains that the diagram is circular to call attention to an important feedback loop. That is, if monitoring processes demonstrate that controls are not working, the monitoring provides the input IT Governors need to change their strategy.

The CIO then takes the marker, and annotates the IS audit manager's diagram to appear as in Figure 2.1-4. The CIO explains that planning, organization, and monitoring are done by immediate staff. Acquisition & implementation consume most of the organization's time, especially in picking out which system variables to closely monitor and how to monitor them. Delivery and support consume the vast majority of the rest of the IT resources, but a consolidated workflow system helps to manage that efficiently. The CIO professes to be happy to hear any insights on the planning and organization processes that arise in the course of audits, but thinks that an auditor's time would best serve the company in the acquisition, implementation, delivery, and support processes.

With this explanation, the CIO has provided the auditors with a description, albeit very high-level, of the control framework with which to view the controls the CIO has implemented within IT processes. The Chief Audit Executive and the IS audit manager agree that if the Audit Committee is willing, they will focus on the company's technology acquisition, implementation, delivery, and support processes. The Chief Audit Executive and IS audit manager may tweak their Technology Risk Model based on the results of the meeting prior to delivering it to the Audit Committee.

2.1.3 Control Frameworks

The example demonstrated appropriate interaction between the audit departments and the technology departments in the audit planning process. The two departments agreed on significant factors affecting risk, a risk model, and understood those factors in the context of a technology *control framework*. A *control framework* is a way of thinking about *how* IT processes are working to produce desired results. In the act of annotating the auditor's diagram in Figure 2.1-4, the CIO is mapping a way of thinking about the IT environment that matches the activities auditors expect to be taking place in the organization. The auditor is led to assume that the organizational structure, policies, procedures, and processes in place will reflect that way of thinking. A well-defined control framework will encompass all existent IT organizations, systems, policies, and procedures that are used to enforce management's ICS. It will allow IT Governors and IS auditors to share an understanding of the methods by which IT management is expected to control the IT environment.

Good IT Governors know when IT processes are working. Because they know both the systems and the business, they know just what it is important to closely monitor. However, it is always difficult to come in from the outside and immediately understand just why an IT Governor appears to be emphasizing some things that are thought to be best practice and not others. That is why auditors, coming in from the outside, will first try to identify the *control framework* that an IT Governor uses to control the IT environment. This helps them put each individual control practice they examine in the correct context of its place in the organization's overall ICS.

Frederick Brooks wrote an addendum to the 20th anniversary edition of *The Mythical Man Month*, that he entitled, "Why is There a Twentieth Anniversary Edition?" One "explanation often advanced", he observed, "is that *The Mythical Man Month* is only incidentally about software but primarily about how people in

---

62 See COBIT Framework.

teams make things. There is surely some truth in this; the preface to the 1975 edition says that managing a software project is more like other management than most programmers initially believe. I still believe that to be true."[63]

Although not as regulated and not as consistently applied, IS auditors use the same basic processes to identify internal controls that financial auditors use to verify them in accounting. Like the AICPA,[64] ISACA certifies members, holds them to professional standards, and publishes guidelines to help them make decisions about appropriate levels of controls. IT controls are increasingly essential to controlled business practices, and CIOs are increasingly held to the same stewardship standards as their accounting counterparts, Chief Financial Officers. There is increasing recognition that operative IT Governance may involve fiduciary responsibility. IT control frameworks are a critical subset of an organization's overall ICS.

2.1.4 To the Auditee:

Risks are inherent in that they exist whether or not there are controls. Risk that controls are inadequate, control risk, simply brings greater attention to inherent risk. Risk that inadequacies in controls go undetected, detection risk, is something an auditor find extremely concerning. Auditors set out to identify risks in order to provide an assessment or opinion on the effectiveness of controls. Their professional standing is at risk when they make that assessment. To do this, they need your help. Present them with whatever exists in the way of an IT control framework. Help them compare it to industry standards so they can be assured that they have covered all bases. The more they understand about how you approach your job, the more likely they will view the risks you encounter the same way you do. If they do not understand your control framework, they are likely to take up considerable amounts of IT staff's time and resources in the risk assessment effort.

Above all, view the audit risk assessment process as a way to test the assumptions that led to the creation of your control framework. Identification of a potential control risk may lead you to strengthen the process before the audit even starts. A well-defined control framework allows the IT Governors and IS auditors to share an understanding of the value to the organization of both the IT Governance and the audit process.

---

63 Brooks, Frederick P., The Mythical Man Month, Addison-Wesley, 1975, Anniversary Edition, 1995, p. 254-255

64 American Institute of Certified Public Accountants

2.2 Review Areas

2.2.1 Audit Objectives

In an audit of X, "X" is often referred to as a *review area*. When a risk assessment process has determined that there is risk in X, so "X" becomes a high-level description of what will be audited. The next step in audit planning is to build a more precise *audit objective* for each individual audit. A review area may be described in such general terms that the planning process ends up breaking it down into more than one audit, each with a precise audit objective and corresponding scope. *Review area* refers broadly to the thing being audited, *audit objective* refers to the purpose of an audit, and *scope* refers to exactly what will be audited. This chapter describes what a review area is and how the objective and scope of an individual audit is determined.

The audit planning process results in a high level list of IS audits and a schedule. Then it must be decided exactly what aspects of the system environment should be audited. Although auditors get some orientation to management's control framework, auditors will never spend enough time with a system to know it as well as its user community, developers, and operations support staff. Instead, they must decide on an angle from which to view the systems environment. The viewing angle must afford a determination that management has adequate controls to minimize risk. To help focus on aspects of the system environment that allow this determination, an IS audit manager will usually refer to different aspects of the systems environment as distinct review areas.

Review areas may be process-oriented, business-oriented, or control-oriented. These review areas will provide focus to the concerns that prompted the audit. That focus will help the audit manager define which systems will be in scope. To illustrate:

A review that is: *Process-oriented*
will focus on: *a given IT process*
so its scope will include: *the systems necessary to determine that the process itself is adequately controlled.*

A review that is: *Business-oriented*
will focus on: *a given business process*
so its scope will include: *the systems necessary to support the business process*

A review that is: *Control-oriented*
will focus on: *how a given set of technology controls are enforced*
so its scope will include: *all, or a representative sample, of the systems for which the control is expected to in place.*

The remainder of this chapter will illustrate how the high level technology risk model can be viewed in the context of a review area to produce plans to audit different systems.

2.2.2 Process Orientation

In the example of the previous chapter, the auditors selected key systems and agreed to focus on the acquisition, implementation, delivery, and support processes for those systems. They decided on a process-oriented review. Process-oriented reviews are becoming more prevalent as the ISACA Control Objectives for Information Technology (COBIT) gain increasing acceptance. Each of the four domains of COBIT have conveniently identified processes that IT managers are expected to implement (see Figure 2.2-1).

However, even in a process-oriented review, not all varieties of IT processes will necessarily be covered in every audit. It may be that all processes are not covered even in an audit of a single domain. Audit objectives will always focus on areas that present the most business risk. For example, in an organization with well defined architecture and very low personnel turnover, the audit objective may simply to be to ensure that the process for managing investments and projects are in line with a strategic plan. In that case, auditors may plan a *Planning and Organization* audit, but skip processes like *Defining Information Architecture* and *Managing Human Resources*. The scope of systems in the planning and organization audit might then be those that are illustrative of the planning process, for example, the purchasing and project management systems.

2.2.3 Business Orientation

Though our examples of audit planning have so far resulted in recommendations for process-oriented audits, any approach is valid as long as the resulting audit plan adequately addresses management's need for independent monitoring of controls. A different set of choices at the risk assessment level may have come up with an entirely different, yet equally comprehensive audit plan. If the IS audit manager had developed a risk model based on business units or company subdivisions rather than on critical systems, it might have instead looked like figure 2.2-2.

This type of risk model will produce audit review areas that are business-oriented rather than technology-oriented. After a discussion of systems risk in relation to this model, the Chief Audit Executive may suggest an “Sales Division” audit. That discussion may be followed by research on how each system is used by the sales organization supports the business process. The research may identify that some systems are more critical than others. The identification may help define an audit objective that included a definition of system criticality along with the statement, “the audit will provide assurance that adequate controls exist in the systems used to support critical sales functions.” All systems that meet the definition of “critical” would then be in scope.

It is important to note that a business-oriented IS audit is not a *business process audit.* Except where business processes are completely automated, pure business process audits are not primarily focused on IT. Their selection is based on risk in business operations such as order entry or service delivery. These review areas may encompass customer service procedures or marketing strategies. They may utilize business best practices or regulatory standards such as Malcolm Baldrige Quality Principles or Equal Opportunity Standards.65 If they cover IT, it is from the perspective of a business user rather than from that of the technology provider. By contrast, a review area in a business-oriented IS audit is always primarily focused on technology controls. That said, it sometimes happens that a business-oriented IS audit and a business process audit are performed simultaneously by and for the same organization.

---

65 More information on these standards is available from World Wide Web: <http://baldrige.nist.gov> and <http://www.dol.gov/esa>.

2.2.4 Control Orientation

Depending on the size and nature of the organization, it may not be practical to attempt an audit of the scope of an entire technology or business process. It may be necessary to focus only on certain aspects of technology controls that are critical to the success of any technology or business process. This is a control-oriented approach. The audit objective is to determine if a given set of controls exist with respect to an application or set of systems identified by platform. The scope is the combination of hardware and software that comprise the application or platform set. Control oriented review areas include, but are not limited to, the list in Figure 2.2-3.

External audit organizations will find it easier to perform control-oriented audits than process-oriented or business-oriented audits because they require less knowledge of the organization under review. Audit procedures for reviews in these areas are well documented and have undergone continuous refinement since the late 1970s.66 While the types of controls in figure 2.2-3 will also be examined in a process-oriented or business-oriented audit, they will be more critically assessed for relevance to the control of the process or business procedure under review.

When control-oriented review occur across a significantly large IT environment, it is common for IT Auditors to classify the controls under review into two categories: *general controls* and *application controls.* General controls are control practices that are done in the same manner throughout the organization's IT environment. Application controls are practices that are performed only in a specific set of systems that represent one or more applications of the same systems architecture. For example, general controls almost always include physical security and media library while application controls almost always include information protection. However, different IT environments will have different splits between general and application specific controls. For example, in an organization that has consolidate all user administration into a Single-Sign-On system, User Administration would be a general control. But in an environment where each application had its own user administration screen, it would be an application-specific control. A clear distinction between general and application controls allows an auditor to consolidate testing of general control practices across application environments and makes more efficient use of the time allocated to a control-oriented audit.

Assessing a technology control in and of itself is straightforward. However, the *result* of a control-oriented audit is still evaluated with respect to the technology or business process it supports. Management responses to results of a control-oriented audit will reveal the extent to which the technology control is germane to IT management's control framework. If the control review area audited is an integral part of IT management's strategy to limit risk, the control-oriented audit will receive close attention. If IT management relies more on controls that are not the focus of the review, the control-oriented audit may not elicit an attentive response. For example, if a government agency is bound by the Freedom of Information Act to share all of its data with the public, then an Information Protection audit may receive little management attention. However, the same agency may be very interested in a Media Library audit.

2.2.5 To the Auditee:

Try to recognize situations wherein you can influence the choice of review area. You may find your influence is more prevalent in planning by Internal Auditors than in planning by External Auditors. External Auditors represent outside interests rather than those of the company being audited, and are not as inclined to solicit your opinions. Review areas may even be specially selected by the Audit Committee without IT

---

66 Champlain, Jack, *Auditing Information Systems, Second Edition,* John Wiley & Sons, 2003.

management advisory. For example, the Audit Committee may contract a security penetration review without even notifying IT management.[67]

Once you understand where you have influence, try to recognize the orientation of the review area selection. The topic of review in any IS audit is always purely information technology, but whether the review is control-oriented, process-oriented, or business-oriented will affect your ability to understand the audit objective. So it is important for you to understand why certain review areas were chosen. The choice provides you with an outsider's perspective on your risks.

It may even be a good idea to step into the auditor's shoes by performing a control self-assessment of the review area.[68] Even a high level risk analysis of the review area will provide you with an auditor's point of view into the processes that you have implemented that reduce risk. An IT manager that understands why the review area was chosen for audit will be able to anticipate not only the auditor's concerns, but also the concerns of upper management.

---

67 Reviews conducted without the knowledge of the IT managers that run the systems in scope are referred to as "blind" reviews. "Security Penetration" reviews is an informal term for tests of security access controls facing a public system or network. Such interfaces are more likely to be subject to unauthorized access, or penetration, attempts.

68 Friedberg and Reisch, "The Value of Control Self-Assessment," *Information Systems Audit and Control Journal,* Vol. II, 1997, p 8,10.

2.3 Control Objectives

2.3.1 Identification

Review area choices determine audit objectives and scope. Given a review area and scope, auditors identify *control objectives* within the scope. An auditor will create a list of control objectives that satisfy review area concerns. For each control objective, an auditor will list control activities commonly used by management to meet the control objective. The actual *controls* in place at the auditee's organization will be identified and tested in the course of the audit. This chapter describes how control objectives determine which controls are tested in the course of an IS audit.

There are a variety of sources from which an auditor may select control objectives for a given audit. The ISACA COBIT publications are popular, but many auditors will instead reference the still relevant and reliable: Systems Auditability and Control Report,[69] the Handbook of IS auditing,[70] and a number of other similar publications.[71] The only requirement is that the overall set chosen for the audit completely address the inherent risks in the review areas within scope. The differences between two sets of control objectives for distinct audits of the same type of system in the same review area should be trivial.

In a "control testing" audit engagement, audit control objectives are expected to be the same as management's control objectives, and the auditor will obtain the list from management. However, even IT managers who have thoroughly analyzed the risks in the review area and have identified their own set of control objectives may not have them documented in a straightforward format. In this case, an auditor may rewrite management's control objectives before matching them with control activities. Where the audit objective does not require auditors to use management's set of control objectives, auditors may or may not adopt a list (if available) from IT management. External auditors may find it easier to perform the same type of review at several different companies following a standard audit program that uses industry standard control objectives. They may not have the time to analyze and incorporate a unique set of IT control objectives proposed by a single client. An audit team may be engaged to perform a substantive audit rather than a control audit. In that case, it would be unprofessional to test for management control objectives rather than test for the predefined criteria required by the substantive audit (and it would be likely to cost the price of the engagement).

2.3.2 Control Activity

Only when control objectives are identified does it become practicable to identify and test controls. However, there is no science in creating lists of control activities that correspond to a control objective. To derive control activities from control objectives, the objectives need to be specific and measurable.

For example, suppose the audit committee has decided that there must be an audit of payroll systems. After conferring with IT management, the Chief Audit Executive has determined that there will be one review area in the scope of the audit, and that is systems security. For that combination of audit topic and review area, an industry-standard control objective is that "to safeguard information against unauthorised use,

---

69 An Institute of Internal Auditors (IIA) publication which was funded by IBM and research by SRI.

70 Warren, Edelson, and Parker, *Handbook of EDP Auditing,* Warren, Gorham & Lamont, 1995.

71 For examples, see the bookstores at World Wide Web: <http://www.isaca.org> and <http:// www.theiia.org>.

disclosure or modification, damage or loss by logical access controls which ensure that access to systems, data and programs is restricted to authorised users."72

Tasked with verifying that management meets this control objective, an IS auditor creates this list of expected control activities:

- confidentiality and privacy requirements
- authorisation, authentication and access control
- user identification and authorisation profiles
- need-to-have and need-to-know data access requirements
- cryptographic key management
- incident handling, reporting and follow-up
- virus prevention and detection
- firewalls
- centralised security administration
- user training
- tools for monitoring compliance
- intrusion testing and reporting systems

Controls that support these activities may be in the form of roles and responsibilities, requirements documentation, change request authorizations, authentication procedures, and/or monitoring systems. These all are evidence of controls established by IT management. These controls may combine to fully support the control objective of "security measures are in line with business requirements."

---

72 In all examples, detailed control objectives and recommended audit steps are derived from COBIT.

2.3.3 Compensating Controls

Where auditors have not made use of control objectives and activities defined by IT management, it is common for the externally-defined control activities to be different than those of IT management. In these cases, it is not unusual for auditors to recognize the reasonableness of the alternative control activities established by management, and to take them into account. In our previous example, suppose when the auditors examined the environment, they could find no evidence of intrusion testing and reporting systems, which is one of the expected control activities. Suppose instead that management had incorporated anomaly detection and security policy compliance checking into its enterprise network management system. In this case, the ability for that system to detect intrusions in the form of unusual or non-compliant system behavior *compensates* for the lack of dedicated intrusion testing and reporting systems. The intrusion detection capability of the network management system is accepted by the auditors as a *compensating control*. Auditors could then test the integrity of the network management system and use that testing as evidence that the control objective of ensuring system security is met.

2.3.4 To the Auditee:

You may be one of the many IT managers who define "controls" as "constraints."73 If that is your definition of controls, it is most likely because the most well understood controls are preventive controls, or access control mechanisms. It is easy to see that in preventing harm from happening to systems, it is often necessary to implement restrictions on system features at the operating system, application, or user level. However, if your definition of "controls" is "activities in support of control objectives," you see that controls are enablers, not constraints. Controls enable you to state with certainty that your systems are configured according to your plans for mitigating risk. Control activity may have the side effect of putting constraints on system users. However, a well designed system will allow controls to peacefully coexist with all other user requirements.

Regardless of how you define controls, as an IT manager, you have goals for maintaining the IT environment in a manageable state. These are your control objectives. Document them in a way that makes the corresponding activity transparent to an external observer. It is to your advantage to share them with the IS auditor for two reasons:

- If the auditor uses your control objective and corresponding activity lists, you are highly likely to pass the control testing phase of the audit.

- The audit itself becomes another way for you to verify that your organization is following your orders.

In cases where a specialized or external audit requires that auditors to adhere to predefined control objectives, the corresponding control activity lists may not always map easily into your technology management strategy. In these cases, it is always acceptable for you to make suggestions. It is perfectly professional to request a copy of the control objectives and expected activity lists at any time in the course of an audit. After reviewing an auditor's predefined control objectives and expected activity lists, it is acceptable to identify the alternative controls that you believe still meet the control objectives. Your initiative in demonstrating that you have a management strategy that calls for alternative control activities may be a significant factor influencing audit results.

---

73 Henry, Kevin, "Operations, the Center of Support and Control," *Information Security Handbook, Fifth Edition,* Auerbach, 2003.

2.4 Audit Programs

2.4.1 Programs as Guides

Auditors will invariably follow a step by step process in performing an audit. The documented process is called an *audit program*. These programs are multidimensional. They serve as guides to ensure that audits are on track. They provide evidence of duly diligent efforts to ensure that audits are complete. They can function as training materials to bring new auditors up to speed in a new technology. Most importantly, they are tools to get the audit done. This chapter will explain these different facets of the audit program and demonstrate how they can be made transparent to IT management.

Auditors enter an environment in search of activity established by management that contributes to control objectives. As a guide in their search, they bring with them an audit program. The audit program will document the review area, control objectives, and the controls an auditor is expecting to find in the course of the audit. It will contain a step-by-step description of the actions that an auditor will perform to ensure that the identification of controls is truly objective. Each step in the step-by-step description is called an audit step. The documented audit steps are all actions that an auditor will take to verify that controls are in place. Therefore, the audit program reveals what exactly will be taken as evidence that controls meet a control objective.

Audit steps in an audit program should be identified by review area, control objective, and expected activity to be observed or evidence to be collected. Those observations and evidence can demonstrate that the given control objective is met. For example, auditors intend to assess the IT organization's effectiveness regarding “Information Protection.” They further define the review area of “Information Protection” as “Security of the organization’s data and access privileges established in conformance with legal and regulatory requirements.” They elect to examine Information Protection in the context of two information technology control objectives: “Ensure Systems Security” and “Manage Third Party Services.” In the course of the audit, they will determine whether these processes are in place by examining the two processes with respect to control objectives corresponding to the process as follows:

- Ensure Systems Security: to safeguard information against unauthorised use, disclosure or modification, damage or loss.

- Manage Third Party Services: to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements.

To complete the audit program, the broadly stated control objectives must be defined in detail, and the auditors must determine what type of evidence will count as verification that the control objectives are met. Complete audit programs identify in detail the technology or behavior that contributes to meeting control objectives, the actual controls. Evidence of controls is gathered via audit steps. The high level audit description in the previous example can be turned into an audit program by adding columns for audits steps, and some placeholders for the auditor to record results, as in Figure 2.4-1.

Note the column labeled “Pass/Fail” in the example audit program of Figure 2.4-1. That column indicates that the printed audit program will also be used to record audit results.[74] The column for “Evidence” likewise indicates that the auditor will be filling in blanks during the course of the audit. The “Evidence” column usually contains a reference to other documents that contain the evidence supporting the Pass/Fail

---

74 It is traditional that audit programs are used in printed form with the pass/fail column blank in order to serve as a checklist in recording results. However, it is becoming more and more common for audit programs to be stored in a database with a graphical user interface through which the auditor builds the audit program and also records the results.

mark for the audit step. This type of audit program provides a determination of completeness in the testing of control objectives. When all the Pass/Fail marks and Evidence references are in, the audit is done.

2.4.2 Program Completion

A complete audit program is created prior to the start of an audit. In most cases, the audit program must be reviewed and approved by the auditor's supervisor before the start of the audit. The Chief Audit Executive or External Audit Partner will often personally review audit programs in order to be assured that the audit will meet expectations. One aspect of that review is to ensure efficient distribution of the work effort within their own firm or department. This consideration leads them to demand that the format of the audit program and associated evidence references provide a level of detail sufficient for IS audit managers who may not be present at the time of the audit to conduct quality control reviews. In addition, the Chief Audit Executive or External Audit Partner needs to determine in advance the level of resources necessary to perform the audit. The audit program shows them exactly what steps the audit team will perform to gather the evidence necessary for independent assessment.

Evidence and independence are key concepts for the IS audit manager who reviews the audit program. An IS audit manager performing a quality control review must decide whether an auditor has planned to identify enough controls on which to base an assessment and whether the planned evidence is sufficiently objective. These decisions are essentially judgement calls, but published standards and best practices do provide some guidance. Conformance to industry standards is a practical method of designing audit programs that enable an objective assessment of management control.

Industry standard evidence may include observations, notes taken from interviews, the results of audit steps, or logical analysis of documented evidence. An auditor must assess the evidence for both quality and quantity, and then document it. Documentation should include the time, the date, the persons present, and a detailed description of the observation, conversation, or analysis process. If there is computer-generated material that provides evidence in the course of an audit step, that should be printed, or otherwise archived in a method that is easily retrievable by a quality control reviewer. The documentation on the archived file should include a description of why the file is considered evidence. In the course of an audit step, an auditor may collect evidence in the form of company documentation or correspondence. That too should be archived and documented as to why it is considered evidence.

There are a few industry standards an auditor will follow in evaluating evidence.[75]

- Evidence obtained from outside sources is more reliable than evidence provided by the organization being audited. For example, a dollar figure on a quote obtained directly from a vendor is more reliable than a budget spreadsheet in determining the expected cost of equipment.
- The qualifications of the person providing the evidence should be considered. For example, if an interviewee describes a technology implementation outside that person's area of technical expertise, it will not be considered as reliable as a description coming from an expert in the field.
- Objective evidence is more reliable than that which requires evaluation or interpretation. For example, a listing of system response time measurements taken every hour is more reliable than a user's description of perceived variances in system response time, because the latter may vary from person to person.

As the Chief Audit Executive and External Audit Partner are not generally present during the audit, they must rely on every individual auditor also being cognizant of these standards. From the level of detail in the

---

75 *CISA Review Manual*, ISACA, 2004, p. 41.

example IS audit program of Figure 2.4-1, an IS audit manager can determine whether the audit team is sufficiently prepared to gather enough evidence of controls to determine that control objectives are met.

Upon review of an audit program, an IS audit manager may determine that the proposed steps are inadequate to the task of reviewing a particular technology. In that case, a technology specialist with expertise in that area may be called in to contribute some audit steps. The detail in the audit steps may come from a variety of sources. There are textbooks, seminars, newsgroups, and web sites on audit steps just as there are for any other technology niche. Where multiple auditors collaborate on an audit plan, the audit program serves as a communication device among them, and also between the audit team and the Chief Audit Executive or External Audit Partner. It focuses the team on control objectives and controls rather than on all possible methods of examining a technology.

2.4.3 Tools for Execution

A very detailed IS audit program should describe audit steps in such a way that a person who is not even familiar with the technology to be audited can follow them and document results. To develop such a program requires considerable expertise in the technology. Once developed, the material required to perform the audit is organized, which allows the work to be divided. The program becomes an invaluable source of educational material for the junior auditor. A trainee can immediately determine what the professional expectations are for the assignment. The step-by-step nature of the instruction makes it easy for inexperienced auditors to identify which aspects of the audit may provide challenges. It helps them to decide whether to solicit advice or assistance from a senior auditor. The senior auditor will often provide help in the form of a more detailed set of instructions for a given step, and this process improves the audit program for future use.

The detailed audit programs also make it possible for auditors with specialized technology experience to be productively shared among audit teams. The rare technical expertise does not have to be utilized redundantly in the planning or even execution processes of similar audits. Rather, IS audit managers can ask technology specialists to execute audit steps that contribute to evidence for a given control objective. The technology specialist auditor then simply moves from audit to audit and executes the predefined steps. For such an experienced auditor, the audit program provides the context within which the test results should be evaluated.

As the program is executed, an IS audit manager may measure progress by reviewing the *Pass/Fail* marks, and comparing them to the *Evidence* references. If the evidence seems insufficient to support the associated mark, the IS audit manager should propose that steps be repeated or new steps be added in order to maintain the quality of the assessment concerning the overall control objective.

However, that a given audit step produces an unequivocal Fail mark does not necessarily imply that a control objective is not met. Even if an auditor can find no evidence of the controls listed in the audit program, there may be compensating controls in the form of other activity that meets the same control objective in a different way. To see how compensating controls are incorporated into an audit program, suppose the tabular audit program in Figure 2.4-1 is used in the actual audit process. The auditors examine *Ensure System Security* in the context of the detailed control objective on *logical access,* which includes the step: “Observe the user authorization process.” The auditors expect that if this control objective is met, then there will be “procedures for user authorization.” They have included an additional step in the audit program to obtain a copy of those procedures, which they intend to accept as partial evidence that the control objective is met.

Yet, the auditors are unable to “obtain a copy of procedures for user authorization.” They are able to independently gather evidence via all the other audit steps for the control objective labeled “Ensure Systems Security.” Analysis of the security policy allows the conclusion that access should be restricted only to authorized users. There is ample evidence that logical access is in fact restricted to authorized users. Yet the fact that there is no evidence of user authorization procedures earns that audit step a Fail mark.

This failure to find a formal user authorization procedure does not automatically mean that the auditors conclude that the control objectives for logical access are not met. Instead, they bring the failure to the IT manager's attention and ask if perhaps there is some compensating control that may make the audit step failure less damaging to the overall control objective of “Ensure Systems Security.” Suppose in this case, IT management describes a compensating control in the form of an automated authorization process based on a job function code recorded in a human resources system. The audit step for “Observe the user authorization process” will replaced by a review of the automated authorization process.

Therefore, while audit programs provide a most concrete and detailed description of an individual audit, audit programs are by their nature flexible tools to be tailored to unexpected situations. From the auditor’s point of view, the most important thing is not the audit program itself, but the framework it provides to understand and assess the control objectives.

2.4.4 To the Auditee:

Analysis of risks results in review areas. Analysis of review areas results in control objectives. Analysis of control objectives results in audit programs. Up to this point, audit work is mainly theoretical. At the level of the audit program, you should verify that the auditor's theoretical risk analysis corresponds to real and readily identifiable technology components, processes, and associated controls. If given the opportunity, roll up your sleeves and help define the audit program.

3. Audit Execution

Audit planning brings an auditor to the point where an auditor can proceed to contact the auditee and begin collecting information with which to provide assurance that control objectives are met. Audit execution is the process of actually mapping control objectives onto current practice and deciding whether the two converge. Auditors are careful to gather as much information as possible about the systems and organizations within scope to ensure that their work accurately represents the control environment they have been asked to review. The various techniques auditors use to do this are described in this chapter.

3.1 Preliminary Data Gathering

3.1.1 Process Overview

Preliminary data gathering is a term covering any information-gathering process use to prepare for an audit. This chapter will describe the preliminary data gathering process and show how it can aid the auditee as well as the auditor. As an auditor gathers information about the technology under review, an IT manager may be gathering data about the audit scope and approach. In between the issuance of the audit plan and the scheduled time of an audit, IT managers may not hear from the auditors. But if they do, communication will usually begin at the time the auditor has scheduled to do some preliminary data gathering.

Prior to an audit, an auditor must prepare the detailed audit program. This may require considerable research into the technology under review. The auditor must assemble as much information about the technology as possible in order to minimize the learning time on site. Basic information required to start that research process is the composition of system hardware and software and its dependency on integration with enterprise-wide tools and techniques such as systems used for change control, single-sign-on, backup and recovery, or monitoring. To collect this information, an auditor will ask the CIO to identify *the IT manager in charge of the system under review*, or the *auditee*. Whether or not the auditor asks the auditee for assistance in collecting the basic system components, preliminary data gathering always includes some form of communication initiation with the auditee to confirm that information. As part of preliminary data gathering, an auditor may also solicit information from the user community. The auditee will not necessarily be informed when this is the case.

If preliminary data gathering requires communication with the auditee a few weeks or months prior to the start of the audit, it usually coincides with the issuance of an audit announcement. Because of this timing correspondence, many audit teams refer to the audit announcement as a “planning memo.” Whatever its label, it is a formal communication from an audit team to an auditee that contains a notification that an audit has been planned within the auditee’s realm of responsibility. It usually includes a request for information that helps in the completion of the audit program. The letter announcing the audit may also request detailed diagrams, systems specifications, or copies of technical manuals. This information may be compared to the risk model that identified the need for the audit. It will help the auditors to decide what detailed control objectives need to be reviewed.

Sometimes preliminary information gathering requests will include information required to complete some of the more routine audit steps, e.g., obtaining a copy of the procedures for security monitoring. Where these procedures are available by fax, mail, or email, the audit step itself may be performed in the preliminary data gathering process.

It is not often that the auditee has had the accommodation of the one-on-one planning meeting that was illustrated in our example planning meeting with the CIO. Therefore, it is not often that the auditee is provided with a complete picture of where the audit fits in the context of an overall risk assessment or control framework evaluation process. From the point of view of the IT manager, the audit planning process will seem to start with the audit announcement letter or a similar phone call and consist of preliminary data gathering. However, from the point of view of the auditor, preliminary data gathering is part of audit execution.

3.1.2 Management Participation

In the first contact, auditors will usually introduce themselves and their mission, ask for information, and provide a date when they will arrive on location. This is the time for the IT manager to begin proactively coordinating a response to the audit. Preliminary information gathering can go both ways. When the auditor asks for information, it is a perfect opportunity to respond with prudently prepared questions. The IT

manager is entitled to ask for a detailed description of the review area, a listing of control objectives, and a copy of the audit program.

IT managers should use the preliminary data gathering process to take inventory of their own ICS and assess whether it is addressing the risks that are inherent in the review area. First, an IT manager should determine which systems fall under the scope of the review area. For example, in a process-oriented review, these will be the set of systems that are necessary to support the process under review. A very thorough process- oriented review will also include systems used to support, maintain, and provide recovery for the systems that support the process.

The IT manager will be expected to demonstrate that the ICS that supports these systems is explainable in terms of the control framework that the organization may have already shared with the auditor. If it is not, it may be time for the auditee to examine operational procedures with an eye toward control improvements. Control improvements are no less supportive of control objectives simply for having been implemented just prior to the start of an IS audit. That is, as long as they are permanent changes to IT processes.

The preliminary data gathering process is also an opportunity for an IT manager to address any issues of concern with the upcoming audit logistics. The IT manager may be concerned that there will not be enough staff on hand to meet both the auditor's requirements and an important deployment schedule. There may be concern about the auditor using system resources during production hours. The IT manager may attempt to negotiate the audit schedule to ensure that these types of concerns are addressed. That said, auditees should be aware that IT management requirements may not hold as much weight as audit requirements. Depending on who commissioned the audit, auditors may not be very flexible. For example, if the Audit Committee of the Board of Directors asks an auditor for a report to be delivered before their next meeting, then there will be no flexibility when it comes to the audit start date.

In between the audit announcement and the audit start date, appropriate interaction between the auditor and the auditee includes any method by which they can share information. The initial conversation between an IS audit manager and the auditor who announces a review may easily turn into a negotiating session. The two organizations negotiate the amount and timing of information that will be provided to each other in advance of the audit, the audit start time, and duration of time the auditors will spend on site. For example, an IT manager may receive a letter like that in Figure 3.1-1. The letter invites the IT manager to call. Appropriate questions to be used by the IT manager in that phone conversation are:

- "Why a user administration review?"
- "What set of control objectives will you test?"
- "May I have an advance copy of the control objectives and audit program?"
- "How long do you plan to do fieldwork?"
- "Will you please make sure to schedule a meeting before you leave the site?"
- "Do you plan to run audit software on my systems?"
- "What's your email address?"

Simply to ask a question does not ensure that an IT manager will get a definitive answer. But given the auditee's status as a stakeholder, it is perfectly appropriate to ask.

Moreover, it is evident from the description of the audit planning process that if an auditor cannot completely describe the review area, it was premature to announce the audit. In that event, IT managers should raise a flag to their own management to see if it is possible to clarify the scope and objectives of the

audit prior to its commencement. On the other hand, if the auditor cannot answer a question concerning detailed control objectives, it may be premature for the IT manager to be asking. The full audit program may not yet have been signed off by the IS audit manager.

It sometimes happens that an auditor will answer a question by saying that, although they have the information requested, they cannot share it. That is an issue for an IT manager to bring to an IT Governor. It is true that auditors are necessarily independent. However, standards for independence do not necessitate gaps in communication. So if auditors do not share information an auditee believes should be available, the issue may be addressed through management channels.

3.1.3 To the Auditee:

The preliminary data gathering initial phone call is usually meant to be directed to the lowest level of IT management that has complete responsibility for the integrity of all the systems and/or processes that are in scope. Sometimes, the first phone call is misdirected. The auditor may have the wrong contact name for a given system or process. It is helpful to the audit process if you create some awareness that IT staff should communicate with auditors only concerning their areas of direct responsibility, and otherwise direct their questions appropriately. Overly helpful IT staff may mislead and/or delay an auditor by commenting on a process for which they have only peripheral knowledge.

Once you have been identified as an auditee for an upcoming audit, see that the auditor learns as much as possible about the technology under review. The more prepared they are when they arrive, the less time they will take of your staff to assist in filling in the gaps. Where systems and/or procedures are complicated, you may decide to clear calendars of key personnel to ensure that those most knowledgeable of the control structure are available to be interviewed at some point during the audit. The preliminary information gathering process should yield enough information to decide whether that level of effort will be necessary.

Above all, use the preliminary data gathering process to learn as much as possible yourself about the review area, control objectives, and audit program. Ask any question that occurs to you. Answer the auditor's questions as best you can. Figure out exactly what the auditors will be looking for when they arrive, while emphasizing relevant aspects of your control framework so they will know where to start looking.

3.2 Fieldwork

3.2.1 Opening Meeting

The vast majority of auditors rival national sales managers in the frequency of their business travel. The end of on-site audit activity is thus frequently referred to as “the time they leave for the airport” or “the time they get on the plane.” *Fieldwork* is a generic audit term that refers to any activity performed by auditors outside the confines of their own office that contributes to the completion of an audit program. This chapter follows the audit process from the first appearance of the auditors on location until the time they leave for the airport. The activity that they accomplish on site is divided into three distinct segments: opening meeting, on-site testing, and closing meeting.

An *opening meeting* is the meeting that is scheduled to commence directly upon the arrival of the audit team on site. It is the first day that an auditor will start executing an audit program. A scheduled opening meeting serves several purposes for the IS audit manager. The opening meeting:

- provides an inflexible deadline before which the audit team must complete preliminary data gathering
- ensures that IT executives are sufficiently informed as to the purpose of the audit
- provides a forum to discuss the participation from IT staff that is expected throughout the fieldwork
- helps to ensure that the audit begins on schedule

The opening meeting also gives the auditors a place to arrive. It is usually held in a conference room with access to business traveler necessities like telephones and coffee. It shields the auditor from having to sit in a lobby while these minimum daily requirements go unmet. The opening meeting will have produced a schedule of events for the audit, and it should also give the auditor a sense of where within the site the remainder of time will be spent.

An audit team will often request a conference room or cube for their use for the duration of the audit. This will ensure that whatever time not spent directly at the side of the IT staff will not be unproductive. In between meetings and field trips, the audit team will congregate there and have informal meetings of their own. Regardless of whether the auditor requests it, the IT management will typically reserve some space in which the auditor may take such refuge. The benefit to IT management is that the auditors will take the minimum amount of IT staff time necessary because they won't be borrowing the staff's desks, chairs, white boards, and phone lines.

Moreover, the opening meeting gives management on both sides the chance to meet each other face to face and ask questions. The IT manager should use the opening meeting to have a systems control framework discussion, and to nail down the review area and control objectives. If there was a great deal of communication during preliminary data gathering, this part of the opening meeting will just serve to remind participants of previously agreed upon logistics.

The invitation for an opening meeting almost always goes to the most senior IT manager stationed at the site of the review. It may be extended to the corresponding IT Governor, even one whose office is at a different location. Though an IT Governor may delegate the opportunity to participate in the meeting, that suggestion is rarely if ever made by an IS auditor. To an auditor, an IT Governor’s fiduciary responsibility seems sufficient to motivate a personal appearance.

Another individual that is commonly invited to an opening meeting is the Information Security Officer.[76] This is because of the prevalence of the use of security tools and techniques used to implement IT controls. Though security itself is generally one review area, aspects of information security appear in almost all other review areas. Therefore, it is likely that the Information Security Manager has general knowledge of the organizational roles and responsibilities within the scope of any review. In fact, it is often the Information Security Officer that attends the opening meeting on behalf of the IT Governor, and introduces the audit team to appropriate contacts in other review areas and escorts them through the rest of the organization.

However, delegation of the responsibility for hosting the audit team sacrifices the personal touches that an IT Governor may display in the presentation of IT management control objectives. Often a casual comment by an IT Governor will reveal the extent to which controls are evident in the IT decision-making process. This type of comment is unlikely to come from a mid-level manager or staff position. Though not always practical, it is to the advantage of the IT Governor to be personally available at the opening meeting and throughout the course of the audit.

At the opening meeting, the review area must be well defined, and the set of control objectives to be tested should be available in writing. An audit opening meeting without defined control objectives may be interpreted as, at best, a legal investigation, and at worst, a fishing expedition. During the meeting, the IT manager is expected to commit that the IT staff are aware of the scope, and to agree with the auditors that the set of controls to be tested is appropriate given the audit objective. Upon review of these control objectives, the IT manager is expected to select members of the IT staff to actively participate in the controls testing. The auditors may be instructed to contact specific people for the management presentation on each control objective.

This explicit delegation is helpful not just to the auditors, but also to those key staff members present at the opening meeting. The directives for cooperation and instructions for specific representation are more likely to be followed if the IT staff participates fully in the opening meeting discussion. The designees for each control objective gain an understanding of the auditor's objectives in addressing a specific subject matter within the context of the overall review.

This instruction and cooperation of the IT staff is expected regardless of whether the negotiation on control objectives is successful from the point of view of the IT Governor. The audit is after all commissioned at some level by the executive management. There is a communication path in that direction if the review does not seem to adequately address risks from the point of view of the auditee. That can be done while the audit is in progress. The list of control objectives tested can be modified at any time prior to the auditors' departure.

Hence, the auditors' departure schedule should be a topic at the opening meeting. Often, an auditor will suggest scheduling a closing meeting with IT management. This allows them to discuss potential control weaknesses with IT management prior to the issue of a draft report or other more formal method of communicating audit results.

3.2.2 On-site Testing

The majority of fieldwork consists in testing control objectives. Because every systems environment is unique, actual test procedures may not be fully developed at the time the auditor arrives on site. An auditee is not expected to help with fieldwork, but it is expected that some IT resources will be available for the

---

76 Though this title or position is certainly not interchangeable at any given organization, the highest ranking person within an organization whose sole job is Information Security will be hereafter generically referred to as the Information Security Officer.

auditor to use to complete audit steps. For example, assume the auditor is following the audit program in Figure 2.4-1. It contains an example audit step with respect to logical security: “Verify that procedures for access control and user authorization on identified systems comply with policy.” Say the organization has a documented policy that states, “Passwords should not be easily guessable.” There are several methods by which this audit step may be completed. Here are three:

- The auditor asks for a terminal access to the system and a list of users, then tries to break into user accounts, first by trying to login without a password, then by trying to guess the user password.

- The auditor asks an IT system administrator to copy the user password file to a floppy disk, then runs a password cracking routine off-line to assess the existence and strength of user passwords, then views the results.

- The auditor asks an IT system administrator to install the password cracking routine on the target system, runs it on the system, then views the results.

In no method does the IT staff perform the audit step, yet each requires a different amount of resources for the IT manager to provide. Given that (i) IT staff time is a valuable resource and (ii) any user activity in a production system may affect critical business processes, it is acceptable for an IT manager to influence the choice of method by which an IS audit step is accomplished. Of course, the influence does not extend to the point where an IT manager can actually withhold the resources necessary to complete the audit step and thus prevent the audit step from being accomplished. But the first choice of the auditor need not always be the method provided by IT management.

To continue with our example, the easiest of the three alternative methods for completing the audit step is for the auditor to have the system administrator to install a password cracking routine on the system (the third method), so the auditor requests it. The system administrator discusses the alternatives with IT manager. Together they decide that to install the password cracking routine on a production system is unacceptable. Together, they approach the auditor and suggest that they load the tool on a test system rather than on the production system. They reason that the test system configuration exactly mirrors the production system, so the auditor should be assured that the reports will look exactly as if they were run on the production system. But the test system is not in the scope of the review, and the auditor does not have independent evidence that the two systems are in fact mirrored. Therefore, the auditor cannot accept this alternative.

Instead, the auditor proposes that the system administrator load the tool on the test system, then copy the production system user account files to the test system (the second method). Then the password cracking routine can be run on the test system and the results will still be valid for the production system. As long as the copy is done in a way that the auditor can observe and verify that the password cracking routine is indeed running on the production system files, then the audit step may be performed on the test system. The IT manager and system administrator agree.

In our example, competing methods of performing the same audit step required comprise and agreement, but the basic plan of activity involved in the audit step remained intact. In the auditor's preferred method, the auditor is looking at the results of the password cracking routine, in the second case, the auditor is viewing the same results. This illustrates a case in which the auditor’s basic plan for completing the step may not be feasible or advisable for the IT manager to accept. However, the IT manager must still find a way to provide resources adequate to complete the step.

To do so, the IT manager must rely on knowledge of the audit process and a clear line of roles and responsibilities between IT staff and the IS audit team in completing fieldwork. Although full cooperation is expected and required of an IT organization being audited, IS audit activity should not significantly impact the day-to-day activities of the IT staff. It is the responsibility of the auditor to come up with a feasible method of performing an audit step, and the responsibility of the IT organization to assist.

In assisting in audit steps, it is important to remember that IT controls also apply to auditors. If it is established procedure to supervise all non-system administrator access to user account files, then such access by an auditor must be supervised as well. The auditor's status as control tester does not change the status as outsider.

Even if an auditor is given a non-privileged account, the use of which does not require supervision, it may be beneficial to have the auditor's on-line activity supervised by a systems administrator. This will allow the administrator to learn the auditor's tools and techniques for determining if controls are in place. It will also allow the system administrator to catch the auditor's questions as they arise.

As the configuration of every system is different, auditors will always run into situations where they have questions on the system configuration. Unanswered questions are likely to become concerns about vulnerabilities which may result in preliminary *findings*. "Finding" is a technical term for an auditor, and the fourth definition in the dictionary accurately records its usage in the audit context: "the conclusion reached after an examination or consideration of facts by a judge, coroner, scholar, etc."77 For an auditor, it refers to those conclusions that result in Fail marks. Fieldwork findings are accumulated as control tests fail to provide evidence a control objective is met. The sooner an IT staff member can answer an auditor's question about system configuration, the less likely that the question will turn into a finding. This of course assumes that the answer to the question makes sense with respect to the IT controls framework.

Answering questions as they arise also saves the auditor from having to keep large lists of questions to be addressed later. Auditors will always keep lists of potential vulnerabilities that need to be discussed with IT management. The more questions that can be addressed as they arise, the shorter that list will be. When a knowledgeable IT staff member answers questions as they arise, this saves the time and effort an IT manager may have to spend, first in a meeting with the auditor and then to research the answers.

Supplying immediate answers to audit questions also may avert unnecessary concerns on the part of upper management. For example, say the auditors look at a system without the benefit of immediate answers and make a list of 32 questions. They schedule a meeting with the IT manager for the next day to "go over the findings." They fax their question list to their manager for quality review, but forget to retrieve it from the fax machine once it is sent. Three different people notice the list on the fax machine and the grapevine circulates that the auditors have a long list of potential vulnerabilities only three days into the audit. The IT manager is then called into the CIO's office, only to explain that all of the potential vulnerabilities are questions that any system administrator could answer to the auditors' satisfaction.

Of course, there may not be resources to monitor all audit activity. Nevertheless, whenever there is opportunity, IT staff should be encouraged to discuss with the auditor what conclusions are being drawn from observations. Throughout fieldwork, the IT manager should make time to periodically ask the auditor:

- "Are you waiting on anyone or anything?"
- "Have you identified any concerns?"

An auditor has no reason not to share concerns with management as they are identified. So if the answers to the above two questions are negative, an IT manager may safely assume that the auditor is so far finding that the controls objectives are met.

On the other hand, there may be concerns. Or the auditor may not have completely analyzed all the information and may want to suspend judgement on whether there are findings. In this case, an IT manager should be quick in pointing out compensating controls. A compensating control is not necessarily less

---

77 *Webster's New Twentieth Century Unabridged Dictionary, Simon and Schuster.*

strong than the expected control. It may be stronger evidence that the control objective is met. But it is the auditor who must ultimately assess the strength of a compensating control. In that assessment, the auditor will follow this basic prevention, detection, and correct hierarchy:

- It is best to prevent undesired events from happening.
- If undesired events cannot be prevented from happening, they should at least be detected.
- If undesired events cannot be prevented and are not detected in time for incident response activities prevent harm from occurring, the situation must be correctable.

For a control to compensate for an expected control, it must be at least on the same level of this prevention, detection, and correct hierarchy as the expected control. Otherwise, it may not be acceptable as truly compensating. If a control objective test calls for a preventive control and the IT manager instead demonstrates a detection control, there must be strong evidence that the risk addressed by the control objective is adequately covered.

To continue the password example above, assume that the activity expected to constitute the control does not exist, and so the audit step fails. The auditor finds that there are several users in the system that have easy-to- guess passwords. When the auditor approaches the IT manager with the information, the IT manager says, “Yes, they have easy passwords, but in order to login to that system, they need a hand-held authentication device, and they have to know another password to authenticate themselves to that device.” The auditor will have to create a few more audit steps to verify this information, but will end up being satisfied that the compensating control supports the control objective the same manner as the control that was expected.

One typical mistake made by an IT manager new to the audit process is to assume that the Audit itself is somehow a detective compensating control. For example, in the password example above, assume that the hand-held authentication is not in place. The auditor finds that there are several users in the system that have easy passwords, and approaches the IT manager with the information. In this example, the IT manager says, “You come here at least once a year and find those exceptions for us. We may not prevent this from happening but there is a detective compensating control. It may not be as good as preventing it altogether, but we will go find those users now and make them change their passwords and it will have close to the same overall effect.” This answer is unacceptable. The information systems audit itself is not an IT monitoring or compliance process. It is a monitoring tool, but it exists outside of the IT process it is monitoring.

The auditor is necessarily an objective outsider. When the Chief Audit Executive or the External Audit Partner send an audit team into the field, the qualifications in terms of audit training and certification allows the assumption that the auditor is well-drilled in standards of evidence. To complete their assurance that the audit program will be faithfully followed, they must also guarantee the auditor's independence. Sometimes, these professional requirements may appear to the IT staff as unsociable. For example, an auditor may refuse to give an opinion on which of two alternative control measures should be implemented or may insist on wearing a business suit in a casual environment. These idiosyncrasies should be viewed as an effort to maintain independence of attitude and appearance in the course of fieldwork.

3.2.3 Closing Meeting

With respect to fieldwork, the term “closing meeting” describes a meeting that occurs at the point at which all fieldwork is done, but the report has not yet been drafted. By this definition, meetings that occur during fieldwork to discuss preliminary findings might be referred to as a “pre-closing meetings” and the last meeting occurring at the last hour of the last day on site is referred to as “the closing meeting.” Some reserve the term “closing meeting” for a meeting in which the final draft report is discussed. In that case, the

word “close” modifies the audit report process rather than fieldwork. At that point, the audit would be completely over.

An IT manager should never let the fieldwork end without finding out what audit steps have failed. If the IT manager has made clear during the opening meeting that a closing meeting is expected, the IS audit manager will usually accommodate the request. Invitees to the closing meeting are usually the same as those invited to the opening meeting. But it is more rare that the invitees will delegate their attendance at the closing than at the opening. The closing meeting will provide a good sense as to what will be reported to the Audit Committee concerning the IT controls environment. Holding fieldwork pre-closing meetings gives an auditee an opportunity to discuss preliminary findings prior to them appearing on a list at the closing meeting.

An auditor may be hesitant to schedule a formal pre-closing meeting. Toward the end of their time on site, auditors will be busy ticking off audit steps, tracking down information, and shuffling meeting schedules. They will not have fully analyzed all the evidence so far gathered. An IT manager cannot realistically demand complete commitment to information shared by an auditor prior to the end of fieldwork. Rather, the information received at a pre-closing meeting should be treated more like a status report.

For example, an IT manager may insist on a meeting with the IS audit manager in the late afternoon on the day prior to the last day on site. The IS audit manager will agree to the meeting, but when asked for a list of audit findings, might say, “We are pretty certain we have fully tested and analyzed the first eleven control objectives, and have these two issues. For the next two, we have not fully analyzed the evidence. Our mainframe specialist is still sitting at the console with the Mainframe Security Administrator as we speak, but we don’t expect much. On the last control objective, we have not started, so we have nothing to say there.”

From this brief status report, an IT manager can infer that there are two substantial issues to deal with and perhaps as many as three more, but probably a conversation with the Mainframe Security Administrator will narrow it to one. There is a chance that the two substantial issues can be quickly resolved. This will leave only a small window of opportunity for the unknown to slip into the real closing meeting.

An auditor may enthusiastically agree to an early closing meeting schedule. The pre-closing meeting also provides a forum for discussion of the auditor’s analysis process. Where an audit step has failed, the auditor’s explanation of why it failed will demonstrate the basic assumptions and first principles underlying the auditor’s logic. These can be expected to be carried forward into the analysis of the as-yet-ungathered evidence. The pre-closing discussion helps the auditor understand how their analysis will be interpreted. It also gives the IT manager insight into how to view the IT processes through the eyes of the auditor.

If there is disagreement or doubt as to the auditor’s conclusions concerning a set of controls that meet a control objective, the IT manager may ask to review evidence gathered by the auditor of any identified control weakness. For example, if the only evidence that a control is not in place is an interview with a dubious source, the IT manager may challenge the evidence and suggest a different interview source. Some negotiation takes place, and the result is that the auditors have a to-do list of fieldwork that will be necessary to perform prior to leaving for the airport.

Every finding that is brought up in the pre-closing meeting should result in an action item for the auditor to complete more audit steps, or an admission that the control objective is not met by the IT manager. If there is no auditor’s action item, there is no way for the finding to be avoided at the closing meeting. Pre-closing meetings are information-sharing sessions; the conclusions of the audit are not yet formalized. If the IT manager accepts that there is a control objective that is not met, but believes the situation can be changed quickly, it is always possible to request another pre-closing to confirm the resolution of the outstanding issue. This usually requires a demonstrable change in IT processes prior to the closing meeting, and a commitment from the auditor to retest. The auditor will most likely accommodate if the schedule allows.

The pre-closing should have identified most of the findings, and ironed out the most significant issues to be resolved. The IT manager involved in the pre-closing meetings should have prepped IT Governors on what will be presented at the closing meeting. Therefore, the closing meeting should introduce no debates or surprises.

If the audit team wishes to schedule the closing meeting for the last hour they will be on site, it serves mutual benefit if the other attendees can arrange their schedule to accommodate. The last hour on site will be the time when all the audit steps are completed and all the findings are in. The IS audit manager or external audit partner will discuss the risks and potential solutions for each control weakness identified. All who attend gain an impression of the overall tone of the report.

The schedule of the report issuance should be discussed at the closing meeting. Audit organizations typically allow an opportunity for IT management to review and respond to the report prior to its formal issuance. The expected date the draft will be available, to whom on the IT management side it should be delivered, and from whom to expect a response are all topics for negotiation and agreement. If the auditors do not bring up the topic of report draft, review, and management response, then the IT manager should directly ask to be involved in the process.

The closing meeting should confirm that the objectives laid out in the opening meeting were met, and that fieldwork was completed. It should take the form of a presentation by auditors to IT Governors or their delegates. There should be no surprises. Ideally, it is simply an opportunity for personal contact prior to receipt of the draft report.

3.2.4 To the Auditee:

Your window to influence the controls testing process starts with the opening meeting and ends when the auditors get on the plane. If auditors perceive control weaknesses, you have from the time the auditors let you know what they are finding until the time they get on the plane to demonstrate that your control objectives are met. If you cannot make that demonstration convincing in person, you will have to make it in writing in the course of the subsequent audit issuing process.

Prior to the opening meeting, you should prepare the staff that will attend. Even a short conversation reminding them of their place in the systems control framework can prevent a lot of confusion as they check with each other during the opening meeting before directly answering an auditor's question. The reminder should be simply an agreement on the consistency of the semantics to be used to describe processes with which everyone is familiar. This preparation is even more important if the IT Governor will not attend the opening meeting in person. What is said should directly and accurately reflect the tone at the top. At the opening meeting, it is also appropriate to delegate one or two staff members as points of contact for a quick answer to a management-related question, should you not be not available at a critical point in the testing process.

If there is not a systems control framework in place at an organization, it is probably not possible to create it in the timeframe between an audit announcement letter and an opening meeting. In this case, the best course of action is to educate meeting attendees on the concept of a systems control framework so they will recognize what the auditor is talking about, and advise them to be quiet and cooperative during the meeting and use it as a learning experience.

Regardless of whether the auditors suggest a closing meeting, you should use the auditors' expectations of their time on site to schedule a "pre-closing" meeting. That meeting should be at least a day before the auditors' departure. In it, request a preliminary assessment of the environment and advise the auditors of controls that should be taken into consideration before any preliminary judgement becomes final. If there has been an initial disagreement on whether a control objective is met, and you believe that the auditor has decided that in fact it is met, then the you should confirm the belief. It may be confirmed by formally

asking the auditor to state that the control objective is met and also state that the issue will not be brought up in the upcoming closing meeting.

Go to the opening meeting with an open mind. Pay close attention to the fieldwork activities and findings. Most importantly, actively participate in the closing meetings.

3.3 Audit Reports

3.3.1 Audit Points

Though an IT Governor may have a bullet list of findings at the end of fieldwork, the organization of those findings may be changed several times prior to the first draft of the audit report. In addition, many audit organizations encourage IT Governors to include comments, or *management responses*, in the final report. Some Audit Committees require it. It is customary, though not required, for an internal audit organization to let IT management review and comment on the draft report before it becomes final. This custom is followed less in the case of external audit organizations, but occasionally will happen. This chapter explains how to interpret the draft report, and how to focus the review comments or responses to have a positive impact on the final report.

Upon return from fieldwork, auditors will analyze fieldwork findings and transform them into a set of "audit points". An *audit point* is paragraph or so of observations on the part of the auditor with respect to a related set of findings. Audit points are themselves referred to as findings. However, because the fieldwork findings correspond to individual failed audit steps from the audit program, there is rarely a one-to-one mapping between audit points and fieldwork findings. It is more often a one-to-many relationship. For example, a closing meeting where ten fieldwork findings are discussed may result in an audit report with only three audit points.

Once the audit points are drafted, the weakness in controls that is reflected in the first draft may be weighed against the importance of the control objectives to the overall ICS. The points may then be reordered according to the level of risk to the business that the associated vulnerabilities introduce. The fieldwork findings that support each audit point will be reviewed and discussed by the IS audit manager and the Chief Audit Executive or External Audit Partner. The outcome of this discussion may be a slightly different set of audit points.

The process by which findings are grouped into audit points follows an analysis along four dimensions:

Condition:a factual description of audit evidence

Criterion:some objective standard as to why the audit point is valid

Cause:the root cause of the situation that introduced the control weakness

Effect:the risk that the condition presents to the audited organization

Condition, criterion, cause, and effect are components of a well-developed audit point. But not all auditors will formally include all four components in every audit point. However, all audit points should include at least the condition.

The *condition* almost always comes first in an audit point. It should contain only facts, and make no judgement. The words "wrong" or "inappropriate" should never enter into the factual description of an audit finding. An example of a condition is:

> Password complexity controls were not implemented. Sixty-eight percent (68%) of the users chose passwords that were guessed by a common dictionary password guessing routine (493 of 723 total users). Most users used a first or last name, sometimes their user or department name (e.g.: "smith", "finance").

Agreement on the condition, or facts, should have been obtained during the closing meeting. The auditor should have evidence in the workpapers to fully support every fact stated. Where there are questions on the condition, it may usually be expanded to more directly refer to the supporting evidence.

The *criterion* demonstrates why the condition is not acceptable. It should refer to an objective standard. The standard may be a legal or regulatory requirement, a company policy, or result of research into industry standards. A criterion corresponding to the example condition might be:

> Company security policy requires that passwords are hard to guess.

The criteria are usually not negotiable or debatable, though if a criterion statement contains a policy interpretation, the auditee may suggest an alternative. For an audience that thoroughly understands the industry standard criteria to which the company is held, that component may be left out in the interests of brevity. If the criterion is left out, the auditee must still make an effort to understand what qualifies as objective criteria for the audit point. For this is the standard to which the management response will be held.

The *cause* should attempt to provide some background into the situation. It is intended to give the reader of the report some understanding of why the vulnerability exists. For example, one possible cause for the poor passwords in the example condition might be:

> No attempts have been made by the IT department to enforce company policy. Rather, individual users are expected to choose hard passwords.

If the cause is left out, it is likely due to the difficulty for auditors to fully understand all aspects of a computing environment in the short duration of their stay. The difficulty in identifying cause sometimes leads auditors to identify a proximate cause rather than the root cause. For example, suppose that the IT organization had in fact approached the user community and suggested automatically enforcing the policy for password choices, but the business users had refused to let them implement it. In this case, the proximate cause is that the attempt was not made, but the root cause is that the users refused to let the IT organization make the attempt. The auditee may suggest that the cause statement be modified to read, “Though the IT department has recommended that this policy be enforced automatically, business managers instead chose to rely on individual users to select hard passwords.”

The *effect* is a description of the risk involved in letting the situation continue to exist. It should refer to the business process which is most likely to be affected by the IT vulnerability. A risk to the computing environment without reference to its effect on the business would leave the target audience (the Audit Committee) wondering why they should be concerned. Agreement on the effect is key to presenting audit results in an objective manner. IT risks often are dependent on the probability of the enactment of a threat. Statements concerning risk therefore require an assessment of the likelihood that there is a perpetrator or natural disaster poised to enact a threat. To continue the weak password example, the effect may be stated as:

> The risk in allowing users to choose easy passwords is that a targeted attempt to access the accounts of a small set of users will eventually succeed (i.e., a “dictionary attack”). A single security breech will result in a long-term undetected security vulnerability (at least until the password expires in ninety days, and only then until one is guessed again). If compromised, the intruder’s activity passes for that of a legitimate system user. The risk is directly proportional to the likelihood that someone will be motivated to gain access to another users’ account. The likelihood is increased where the account has access to critical corporate resources or operations such as insider information or asset disbursements.

If the target systems do not in fact manage information critical to corporate resources or operations, then the risk to the business may be significantly less. The auditee should ascertain that the audit report presents risks as realistically as possible.

A consolidated audit point that combines all four examples is illustrated in Figure 3.3-1.

In the ideal scenario, the IT Governor responsible for the review area should have access to a draft of the final report that includes all audit points and at least a week to request revisions. Though some of these components may be missing or implied, it should be possible to obtain agreement with the auditor on all

four components of the audit point. Even if the draft is factually correct, if the wording or tone offends, the auditor may be requested to change it.

3.3.2 Recommendations

In the example of Figure 3.3-1, the documented audit finding is followed by a recommendation. The criteria, cause, and effect components of an audit finding make it clear that the condition identified the finding is something management must correct. The recommendation is not a formal component of the audit point itself, but it serves to give IT Governors an idea of the type of an action required to reduce the risk identified by the audit point. A recommendation for activity to be performed in response to an audit is not advice for expanding an IT manager's job function, it simply highlights the fact that current activities performed in the course of executing the function are insufficient to address known risks. From the time a finding has been formally identified via the audit process, management is responsible for corrective action as well as any outcome that arises with respect to the risks that the condition presents.

Historically, audit points are followed by recommendations in recognition that management may not have experience in addressing the given condition. They provide a guide on how to close the vulnerability. But IT managers that are sophisticated at addressing risk often devise their own solutions to audit findings. It is not necessary that the auditee agree with the recommendation that follows the audit point, but it is better if the audit team and IT Governor can present one solution to upper management. This agreement leaves little doubt in the minds of the Audit Committee that the risk will be adequately resolved. Where there is disagreement between auditors and auditees on how to close vulnerabilities, it is more difficult for upper management to be completely assured that IT Governors are diligent in addressing risks. So if the auditor presents a recommendation that an auditee knows will not be followed, it is worth the time to try to persuade the auditor to adopt a different recommendation to close the vulnerability.

Suggesting an alternative recommendation will not offend an IS audit manager or challenge the serviceability of the auditor for the task of auditing. It is simply an admission that a person intimately familiar with the technology may come up with solutions more efficient than an independent outsider could recommend. Even for detailed and thorough recommendations, IT engineers may devise different ways to address control weaknesses that an auditor finds, and sometimes it is appropriate that the organization that must live with the solution be the one to create it. Discussing alternative correction strategies with auditors may also be helpful in devising cost-benefit scenarios of alternative corrective actions.

Whether or not the official recommendation is agreed to by IT management, there may be an opportunity to answer every audit point in the report with a written management response. The management response is more than just a description of the appropriate solution to the identified issue. It is an action plan. Where possible, an IT manager should correct vulnerabilities as recommended on the audit report before the response is due. Then the response can read: "Management agrees. Action completed." In the eyes of an Audit Committee, this is the ideal management response.

Where action plans to close any identified vulnerabilities need more time, the description of the solution should be well integrated into activities that are routinely performed by the IT organization. This gives the impression that correcting vulnerabilities is expected and routine. Only in the most obvious cases of pre-identified business risks should an IT manager present a solution to an audit vulnerability as a costly and time-consuming new project. In such a case, a question arises as to how IT management could have lived with the risk prior to the audit without repeatedly notifying the Board of Directors that this threat to business continuity existed.

3.3.3 Executive Summary

The audit points are the most significant part of the audit report, but they are the last to be read, if ever. The first read item on the audit report is the Executive Summary. This is usually a two-pages-or-less summary of audit results. It will devote approximately one sentence to each audit point. It will contain a one-line

indication of whether the Chief Audit Executive or External Audit Partner is satisfied that IT Governors adequately addresses business risk.

The line may read something like this:

> Policies and procedures in place reflect best practices in most of the areas reviewed. Our overall assessment for the environment is satisfactory.

Or it may read something like this:

> We applaud the efforts of IT management to improve controls, but the recognition of the job still to be done renders the overall assessment for the environment unsatisfactory.

From the point of view of IT management, the first assessment is obviously more desirable than the second. It is important to closely review the executive summary section of the audit draft and be alert for words that seem to carry the weight of final pronouncement. Audit organizations often have pre-defined criteria that are consulted prior to making these assessments. A telephone discussion on the proper interpretation of the executive summary may be in order.

The executive summary is brief because the many of those who are required to read audit reports may not need to know the contents in detail in order to perform their responsibilities with respect to them. There are usually several people on an audit report "copy-to" list. This is the list of people who, in addition to the executive to which the report is addressed, will get a copy of the report. The copy-to list will always include the IT manager responding to the audit, and it will also usually include:

- the chain of IT command between the auditee and the CIO
- the head of the affected business unit(s)
- the chief financial officer
- the chair of the Board of Director's Audit Committee
- the Chief Audit Executive
- the External Audit Partner (regardless of whether it was an internal or external audit)

If there are more names on the list, it may be to the advantage of the IT manager to find out why. It may be that the auditor is thinking that another organization will be affected by a vulnerability identified in the report. Or it may be that there is an oversight function appointed by the Audit Committee that will be tracking audit results. If a copy-to list does not appear on the draft report, it is perfectly acceptable to ask the auditor for it.

3.3.4 To the Auditee:

If there is one thing to keep in mind while participating in the audit report process, it is that you are a participant. If the auditors provide you with a draft, it is for the sole purpose of soliciting your comments and responses to audit points. Understand the condition, criteria, cause and effect of each finding. Negotiate acceptable recommendations. Carefully plan and wordsmith the management response to each audit point. The effort could save countless hours of meetings and explanations with everyone and anyone who gets a copy of the report.

Review the copy-to list and identify anyone on the list who will be surprised by the report or who may misunderstand the executive summary. You should contact these people and discuss the audit points with

them before the final report is distributed. Depending on the circumstances, it may even be advisable to have the IS audit manager participate in a pre-report distribution meeting or conference call.

Most importantly, if you disagree with the wording of the executive summary, but cannot persuade an auditor to change it, that information should immediately be communicated to the CIO. It is always better to hear bad news from someone in your own organization.

3.4 Remediation

3.4.1 Periodic Queries

In most controlled organizations, audit points are immediately addressed as identified in the management action plan. The audit is not completely over until the management action specified in the report is taken. However, there are times when control improvements fall to the wayside and audit point remediation must be prompted by periodic status queries. In some regulatory environments, an internal audit department is required to report to the Audit Committee any situation in which management action plans are unreasonably delayed. Hence, many internal audit organizations have established a follow-up program to ensure that findings are addressed. However, even in cases where audit follow up is not a regulatory requirement, it is common for management to establish tracking of audit issue resolution.

A proactive audit follow up activity is particularly crucial to manage if different sets of auditors from different organizations have overlapping responsibilities, and thus exposure to the same finding. Where an Audit Committee hears the same vulnerability assessment year after year, the IT professionals in charge of supporting the corresponding process are targets for rebuke whether in the job for 30 years or 3 months.

3.4.2 Tracking Accountability

At the time an audit report is issued, it seems clear to the auditor what the finding is and which IT organization is accountable for addressing it. It is usually clear to the auditee at that point as well. However, if the vulnerability resolution takes six months to execute and there is an IT reorganization in month three, the vulnerability may get lost in the shuffle. A periodically scheduled query on audit remediation progress will bring attention to the fact that an audit remediation activity may be at risk of neglect.

After an IT reorganization, it may not always be clear exactly who in the audit report distribution list has accountability for addressing that finding. It may not be anyone in the original distribution. In some cases, all parties that received an audit report will act appropriately to create awareness of the item to be addressed during the reorganization, but the new person on the job will be too unfamiliar with the environment to understand the risks that have been identified.

In such cases, auditors will refer to the existing IT Control Framework, or seek an audience with the CIO to receive an update on changes to it. It is critical to any audit follow up process that IS auditors receive correct information on any new IT management process that may be utilized to focus on a neglected audit finding. Nevertheless, regardless of whether audit is able to make contact with a person accountable for remediating a past audit finding, it is always the current person with responsibility for the process that includes the corresponding control objective that should answer the periodic tracking query.

Where a neglected audit finding falls within the realm of responsibility of a new employee, an audit follow up process serves as a control environment initiation for that IT manager. Post-initiation, it is expected that a reprioritization for the neglected audit remediation will be effected.

3.4.3 To the Auditee:

For most IT professionals, the audit report is the most visibility they will ever get in their career. Occasional notice as the addressee of a report is not a bad thing because it calls attention to the fact that you are responsible for the smooth operation of critical information systems. However, repeated citations on audit follow-up memos may quickly become a situation where too much publicity is actually a bad thing.

Therefore, if there is not enough upper management support to resolve an audit issue, do not claim in the audit report management response that you will resolve it. Instead, identify the constraints you are under and defer the decision on control improvement to upper management. This way, the person’s name on the

periodic audit follow-up activity is not yours. If you honestly have no way to address an audit finding, this is not finding a scapegoat. This is placing accountability where it belongs.

Whenever you take a new job, one of the first questions you should ask is, “What are the outstanding audit issues the organization is accountable for addressing?” Once you have the answer, make it a priority to find out how much remediation work has been done to date and whether you can take advantage of an existing process or project to ensure that it finding not carry through into your administration.

4. Case Study

The foundations covered, the planning processes understood, and the audit execution steps grasped, the remainder of auditing can only be learned through experience. This chapter illustrates a sample set of experiences which occur in the course of a typical IS Audit. It provides an example of the audit process, following the previously described progression from management concern to audit report. If you are comfortable that you fully understand and appreciate the previous chapters, you may wish to skip the example and continue with the "To the Auditee" section which follows. However, the example is easy reading and serves to bring the audit process home in such a way that IT managers can see themselves in situations similar to those in the case study. The IT manager in the case study handles every challenge with appropriate professionalism and admirable expediency.

4.1 Management Concerns

4.1.1 Management Concerns

The company in the case study is a software services company: SoftServe, Inc. The company has three main lines of business:

- Outsourcing – Maintaining a client's systems environment in SoftServe's own data center, and providing telecommunications facilities for the client to access the software remotely.

- Deployment – Configuring and deploying software at a client site. Work is performed on a project basis, with specific due dates and deliverables per project.

- Consulting – Contracting where the work performed by SoftServe's consultants is managed by the client.

SoftServe has just deployed a new customer service application called CONE, which stands for Condition Online for Newest Effort. It is an on-line status review system where customers can review project details. Each line of business had its own version of what comprises project status:

- Outsourcing – number and type of systems deployed, current software and hardware versions installed.

- Deployment – project schedules, milestones completed, critical path issues status.

- Consulting – staff schedules, time sheets, expense report detail.

All the customers love SoftServe's CONE. The Outsourcing business even has a few major customers who would like to see it expanded. The expansion they have requested is to use the Internet to enhance an existing cumbersome change control process.

In the current process, to order a new system to be installed or to request an upgrade to their hardware or software, clients currently send email. SoftServe manually enters the request in a desktop change control system, then assigns it to a SoftServe engineer. The engineer contacts the client to request additional information, and fully documents the request. The documentation is then passed on to operations personnel, who open a ticket for it in their work order system, then call the client back to schedule the change. The larger clients feel that an interactive on-line change control system would allow them to make more efficient use of their engineer's time in communicating and scheduling changes.

The President of the Outsourcing business unit, Perry Presouts, asks a few of his top engineers to look into what changes would need to be made to the customer service application to provide an on-line interactive change control system. They deliver a report that outlines the systems development that would be necessary. The report contains a one-line caveat that concerns Perry: "The controls around the CONE application have never been tested. Assuming they are implemented as documented, they will be sufficient to protect the new application from unauthorized access."

4.1.2 The Audit Process

Anna Auddir, the Director of Internal Audit, has worked for SoftServe for three years. She is a Certified Internal Auditor and a Certified Information Systems Auditor. Anna is in the course of conducting executive

interviews aimed at putting together the annual audit plan. Perry Presouts is on her schedule to interview. She calls him. The gist of their conversation is this:

> Anna: “It’s that time of year again. I am putting together the audit plan and I need your help.”
>
> Perry: “Whatever I can do for you, Anna, I will.”
>
> Anna: “Would you have an hour or so on your calendar next week? I need to catch up with you on a few things and it would be easier to do it in person.”
>
> Perry: “Of course, let me see, how’s Tuesday?”

4.1.3 External Influences

SoftServe is a public company operating globally. It collects and redistributes customer data that it defines as defined as personal. SoftServe has a number of contracts with customers in which internal control requirements from an IT perspective rival those of the most strict regulatory agencies.

Perry’s recent engineering report and Anna’s annual phone would be enough to make him concerned about addressing risks with the planned new on-line interactive change control system. Moreover, he has a lot of choices on just how to address those risks as the system has not yet been designed. Perry contacts his legal staff to ask about SoftServe’s potential liability for accepting change instructions for customer’s systems that may have been entered by someone who hacked into a customer’s Internet account. Legal advises that the method used to accept customer’s Internet orders must be documented and agreed to by the customer via a digital signature, and the signature together with the order should then be archived on a Write-Once-Read- Many (WORM) device. They also advise that SoftServe must be prepared at all times to show that all documented internal controls are actually in place.

4.2 Audit Planning

4.2.1 Risk Assessment

When Anna shows up in Perry's office, she asks open-ended questions designed to get Perry to think about systems risk. The discussion proceeds as follows:

Anna: "When you think about all the systems required to successfully operate the outsourcing business unit, which of those thoughts keep you up at night?"

Perry: "I don't know, I guess it is that some10-year-old will hack into our new on-line interactive change control system and put in orders to make some change to our largest customer's payroll system.

Anna:"We have a new on-line interactive change control system? What do you call it?"

Perry:"Don't worry, you aren't that far behind, we have not implemented it yet. In brainstorming sessions, we've been calling it CUP, which stands for Customer Updates Projects. It goes with CONE, you know? The idea is to let customers use the Internet to put in change orders so they get done faster."

Anna:"I understand that it would not be a good thing for a 10-year-old to hack into it. What damage could one do?"

Perry:"Oh, only that we might accept the order as valid, implement it, with the result that SoftServe is sued by the customer for rendering them unable to meet a union payroll date or some such other media event. The long term impact of this type of incident would be devastating as the company relies on its reputation as a tightly controlled systems environment to retain existing customers as well as draw new ones."

Over the course of the week, Anna has similar conversations with other business unit presidents. Back in her office, Anna summarizes those conversations for Ian Itaud, SoftServe's manager of IS audit. Ian uses her information as input to a technology risk model. His first draft is in Figure 4.2-1.

Ian Itaud shows Anna Auddir the risk model. She points out that the model allows a system that affects business continuity to possibly never be reviewed. They discuss the fact that the Scheduling Time, and Expense system is critical to one of the three business units, but the current model may have it miss being audited until its reputational or perceived risk increases. They decide to change the weighting algorithm of the Last Audit column. If the number of years is none, the weight is now 10. They then discuss the Voice Telecommunications system. Simply because none of the interviewees expressed concern about it, it may escape being reviewed, potentially forever. They decide that, given that the perception value is entirely subjective, it should not be given equal weight with reputational risk. They decide that instead it will be the insider's view of reputational risk, and it will contribute to 10% of the reputational risk number. Ian revises the Technology Risk Model. He attaches it to an email to Anna, with this explanation:

From: Ian Itaud (IS Audit)

To: Anna Auddir (Audit)

Subject:Technology Risk Model Draft

Attachment:TechologyRiskModel.xls

Based on my research into the systems environment at SoftServe, I have classified each system into one of 10 categories. I have reviewed each business units' usage of each category and assessed their need for the category for business continuity. I have also reviewed the audit history for each system category. I have combined this research with your interview notes, and attempted to quantify the risk involved in each system category. The attached spreadsheet shows the Technology Risk Model created through this analysis. If our systems audit approach will be based on this risk model, this year we will probably review Internet Systems, Data Telecommunications, Billing Systems, Backoffice systems, and Voice Telecommunications. Please let me know whether you would like me to continue this analysis or to consider it complete.

Regards,

Ian

Anna Auddir then forwards this email individually to the CIOs of the three business units, with a personal note. For example, to Olivia Outcio, the CIO of the Outsource business unit, she sends this email:

From: Anna Auddir (Audit)

To: Olivia Outcio (Outsource)

Subject:FW: Technology Risk Model Draft

Attachment:TechologyRiskModel.xls

Olivia:

Attached is a draft of the Technology Risk Model upon which we will base this year's systems audits. I'd like a chance to discuss it with you to see whether it is compatible with the control framework with which to view your systems.

I'll be in your building Monday and Wednesday of next week, and Ian will be with me Wednesday. Is there a chance we can get on your calendar?

Best Regards,

Anna

4.2.2 Review Areas

Olivia Outcio, Anna Auddir, and Ian Itaud meet in Olivia's office the next week. Together, they look at the Technology Risk model. Their conversation goes like this:

Olivia: "I never thought of business continuity being dependent on the Corporate Internet Systems. After all, we've been in business for many years without them."

Ian: "That was a hard judgement call. I based the decision on the fact that many of our competitors are offering this type of real time data to our clients. Our existing way of sharing this type of data with our clients is monthly reports and weekly status meetings. The Internet systems are the only way we share that data real time. So I decided that we had better start considering those systems as necessities rather than something that it is nice to be able to offer. In the case of your business unit, we are being asked to

view potential new Internet offerings as part of the Internet systems. One of the new offerings could replace the existing change control systems, so that makes the business continuity connection more clear."

Olivia"From that angle, you are right, but currently, all that is out there are status reports that we now run daily instead of monthly. We could be faxing those if we had to. But it seems like a good idea to see if we can rely on the Internet systems. So what kind of review do you expect you'll do on those systems?"

Ian pulls a cardboard chart out of his notebook labeled, "Industry Standard IT Control Objectives" and hands it to Olivia (see Figure 4.2-2.).

Ian:"We thought we'd look at the industry standard systems control objectives and identify where we at SoftServe had the most need for controls. This chart covers it all. Is there something you have documented that starts at this high a level description of the control environment, but that also would provide the right framework with which to observe the controls around the Internet Systems?"

Olivia hesitates as she studied the control objective list. The she turns to her terminal and clicks on a few links, the first click is the Web Page depicted in Figure 4.2-3.

Olivia:"Perhaps the organizational process flow? And I also see some things in here that would be reflected in the quality metrics. You can find both of those on our Intranet web page."

Anna:"This will definitely help us plan all our reviews!"

Ian:"I see that under the quality indicators, there is a separate section for systems containing sensitive data, why is there a separate quality process?"

Olivia:"Oh, because if there is sensitive data, we require that the developers incorporate our consolidated access control system into the code so clients can use our centralized access control server. I was going to mention that in your system categories, you have some non-sensitive systems that overlap with sensitive ones. I would have thought for audit purposes, they maybe should be separate."

Anna:"That's exactly why we are here, to see if our approach makes sense to you. What do you mean?"

Olivia:"Well, some back office systems, like AR and AP, we treat as sensitive because of the assets they control, and others, like the GL, we control entry into, but we let a lot more people have access. To lump them into a group as equally in need of review may not be appropriate. There is a similar incongruity within the set of all Scheduling, Time and Expense Systems."

The three of them continue to analyze the risk model. After similar meetings with the other two business unit CIOs, the model ends up looking like Figure 4-2.4. Anna brings the Technology Risk model to the audit committee planning meeting. It is decided that the Internet systems will be reviewed as part of the annual audit plan.

4.2.3 Controls

Ian now has his marching orders. He hits the Internet in search of best practices with respect to controls for Internet Systems. He finds that they range from very comprehensive technology management strategies to minute detail on configuration parameters for vendor-specific software. The level of generality he is looking for does start with the management strategy, but he does not yet have a comprehensive list of all the vendor software used in SoftServe's Internet Systems.

Nevertheless, Ian has enough information to map industry standard control objectives to control best practices in the management strategies and corresponding operational procedures for Internet Systems. He leaves the detail on how to test each control activity for later. For now, he spends his days mapping controls to control objectives and making sure he leaves no control objective uncovered. He starts to keep lists like the one in Figure 4-2.5.

4.2.4 Audit Program

For the next three weeks, Ian struggles with the control test procedures required to flesh out the audit program. He knows that the time devoted to the audit will not allow him to review every aspect of the Internet Services environment according to the strictest industry standards. His approach is to determine which basic requirements were most relevant to protecting against the greatest risks to the Internet Services environment at SoftServe. He decides what is important for him to cover for SoftServe is requirements for Confidentiality, Integrity, and Availability of the Internet Services. He reviews this decision with Anna Auddir, and she agrees.

Ian then must decide specifically which control objectives and associated activities contribute the most to the confidentiality, integrity, and availability of SoftServe's Internet Systems. He consults the COBIT chart in Figure 4.2-6. The chart is meant to illustrate the information criteria that are impacted by activities that contribute to the COBIT high level control objectives. He uses the chart in reverse. He selects the high-level control objectives that are primary or secondary in meeting his criteria of Confidentiality, Integrity, and Availability. He folds into his program all the COBIT detailed control objectives that correspond to the high level criteria he has chosen. He uses his research notes to identify the control activities that correspond to the control objective. He creates audit steps to test for those activities. He develops an audit program. He sends it to Anna Auddir. His draft program is too large to appear as a figure, so it is included as Appendix A.

Anna marks up Ian's program with changes. The most significant one is that she wants him to add the control objective of "Educate and Train Users" and "Assist and Advise Customers." Though these are not primary for Ian's criteria, Anna knows that it is very important for legal and regulatory reasons that users are informed and aware of the consequences of their activities on SoftServe's Internet Systems. Ian incorporates her changes.

He organizes his program according to the control objectives, control activities, and test procedures as best as he can given what he has been able to learn about the environment. However, he finds that he lacks detail on a few of the systems. For these, his audit tests appear as nothing more than placeholders. Nevertheless, he completes a draft.

Anna reviews it but she is not familiar with the Internet Systems Technology so she does not feel comfortable approving it. However, she has an information systems risk consulting group with expertise in the area on retainer just for events such as this, so she passes it by them. After a few comments and corrections, the draft is approved. Ian gets the nod from Anna to start the audit.

4.4 Audit Execution

4.3.1 Preliminary Data Gathering

Ian starts by calling Olivia to find out the name of the IT manager assigned to maintain the Internet environment for the Outsourcing business unit. It turns out to be a cross-business unit IT services division managed by Mike Manager. Ian writes Mike this email:

> Mike,
>
> I am conducting an audit of the Corporate Internet Systems at SoftServe. As the environment is managed out of your organization, I hope you will provide me with a description of the system architecture. For each system that provides data or services to the Internet, please send a network connectivity diagram, and a description of the operating system and software applications loaded on each machine. I expect to begin the audit three weeks from today.
>
> If you have any questions or concerns, please to not hesitate to call. I am available by phone (212-555-1234) or email (iitaud@softserv.com).
>
> Best Regards,
>
> Ian Itaud

The email invites the Mike to call, so Mike picks up the phone. The conversation goes like this:

Mike:"Why an Internet review?"

Ian: "Pretty much because of the plans for expansion. Not because there is anything particularly risky about the current environment."

Mike: "How do you come up with control objectives for what is not there yet?"

Ian:"For systems under development, we usually work with industry standards and apply them to the planning and development stages of the project. But I still have to do a little research on the specifics of the technology to make sure that our program covers the risks in the new Web access application. By the way, do you have a technical design diagram that you could send?"

Mike:"Of course, I'll send a diagram. But the person who knows the most about that is Eileen Engineer. Feel free to call her direct, extension 7654. So do you have the list of the audit tests you expect to do on the systems?"

Ian:"They are due to Anna by April 28, so definitely by then. I am finishing up a rather large review of our new acquisition but I am sure I will be on target with that deadline.

Mike:"How's the acquisition working out?"

Ian:"Oh, very well, everyone is really pleased."

Mike: "That is good news. But about those control tests, we've been doing quite a bit of standard setting here. I'd really like to take a look at your industry standard control objectives

to map them onto our practices before you start. Do you think you could email them to me for comment before you finish them?"

Ian:"All the control tests will not be complete until a day or two before, but I'll bring it to the opening meeting. That's May 6. I'll bring a couple of copies."

Mike: "And the audit program as well? I was hoping to get that so I could judge the amount of effort that will be expected of my staff."

Ian:"Of course. That I can send now."

Mike:"Great. So, you'll be here May 6. You know, it seems your schedule is running tight and we have a major deployment that week. What would you say to coming the week after?"

Ian:"I'd love to postpone, but I will have to take a close look at the schedule before I can commit. It would certainly make it easier for me to get you advance copies of the control objectives. I'll let you know."

Mike:"Thank you, that would be a relief, and I'd be happy to write a letter expressing my concern with the deployment if it will help. By the way, how long do you plan to be with us?"

Ian: "Two weeks, tops. We'd like to get out by the middle of the second week. Will you be in the office the whole time? We usually try to schedule a closing meeting before we leave the site."

Mike:"Oh I wouldn't dream of missing it. That reminds me, I will need to make sure I have enough administrators on call. If you need anyone exclusively, I need at least 48 hours notice to put someone on schedule."

Ian:"No problem. At the opening meeting, we'll set a fieldwork schedule for the whole two weeks. We should have a very good idea of how much systems time we'll need by then."

Mike:"Systems time, that reminds me, do you plan to run audit software on my systems?"

Ian:"Well, we do have a few audit tools we run. Simple query programs. I'll need to know the operating systems versions in the scope of the review."

Mike:"No problem, send an email to Allen Admin for any operating system info you need. Now, I don't mean to give you an obstacle, but last time someone loaded audit programs on our systems, we had users calling to complain about slow response time. You'll need to schedule in some time to run those on a test system first. Better yet, ask Allen to do it for you before you come. I'll make sure it gets done."

Ian:"Great. That will save us time. Thank you, I'll send it in advance. Is Allen the person to get policies and procedures from as well?"

Mike: "No, but I'll see that you get them. What's your email address?"

Ian Itaud gets link to a website containing documentation in email from Mike Manager. He then calls Eileen Engineer to figure out how to interpret it. They have a long technical conversation that starts out like this:

Ian:"Hi, I am Ian Itaud from IS Audit. I am doing an audit of the Internet Systems and Mike Manager gave me your name for architectural questions."

Eileen: "Sure, Mike mentioned that to me the other day. What can I do for you?"

Ian: “Well, I was a little unclear of how the components worked together from reading the architecture description on the website. Can you describe the mechanism by which the web application connects to the database?”

Once Ian has finished reviewing all the material on the website, he has a list of operating system platforms and third party software that comprises the Corporate Internet Systems. These overlap with some has some audit programs he wrote the previous year, and he looks closely at the software version numbers and administration procedures to make sure they did not change.

He sends the audit program to Mike Manager via email and schedules an opening meeting.

4.3.2 Fieldwork

4.3.2.1 Opening Meeting

The opening meeting is held on a Monday morning. It is attended on the IT side by Mike Manager, Eileen Engineer, and Allen Admin. From the audit side, there is Ian Itaud, and two audit staff members: Sue Senior and Joe Junior. Together, the attendees step through the audit program. They look at a diagram that Eileen brought, depicted in Figure 4.3-1. Ian asks Ellen some questions and marks up the diagram with her answers as in Figure 4.3-2. He also keeps a notebook where he labels the first page, “Opening Meeting.” He is careful to record the date, time and meeting attendees so that the diagram notes will be sufficient to provide evidence that they were received in the course of the opening meeting discussion. He takes more detailed notes in his notebook, as all three auditors will do throughout fieldwork.

At the end of the discussion, Ian lists the systems that fall within the scope of the review. The list is:

UNIX machines – proddb1, proddb2, prodweb1, prodweb2

Firewalls - fwint1, fwint2, fwext1,fwext2

NT machines – Administrator workstations on the Network Management network

Routers – rtrint1, rtrint2, rtrext1,rtrext2, choke router on network management network

Ian asks Mike how he came up with this particular architecture and whether he assessed risks with respect to these systems. Mike pulls from his notebook some high level planning documents he used at the early stages of the project. They spend a few minutes discussing how the documents were generated. Then they put together a schedule for the first week of the review.

Monday PM tour physical location of equipment in scope with Barb Building, Mike will introduce Barb after opening meeting

Tuesday AM Sue to interview quality assurance director and development project manager on change control process - Quinton Quality and Donna Developer

Joe to interview review IT acquisitions process - Mike to provide contact

Tuesday PM review firewall and router configurations with network operations center - Allen Admin will coordinate

Tues Evening run network scans on production environment from Internet and internal network

Wednesday test audit software on test UNIX server and NT workstations – Allen Admin

Wed Evening run audit software on production environment – Allen Admin, Eileen Engineer

Thursday observe operating procedures with Allen Admin's staff

Thurs evening run database audit software with database administrators – names to be provided by Mike Manager

Friday review business recovery plans with Bob Backup

They agree to meet again on Friday afternoon to measure the progress and to schedule the remaining time on site. They also schedule a pre-closing meeting for Thursday morning of the following week.

4.3.2.2 On-site Testing

Interviews and testing on Tuesday proceed. Wednesday morning, Allen Admin, Sue Senior, and Joe Junior get together to run the audit software on the test system. Sue gives Allen a floppy. Allen scans it for viruses on the test NT workstation. Sue points out that one of the files contains the UNIX audit software. Allen transfers the file across the network to the test UNIX machine.

The other file on the floppy contains an NT executable that they run from the floppy. The results are stored on the floppy by the program. Results contain the configuration of the machine, its user list, its network routes, and other parameters relevant to assessing the controls in the environment.

The UNIX software is a bit more complicated. As a precaution, Allen first runs some security software that does a file integrity check on the test machine. He explains to Sue and Allen that he will run the software again after the test is complete to see what effect the audit software had on the file system, if any. He then carefully reads the audit software install instructions, and demonstrates to Sue and Joe that he is executing the installation process as instructed. When the installation is complete, Allen checks to see who is logged into the test machine and finds that Donna Developer has an active session. Allen then calls Donna Developer to let her know that they are running unknown software on the test machine. Donna asks that they wait a few minutes because she is in the middle of compiling a critical piece of software. Although there is little risk that the audit software will interrupt Donna's compilation process, Allen agrees. Allen, Sue, and Joe go for coffee.

The audit software is finally run on both the UNIX and the NT systems. Unfortunately, one of the steps on the audit plan the software was meant to address does not work on the version of the UNIX operating system that they are running. The step is:

> *Check every user account on the system to see if there are any accounts that (i) have not been accessed in 90 days and (ii) are not as yet disabled.*

So Sue Senior requests a login to the system so that the step can be executed manually. She intends to accomplish the audit step by having Joe Junior view the relevant user account files, checking the users one by one. Allen Admin tells Sue Senior that Mike Manager will have to approve that access. He leaves Sue and Joe in a conference room, and goes back to his office. He calls Mike and informs him of the request. He points out that any system login that has permission to view the user account file may also write to the account file and to other configuration files. Allen and Mike discuss changing the permissions on the file for the duration of the audit. But that alternative will leave the user account file writable by other users who are not system administrators. Neither alternative is acceptable to Mike. Mike asks Allen to be creative and try to come up with another alternative.

Mike looks at his calendar and schedules a meeting with Sue and Allen for the next morning, Thursday. He had purposely left blocks of time available on each day of the audit for just such an event. Sue brings Joe to the meeting. The conversation goes like this:

Allen: “I hesitated in giving you access to the production system yesterday because there is no way to give you the on-line access that you want for the audit without compromising the integrity of our system. But I have an alternative. Would it be ok if we gave you the system account files that you need to see on a floppy disk so you can look at them on one of our PCs?

Sue: “I understand the hesitation you have in providing administrative access to productions systems. But the suggested alternative does not work for us. Unfortunately, files on a floppy could have come from anywhere and I do need to verify that the account files we are looking at are actually those that control access to the system. Though I do not doubt for a minute that you would make every effort to deliver the files totally intact, I would have no objective evidence that the files actually came from the account configuration directories of the systems in scope. Suppose instead that we view them on line but have someone from your group look over our shoulder to make sure that we don’t inadvertently enter any commands that will have an adverse affect on the system? We have already scheduled observation of operational procedures for today.”

Mike:“How much time it will take to complete those audit steps?”

Sue:“Joe, since you will be the one looking at the account files, how long do you think it will take you to get through them?”

Joe:“Oh, at least an afternoon, so let’s say approximately 4 hours.”

Allen:“I am afraid it will be impossible for anyone in my group to spend that much time in one sitting this afternoon. Because there were so many different operational procedures you wanted to review, instead I had scheduled people to be available on a rotating basis depending on their skill set.”

Sue:“How much time did you intend to be devoted in one sitting?”

Allen:“About a half an hour, give or take.”

Mike:“Suppose we do it this way. Joe, if somebody copied some files across the network, would you know enough to recognize what directories on what machines they were coming from and what directories on what machines they were going to?”

Joe:“For UNIX and NT machines, yes.”

Mike:“OK, then why don’t you supervise one of Allen’s system administrators in copying the relevant system account files to a floppy disk. Observation of the copying process qualifies as evidence that the files do in fact come from the system itself, right Sue?”

Sue:“Yes, that’s a great idea, then we can look at them at our leisure. Thank you.”

Mike:“Good, so now that that’s resolved, let me use our time together here to get some status of the efforts here. Find anything yet?”

Sue:“Well, I was a bit concerned during the physical access tour that I was able to get into the computer room without signing in. It looked to me like the visitor procedures are not being followed.”

Mike looks amazed. He calls Barb Building on the speakerphone.

Barb: “SoftServe. Barb Building here.”

Mike: “Barb, how come Sue got into the computer room without signing in?”

Barb: “Don't you remember Mike? You introduced her to me and personally ok’d her access. After all, she is here to test our controls so I figured that was as good as a job function requiring computer room access. The only people who don’t get cards are those whose job function doesn’t normally require access.”

Mike: “The procedure is that everyone who doesn’t have a their own access card signs in, regardless of their job function. Just because I approve the procedures, don’t make my requests exempt from them! Now Sue thinks we let people who don’t have access card keys of their own in without keeping track of who they are!

Barb:“What?! I can prove that every other visitor in the world signs in! Sue could come down to the computer room look at every person in the computer room right at this minute and find only people with access cards and contractors who were made to sign in. She can look at the sign-in log going back three years and correlate that with all our visitors!”

Sue:“The on-the-spot visitor inventory and sign-in log may be enough evidence that there is a control, even though I somehow slipped through it. Joe, will you go down to the computer room and work on that?”

Joe:“OK. Barb, will you meet me at the door?”

Barb:“Definitely, and this time you’ll sign in!”

Everyone laughs as Joe leaves the room.

Mike:“Ok, now that that’s resolved, find anything else?

Sue:“No, that’s the only concern I have so far, though I may not have completely analyzed all the evidence we’ve collected so far. The firewall and choke router rules are pretty complicated.”

Mike:“That’s fair. Are you getting all the evidence you need, or are you waiting on anything?”

Sue:“I think we now have all the contacts we need, thank you for the email. We did get in touch with Denise Database, so we are on for the database testing tonight. We were supposed to meet with Quinton Quality Tuesday, but he was out sick and isn't back yet. I was planning to ask you if there was someone else we could talk to instead.”

Mike:“I would really rather you waited for Quinton but if he isn’t back by next Tuesday, I’ll go over the change control process with you myself. How’s that”

Sue:“Sounds good to me.”

Mike:“So other than that, is everything still on schedule?”

Sue:“Yes, everyone has been very cooperative, thank you.”

Fieldwork proceeds. Friday afternoon, Mike Manager, Eileen Engineer, and Allen Admin, Ian Itaud, Sue Senior and Joe Junior attend the scheduled status meeting. Though very pressed for time, Ian manages to prepared a brief status update of the auditors’ progress through the audit program, see Figure 4.3-3.

Mike:“It looks like you are uncomfortable with our change control procedures. Did you get ahold of Quinton?”

Ian:“Yes, we did, yesterday, and Quinton took us through the process, which is definitely a good one. Our only concern is that, in his absence, there was no one that seemed to have any experience with it. In an organization this size, it seems a bit shaky to be that dependent on any one individual. We just made note of it to share our opinion with you. As changes in the Internet Services systems are not that frequent and usually not that urgent, we don’t consider it an audit finding.”

Mike:“What here is an audit finding?”

Ian:“Two concerns so far with systems security. One with administrative access and one with the application access to the database.”

Mike:“Details, give me details.”

Ian:“Well, you allow the root user to log directly into the machines to perform administration tasks. Since more than one person knows the password to that account, you have no way to track which individual was logged in at a given time.”

Mike:“Allen, how many people know the root password?”

Allen:“My group, six people. They have to know it to get their jobs done.”

Ian:“But they don’t have to login directly. They could login with their own ID and use the UNIX switch user – su – program to become the root user. Then their access to the administrative account is logged.

Allen:“But once they are root they can erase the logs anyway, if anyone wanted to be malicious, making them know two passwords to become root won’t save us.”

Sue:“True, but you can design security detection mechanism that will let you know if the logs are tampered with. You can also use security tools to configure the su process to allow authorized users without having them use a second password. The idea is to make it difficult and detectable for someone to subvert controls. Now it is too easy for someone to deny making unauthorized system changes. There is no way to distinguish one administrator’s activities from another.”

Mike:“Eileen, do we have any automated processes that login as root? Does anyone but Allen’s group need this feature?”

Eileen:“No. We could make them start using su tomorrow and it would not affect operations. However, I will probably want to evaluate some of the security tools Sue is talking about for a longer term solution that may be easier to manage.”

Mike:“Sure, of course, but I see no obstacle to seeing if we can get started now. Allen, make the change in our test environment tonight. See what happens. If it goes smoothly, we’ll put it into production next week and show it to Ian here before he leaves. If we do that Ian, does it come off the report?”

Ian:“Yes.”

Mike: “Good, what else you got?”

Ian:“A database control issue. The way the web application is developed, all database users use the same password. The developers code it into their applications. It is sent in clear text through the network. We are concerned for two reasons. One, that it might not be strong enough authentication. Two, that as developers leave the firm, or code is ported within the firm, the password becomes exposed. Sue needs to spend more time to really define it, but since you asked what we’ve found, we thought we’d let you know there may be something there.”

Mike:“Hhhmm, are you working with Denise Database on that?”

Sue:“Yes, and Donna Developer.”

Mike:“Tell you what, let’s have Eileen sit with you after this meeting to get a clearer idea of the concerns. Maybe she can help define what the control issues may be. Next topic, for what else can I provide clarification?”

Ian:“Well, everywhere there is a question mark in this status, we have not yet found the right person to speak with on an issue. Perhaps you could point us in the right direction?”

They then put together a schedule for the second week of the review:

Mondaytour off-site storage and both internal and external recovery facilities

Tuesdayreview and analyze metrics collection and management reporting process

Wednesday perform follow-up tests and interview, prepare high-level findings list

Thursday pre-closing meeting and follow-up activity

Fridayclosing meeting

4.3.2.3 Closing Meetings

By Thursday morning, the database issue is clearly defined. Unfortunately, the vulnerability is part of the architecture of the deployed application and cannot be immediately fixed without a full development QA test cycle. Eileen Engineer has had off-line meetings with Denise Database and Donna Developer and reported to Mike Manager that they are having trouble agreeing on an architecture that can be deployed quickly. Donna Developer wants to make the change as part of the new release that is due out in two months. Denise Database says it can be done more quickly, but that she would need to hire an expensive consultant to get the job done without delaying her current projects. She would also need Donna Developer to create a patch to the deployed application.

The preclosing meeting is attended by Mike Manager, Eileen Engineer, Donna Developer, Denise Database, and Allen Admin, Ian Itaud, Sue Senior and Joe Junior. Ian distributes a bullet list of preliminary findings:

- Direct root login
- Application database access issue
- Database backup vulnerability

They discuss the first two issues, which they are already familiar with. The root login problem has been fixed and they schedule a time for the afternoon for Sue and Joe to verify that. Mike has brought Donna and Denise to the meeting so they could discuss with Ian and Sue their ideas for correcting the database login vulnerability, and to hear from Ian and Sue how other organizations with similar applications have approached the issue. Mike finds that the discussion is helpful, but that the issue will undoubtedly appear in the auditor's report. The they discuss the new item:

Mike:"What is the database backup vulnerability?"

Ian:"The database files are dumped to a disk and backed up to tape. But the recovery timeframe does not meet the control objective that reads: 'The continuity plan should identify the critical application programs, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs.' The audit step that failed was: 'Review software and data backup and restore procedures to verify that recovery from backup is possible within predefined minimum recovery time intervals.'"

Denise:"But we don't really need the tapes, that database is replicated to our Chicago office."

Mike:"I should have caught that in your audit program. The control you outline to meet the objective is not necessary in this case because we have a compensating control. The replication process. Will you have some time this afternoon to let Denise show you how that works?"

Sue:"Of course."

The Friday closing meeting is attended by Olivia Outsource, Mike Manager, Eileen Engineer, Ian Itaud, Sue Senior and Joe Junior. Most of the time in the meeting is spent explaining the application database login problem to Olivia.

4.3.3 Audit Report

Two weeks later, Ian issues a draft report and sends it to Mike. The major finding appears in Figure 4.3-4. Mike forwards it to Olivia. They discuss Ian's recommendation versus Mike's ideas for addressing the vulnerability. Once they are agreed, Mike calls Ian.

Mike:"Ian, we've been working on that architecture since you were here and we believe we have a solution. Its not exactly yours, so I'd like to pass it by you before committing to it if that's ok.

Ian:"Sure, what did you come up with?'

Mike:"We've provided an individual database login for each user. Using records from our provisioning system, we have limited each user's database access to just what that user should be able to see. The password is the same as the web login and the application encrypts it upon login and programmers have a routine that decrypts it when the user requests data. It never writes it to disk. We think it is a major improvement."

Ian:"Sounds good to me. If you send me a technical specification, I can probably confirm that opinion."

By the time the report is issued, Ian has endorsed Mike's approach to resolving the issue. The audit report is published as in Appendix B.

4.3.4 Audit Remediation

Two weeks later, Ian is updating his list of IT issues for the quarterly meeting of the Board of Directors. Though Mike's issue is too new to appear in the actual presentation, it does appear on the tracking list. Ian reflects that he used to keep the list in a word processing file, but over the five years he has worked at SoftServe, it has grown too unwieldy to manage in text format. He now keeps it in a database. The database schema for the latest finding is populated as follows:

IS AUDIT NO: 423

BU:Outsourcing

AUDIT AREA: Internet Systems

DATE:XX/XX/XX

MANAGER: Mike Manager

STATUS: Open

FINDING: Database password vulnerability

RESPONSE: Software development project #324243

RESOLVE DATE: YY/YY/YY

Once all finding from this quarter are entered, Ian does a query on the database:

```
select * from FINDINGS where (Resolve Date > 90 days past) and (Status = Open)
```

He cuts and pastes the result of this query into his presentation to the Board. On his way to join Anna in the Board Room, he makes each Board member a copy of the original audit report, all follow up memos he had sent this quarter to the managers responsible for addressing the findings, and also a chronicle of the latest management responses.

4.4 To the Auditee

IT controls are a logical outcome of the growth of automation. Management oversight of IT activities is a logical evolution from management oversight of accounting functions. Your stewardship responsibility is obvious to the auditor, but may only become obvious to you or your staff in the course of the audit process. The IT professional who understands that IT risks are faced daily whether or not there is an auditor in attendance is prepared not only for the challenges of meeting an auditor, but for the challenges of fiduciary responsibility in general.

Of course, IT professionals have long been on their own quest for controls to address management concerns. This is evident in the establishment of quality assurance departments and segregation of duties within IS job functions. The introduction of IS policies has been driven by the need for control around IS processes. The expansion of audit from just the financial system to the entire systems environment is an effort by IT-aware management to establish that controls are in place to reduce business risk.

You benefit from the audit planning process. It is clear that the auditor has different assumptions and expectations concerning the audit. Nevertheless, there are areas of common concern. A shared systems control framework enhances communication of these concerns. This shared framework produces agreement on review areas, for review areas present themselves through the consideration of risk involved in the control framework. The variety of possible review areas demonstrates the varying detail by which an audit may initially be planned.

From a review of risks in a given review area, it is a short leap to establish control objectives to minimize those risks. This focus on minimizing risk in turn leads to a critical analysis of methods to minimize risk, or to a focus on individual controls. As you are responsible for the integrity of the systems under review, your initiative in defining control objectives and associated controls significantly influences the course of an audit.

The focus on control objectives and the identification of supporting controls leads to examination of evidence that controls are in place. For auditors, the examination process is facilitated through audit programs. The design of an audit program demonstrates that it maintains independence requirements and evidentiary requirements while allowing for the identification of compensating controls. Audit programs contain detailed audit steps to provide both educational value for the junior auditor and the maintenance of quality standards in audit workpapers. For you, audit programs are a road map to the maze of activity that surrounds you during the course of an audit.

From the first letter or phone call from an auditor to the receipt of the final report, you are given the opportunity to participate in the risk assessment process. The opening meeting, fieldwork, and the reporting process all introduce opportunities for you to contribute perspective on the risk model, the audit program, and the control objectives under review. To emphasize and elaborate on the positive behavior exhibited by the IT professional in the case study, you should:

- Accept the validity of the exercise as a management tool.
- Review the audit plan and understand the auditor’s strategy.
- Coordinate your organization’s response the audit process.
- Use the reporting process to demonstrate your organizational strengths.

Such behavior will not only help you get through the audit, but it will identify you as a valuable player in the field of IT Management.

Show yourself capable of accepting stewardship responsibility by maintaining a strong yet flexible ICS. Even if it proves inadequate to mitigate an audit-identified risk, control mechanisms must be created (effected) before they can be revised (affected). The point is that mechanisms that effect control implementation are more easily revised than created. In the context of the executive management concerns described in the first chapter, you will be viewed as an IT professional that can in general handle fiduciary responsibility.

Appendix A

Draft Audit Program for SoftServe Internet Services

These high level control objectives:	are expected to be implemented via these control activities:	and will be tested by executing these audit steps:	Evi-dence	Pass /Fail
Define the information architecture	IT Management's plan for managing Internet Systems information is well defined and well rooted in business requirements.	A data dictionary exists for all critical business information.		
		Data ownership principles are well- defined and supported by documented business requirements.		
		Data ownership models are supported with strategic information architecture.		
		Security tools and techniques are consistently and uniformly specified in support of data ownership models.		
		Security administration techniques allow business users to make decisions on data access.		
		Interview business users authorized to grant access to data to verify that they understand data ownership models and their stewardship role.		
Assess risks	Management should establish a systematic risk assessment framework. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. The process should provide for risk assessments at both the global level and system specific levels (for new projects as well as on a recurring basis) and should ensure regular updates of the risk assessment information with results of audits, inspections and identified incidents.	Obtain an understanding of management's risk assessment framework with respect to IT.		
		Verify that management's risk assessment framework include appropriate metrics with which to assess level of business risk in Internet Service offerings.		
		Verify that management's risk assessment framework contains an appropriate variety of independent information sources.		
		Verify that management's risk assessment framework includes a methodology for folding in new projects and new information about existing projects.		
		Verify that management's risk assessment framework has been reviewed and, if		

		necessary, updated within the past twelve months.		
	Management should establish a general risk assessment approach which defines the scope and boundaries, the methodology to be adopted for risk assessments, the responsibilities and the required skills. The quality of the risk assessments should be ensured by a structured method and skilled risk assessors.	Review management's approach to assessing the risk to the business presented by Internet Services technology.		
		Verify that management's risk assessment approach defines appropriate scope and boundaries.		
		Verify that management's risk assessment approach includes a well- defined and documented methodology.		
		Interview management's risk assessors; determine whether their skills and experience are appropriate to the task.		
	The risk assessment approach should focus on the examination of the essential elements of risk such as assets, threats, vulnerabilities, safeguards, consequences and likelihood of threat.	Verify that risk identification includes an accurate depiction of assets available through Internet Services.		
		Verify that risk identification includes an accurate depiction of threats to Internet Services assets.		
		Verify that risk identification includes an accurate depiction of vulnerabilities inherent in Internet Services offerings.		
		Verify that risk identification includes an mapping of safeguards to threats that is based on the severity of the threat and the probability that the threat will be enacted.		
	The risk assessment approach should ensure that the analysis of risk identification information results in a quantitative and/or qualitative measurement of risk to which the examined area is exposed. The risk acceptance capacity of the organization should also be assessed.	For each Internet services offering, obtain the measurement of risk identified with exposed areas.		
		Verify that the measurement of risk to relevant exposed areas does not threaten the business continuity of the exposed organization.		
	The risk assessment approach should provide for the definition of a risk action plan to ensure that cost-effective controls and security measures mitigate exposure to risks on a continuing basis.	Review the results of the risk assessment process.		

		Verify that the results of the risk assessment process include a determination of the cost required to reduce risk to an acceptable level.		
		Verify that there are affordable security measures to mitigate risks on an on- going basis.		
	The risk assessment approach should ensure the formal acceptance of the residual risk, depending on risk identification and measurement, organizational policy, uncertainty incorporated in the risk assessment approach itself and the cost effectiveness of implementing safeguards and controls. The residual risk should be offset with adequate insurance coverage.	Verify that risks identified by the process are appropriately assigned to business or IT management.		
		Review processes that ensure that significant IT decisions affecting the Internet Services environment weigh risks to the business of failed cost/ benefit analysis.		
		Verify that there is a plan to reduce each residual risk.		
		Verify that there is appropriate insurance coverage to mitigate the business impact of residual risk. Verify appropriate equipment, data, program, and/or media coverage, including replacement values, time limits for notifying insurance company about newly acquired equipment and coverage for equipment in transit or which is moved to a new location.		
		Assess risks of items and/or events excluded from coverage.		
Manage quality	Senior management should develop and regularly maintain an overall quality plan based on the organizational and information technology long-range plans. The plan should promote the continuous improvement philosophy and answer the basic questions of what, who and how.	Review the information technology quality assurance plan with respect to a new internet service offering.		
		Verify that the system development life cycle contains an appropriate level of detail to be immediately applied to the Internet Services Systems.		

		Verify that the system development life cycle contains steps for development, acquisition, implementation, and maintenance.		
		Obtain documentation defining IT management's monitoring process of the system development life cycle for the Internet Services Systems.		
		Identify the IT manager responsible for determining that Information Services quality standards and procedures are enforced in the Internet Services systems environment.		
	The organization's senior management should define and implement information systems standards and adopt a system development life cycle acquiring, implementing and maintaining computerized information systems and related technology. The chosen system development life cycle methodology should be appropriate for the systems to be developed, acquired, implemented and maintained.	Confirm that requirements definition and system design consider control and security practices.		
		Confirm that requirement definition and system design consider external regulations and laws.		
		Verify that the systems development lifecycle methodology is observed for the new offering.		
		Verify that management has appropriate authorization procedures for new deployments to ensure that systems development lifecycle methodology must be observed for the new offering		
	Senior management should implement a periodic review of its system development life cycle methodology to ensure that its provisions reflect current generally accepted techniques and procedures.	Obtain documentation with respect to the quality reviews ever performed on the Internet Services systems.		
		Verify that the quality reviews include an assessment of the quality of the techniques and procedures used in the Internet systems development lifecycle methodology.		
		Verify that the Internet Service systems development lifecycle methodology is appropriately updated as per the results of periodic review procedures.		
	Management should promote an organization which is characterized by	Determine whether standards for quality maintenance have been communicated to		

	close cooperation and communication throughout the system development life cycle.	the concerned staff and enforced		
		Determine whether process interfaces between IT and business drivers are adequate to collect requirements for the Internet Services systems.		
	Management should establish a system development methodology that includes feasibility, requirements, design, development, user & admin procedures, system testing, user testing, training, and transition issues.	Review the deliverable definition process to determine its adequacy in identifying and measuring the deliverables of a given project in terms of expenditure versus benefit.		
		Verify that the software versions used in the Internet Systems are up-to-date, or at least vendor supported indefinitely.		
		Confirm that the needs analysis that led to hardware and software selection included data size and structure, functional specifications, and performance requirements.		
		Review the process by which assets that are no longer needed are retired.		
		Verify that systems documentation includes definition of input files and variables, descriptions of reports, access procedures, control techniques, programming logic descriptions, activity sequences, and recommendations for segregation of duties.		
		Review types of training materials and/ or manuals to make sure that the needs of each affected community (users, programmers, operations personnel) are addressed.		
	The organization's system development life cycle methodology should provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programs created as part of every information system development or modification project.	Verify that testing documentation includes definition of input files and variables, access procedures, expected output logic descriptions, activity sequences.		
		Verify that appropriate tools control test case generation and maintenance.		
		Verify that appropriate tools support the regression testing process and that testing includes regression testing methodologies.		
		Verify that testing includes regression testing methodologies.		
		Verify that testing includes stress testing that mimics the expected production		

		environment.		
		Verify that test cases are constructed by sophisticated business users.		
		Review the process by which issues identified in testing are tracked, corrected, and incorporated into new releases.		
		Sample issues found in system testing and follow them through the process that ensures they are addressed.		
		Review documentation on test results to ensure an appropriate level of detail.		
	The organization's quality assurance approach should require that a post-implementation review of an operational information system assess whether the project team adhered to the provisions of the system development life cycle methodology.	Determine whether IT Management performed a post-implementation review to assess whether the project team adhered to system development life cycle methodology.		
		Determine whether IT Management performed a review to assess whether the IT targets for the internet service offering were achieved.		
	The quality assurance approach should include a review of the extent to which particular systems and application development activities have achieved the objectives of the information services function.	Obtain a list of metrics used by management to assess whether quality goals have been achieved.		
		For each system or set of systems under review. obtain an instance of the metrics defined for measuring quality.		
		Verify that actual system metrics may be used to assess quality in the manner expected by management.		
		Obtain copies of reports of quality assurance reviews, also review distribution lists.		
Acquire and maintain applications Software	Application software should effectively support business requirements.	Obtain copies of application functional requirements documents and verify that they are signed off by business users.		
		Verify that security requirements are incorporated into application requirements, not the subject of separate documents.		
		Review technical specifications for application programs to ensure that they are consistent with functional requirements.		
		identify where in the system development life cycle methodology the following system design issues are addressed: input, processing, output, internal controls, security, disaster recovery, response time,		

		management reporting, change control.		
		Review systems development lifecycle process and identify appropriate approvals to proceed are required for requirements, design, development, and deployment stages.		
		Determine whether application user help screens and help desk support process plans cover every aspect of functionality.		
		Determine whether requirements design specifications guarantee the accuracy, completeness, timeliness and authorization of inputs and outputs.		
	Application software design should make efficient use of IT resources.	Determine whether application architecture is supported by a strategic plan.		
		Verify that application architecture components are consistently reusable.		
		Observe the application user interfaces for consistency in look and feel.		
		identify system interfaces and ensure they meet security, availability, as well as functional requirements.		
		Review application data models for consistency with strategic information architecture.		
		Review technical specifications for application programs to ensure that they contain enough detail to allow programmers to be immediately productive.		
		Review application file system configuration and support procedures.		
		Identity the application testing standards and determine whether they are appropriate.		
Acquire and maintain technology infrastructure	Management should ensure that technology infrastructure components adequately support Internet applications.	identify the process by which Internet Systems technology infrastructure is decided. Determine whether the decision process includes feasibility, cost-benefit, and strategic planning.		
		Review the process by which system administration procedures are developed. Verify that it covers every technology component.		
		Verify that network protocols and paths are well-defined.		
		Determine whether hardware architecture is periodically reassessed and new developments incorporated into long term plans.		
		Verify that all infrastructure components have adequate maintenance contracts or inhouse maintenance capability.		

		Verify that all infrastructure components are designed for fault tolerance and automated recovery.		
		Review overall Internet Systems architecture for single points of failure.		
	Management should acquire technology infrastructure components in an efficient and effective manner.	Review the process by which technology hardware and software is acquired.		
		Confirm that the purchase order and receiving process are tied to an inventory tracking process.		
		Confirm that the purchase order, receiving process, and inventory tracking process include software license agreements.		
		Review the organization's policy and procedure with respect to open source software to ensure that its use, if any, is adequately supported.		
Develop and maintain procedures	Management should establish and maintain methods of producing procedures with respect to service levels, operational process, and end users.	Identify management responsible for the production and maintenance of procedures required to support the Internet Systems.		
		Determine whether requirements analysis, user feedback, and industry standards are used in the creation and maintenance of procedures.		
		Interview operators, administrators, and end users to determine whether documented procedures adequately address their needs.		
	The change process should ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.	Verify that planned procedure definition includes procedures for user administration, secure OS file configuration, secure DBMS table configuration, backup and recovery, and security and performance monitoring.		
		Verify that procedure definition includes instructions for updating copies of the procedures, and for creating awareness that new procedures are in effect.		
Install and accredit system	Management verifies that systems are fit for their intended purpose.	A test plan covering all areas of information system resources exists: application software, facilities, technology and users.		
		Implementation plans include test strategies and plans.		
		Testing strategies include user acceptance test in a pilot environment.		
		Implementation plan leaves time for correction following initial user acceptance testing.		
	Records of development effort demonstrate attention to requirements.	Application performance benchmarks reflect system sizing criteria.		

s		Data conversation strategies are incorporated into the development process		
		Operational tests are conducted with administrators, operators, and help desk personnel.		
		Pre-implementation reviews verify that security and regulatory requirements are adequately met.		
		The development of training materials is incorporated into the implementation plan.		
		Post-implementation reviews are conducted with end users.		
Manage changes	Management should ensure that all requests for changes, system maintenance and supplier maintenance are standardized and are subject to formal change management procedures. Changes should be categorized and prioritized and specific procedures should be in place to handle urgent matters. Change requestors should be kept informed about the status of their request.	Verify that change control procedures, exist, are current, and are followed. Randomly sample changes and compare to documentation that is produced according to procedure.		
		Verify that version control procedures allow continuous identification of system components installed in development, test, and production environment		
		Verify that all systems personnel understand how to implement changes according to a controlled process.		
		Review controls in place to prevent modification of a program after approval but prior to move into production.		
		Confirm that production changes are based on formally approved documentation, which is approved at an appropriate level by both the user/ customer and application development management.		
	A procedure should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.	Confirm that production changes are reviewed and approved by all operational groups that must support the environment to which the change is being made.		
		Determine if all approved changes are accompanied by a documented back-out procedure which is tested prior to deployment, and executed in the event of problems are encountered post-implementation.		
	Management should ensure that change management, and software control and distribution are properly integrated with a comprehensive configuration management	Review change control procedures and identify method by which all changes are subsequently accounted for (e.g., sequential prenumbering, logging request		

	system.	forms, source code control identifiers).		
		Review use of emergency modification procedures. Determine if controls ensure that emergency actions are monitored and tracked, and that changes are incorporated into all future program releases through the change control process.		
		Verify that configuration changes to network equipment are requested, documented, and audited. Ensure that they are incorporated in network diagrams.		
		Sample source code changes and ensure procedures were followed through tracing the audit trail.		
	Management should ensure maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorized access to automated systems.	Verify that maintenance personnel have well-defined job descriptions.		
		Verify that the job descriptions of maintenance personnel correspond to their system access rights.		
		Verify that it is not possible for any individual maintenance personnel to make system changes that are not monitored or traceable back to the individual.		
Define and manage service levels	Management should accurately set business expectations for system cost and performance through well-defined services levels.	Determine whether historical performance, user input, and industry benchmarks are used to create and adjust service level target.		
		Determine whether cost/benefits of alternative service levels were considered in define Internet Systems service levels.		
		verify that service level objectives take into account system security, availability, continuity planning, and capacity for growth.		
	Management should monitor system operation to ensure that service levels are met.	Determine whether the content and frequency of operational reporting is adequate to determine if service levels are met.		
		Compare actual system performance characteristics and compare to operational reporting for the same time period.		
Manage third party relationships	Procedures are established to ensure that third party services are performed as expected.	All contracts for third party services are supported by formal requirement definition.		
		All contracts for third party services are preceded by Requests for Proposals to multiple vendors.		

		All qualified request for proposal responses are thoroughly evaluated.		
		Legal, security, and regulatory requirements contribute to requirements for third party services.		
		Industry standards are considered in requirements for third party services.		
		Objective references are consulted in evaluation of third party services.		
		Measurable criteria are set for service agreements.		
		Legal contracts are in place with all third party service providers.		
Ensure systems security	Information Technology security should be managed such that security measures are in line with business requirements.	Obtain a copy of information security policy.		
		Verify that the security policy production process identifies and addresses IT risks.		
		Verify that the security policy production process identifies and addresses regulatory requirements.		
		Verify that IT requirements with respect to security measures follow policy.		
		Verify that security planning is integrated into the IT planning process.		
		Verify that the security implementation process identifies and addresses operational considerations.		
		Verify that decisions with respect to security mechanisms utilize accurate technology assessments.		
		Verify that procedures for access control and user authorization complies with policy.		
	Access controls should ensure that users are responsible for the use of their own accounts.	Obtain identification, authentication, and access granting procedures for the Internet Systems environment.		
		Verify that system administrators have procedures to protect administrative and generic accounts.		
		Verify that all users have hard to guess passwords		
		Verify that user passwords expire.		
		Verify that dormant accounts are disabled.		
		Verify that multiple attempts to guess passwords will lock an account.		
		If logon scripts are used instead of environment profiles to restrict the user's environment within the system determine whether reasons for using scripts are valid.		

		Ensure that passwords or stronger authentication mechanisms protect access to the configuration mechanisms of network equipment. Verify that the passwords are shared on a need-to- know basis.		
		Review procedures to deactivate any account which has not been used in 90 days.		
		Review method by which user is given an initial password. Ensure that is it is verbal, with prior authentication of user identity. Ensure that the user is instructed (or forced, system permitting) to change the password once it has been delivered.		
		Review method by which user reports a forgotten password, and the method by which it is reset, the user is authenticated, and a new password is delivered. Verify that the process cannot be social-engineered.		
		Verify that users cannot defeat password controls, that passwords change, are hard to guess, and accounts are locked if subject to guessing attacks.		
	Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included.	Verify that no users have remote access.		
		Review employee and client termination procedures to ensure that they contain procedures for removing computer access and for changing passwords to shared accounts.		
		Verify that there is a one-to-one correspondence between the set of users configured in the system and the list of individuals who have been granted access.		
		Determine how user access request is mapped onto system, dial-up, and/or network access. List the individuals responsible for validating access requests for a given sample, dial-ups, or networks, and verify that the access is authorized.		
		Determine how user request form is validated before user access request is granted, e.g., if validation is by signature, determine how the signature is validated.		
		Ensure that all operating system, database management system, and application security features that limit access to files		

		are configured to ensure that users have the minimum access possible to perform their job functions.		
		Verify that user administration procedures identify specific individuals responsible for validating access requests for each user group, including administrative groups.		
		Verify that users know how to change their own passwords.		
	Users should systematically control the activity of their proper account(s). Also information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.	Sample users and determine if awareness activity and documented procedures indefeasibly educates users on risks and responsibilities, including company policies and standards related to system use.		
		Verify that users are given a way to review the last time they accessed a file or logged into a system.		
		Verify that users know how, to report a security incident.		
	Authentication tokens should be secure and nonrepudiable. Authentication sessions should not be subject to Internet recording and replay.	Verify that all authentication information entered by a user is entered through an encrypted channel.		
		If a user is allowed to maintain simultaneous Internet sessions, verify that the authentication, integrity, and transaction flow processes are designed to distinguish session activity rather than user activity.		
		Verify that users who require secure email are educated on advanced security features, including signing, sealing, and password control techniques.		
	Security activity should be logged and any indication of imminent security violation is notified immediately to the administrator and is acted upon automatically.	Review procedures to identify an account that is the subject of repeated failed access attempts.		
		Verify that automated network monitoring solutions exist where technically feasible.		
		Review user auditing and monitoring procedures to ensure that individual user system and network activity is traceable to an individual, including the use of administrative accounts.		
		Verify that available audit logging features are adequate and enabled for detecting security-related activity and verify that audit logs are monitored.		
		Review procedures to monitor and respond to invalid access attempts, unexpected system events such as reboots,.and changes to system and user configuration files.		

		Verify that a procedure exists to identify suspicious files and that duplicate commands are found, investigated, and removed.		
	Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme.	Verify that the information protection policy minimizes risks of liability from managing customer information.		
		Verify that the information protection policy adequately restricts information on system security access and detection mechanisms.		
		Review Information Protection Awareness program. Verify that it communicates information protection policy to every member.		
		Ensure that information protection policy designates roles and responsibilities with respect to levels of information protection.		
		Verify information protection policy compliance of corporate policies and standards with government and regulatory agencies.		
		Review measures that management takes to enforce information protection policy. Ensure that information protection policy designates information handling (including labeling) procedures for different levels of information protection.		
		Determine the level of sensitivity of data stored in data center. Verify that the level set complies with information protection policy		
		Determine if data center personnel are aware of the sensitivity level of the data stored in the data center, and follows corresponding procedures.		
	Management should establish a computer security incident handling capability.	For all types of system, network, application, and database accounts, verify that a procedure exists to respond to account-related security incidents.		
		Observe system security monitoring. Confirm that unexpected user activity is investigated.		
		Review the process by which public security alerts are disseminated and require a decision process. Confirm that decisions concerning publicly broadcast security incidents may result in immediate configuration changes.		

		Ensure that an incident tracking and problem resolution procedure supports the Internet Services environment.		
		Review security logs and alerts to obtain evidence that security incidents are identified.		
		Determine whether that management has independent and objective assurance that the Internet Services Systems can withstand a state-of-the-art hacker attack.		
	Internet Services administration features should not be available to Internet users.	Review network design, verify that administrative traffic is limited to planned access paths that minimize its interaction with user desktops.		
		Identify all systems used to manage administrative access to network routers, hubs, and servers. Verify that there is no non-administrator advertising or access to those systems.		
		Review network connectivity diagrams that contains detailed components of the network connections of each system under review. Identify all network connections to public, dial-in, or other networks not directly managed by SoftServe, Inc. Determine if traffic routing or filtering is employed to restrict data coming into or out of the Internet Services System environment.		
		Verify that the systems under review have no ports accessible from the Internet that are not absolutely necessary for users to run the application. From an Internet connection that is not managed by SoftServe, scan all IP addresses registered to SoftServe. Verify that only expected ports are accessible.		
Manage data	Management should establish data preparation procedures to be followed by user departments. In this context, input form design should help to assure that errors and omissions are minimized. Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.	Where data must be entered by IT personnel (that is, for master file data or other types of data that does not originate with the Internet user or customer data imported from other systems), verify that this data entry follows a documented process.		
		Verify that appropriate field-level and form level checking is in place to assist in accurate data entry. Determine if accuracy or completeness of data is maintained throughout the input process by record counts, batch totals, hash totals, or statistical sampling and manual checking.		

		Verify that input errors are logged and monitored on at least an aggregate basis to determine whether error handling procedures are in need of enhancement.		
	Transaction data entered for processing (people-generated, system-generated or interfaced inputs) should be subject to a variety of controls to check for accuracy, completeness and validity. Procedures should also be established to assure that input data is validated and edited as close to the point of origination as possible.	Access Internet services as a user. Verify that appropriate field-level and form level checking is in place to assist the user in accurate data entry and to prevent automated processing of incomplete or unauthorized transactions.		
		Identify reasons why Internet-entered transactions may not be immediately processed. Review process to detect, report, and, if possible, correct these transactions.		
		Review data import procedures to ensure that batch totals, check digits, and/or other appropriate controls maintain data accuracy and completeness.		
		Identify critical data imported into Internet Services systems (e.g. credit limits, account ranges). Verify that application and database controls are in place to maintain the integrity of the user-entered data.		
	Management should ensure that adequate protection of sensitive information is provided during transmission, transport, and storage.	Review the controls which prevent users from requesting and receiving other customer's data.		
		Review procedures for delivering data to archive location(s) and to recovery location(s).		
		Review procedures for labeling storage media to provide assurance that files are accurately identified.		
		Verify that media storage labels accurately reflect the retention period.		
		Determine if information protection policies are followed in information transport procedures.		
		Review procedures for transmitting customer information over non- Softserve-owned networks.		
		Verify that controls prevent unauthorized transmission of customer information.		
		Determine if information protection policies are followed in information transmission procedures (i.e. customer data is encrypted.)		

		Determine if information protection policies are followed in data storage procedures.		
	Procedures should be in place to ensure back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.	Review backup requirements for data, including on-site and off-site libraries, generations, storage media and retention periods; systems, programs and user documentation; restart/ recovery procedures; and special forms and supplies.		
		Review exact location of backup copies of application software, production files and documentation.		
		Review backup and restore procedures for Internet Services environments. Verify that they cover every environment component.		
		Verify databases are stored on a different hard disk drive than their database recovery log.		
		Verify that backup and off-site copies of application software are updated or replaced with each program revision.		
		Verify completeness and accuracy of instructions on how to perform, store, and restore from each required backup.		
	Transaction data should be collected in a manner readily identifiable to the end user.	Verify that the user is not notified of the completion of a transaction until all data has been authenticated and accepted into the database (e.g. through a two- phase commit process).		
		Verify that if a user cancels a transaction or drops an Internet connection in mid-transaction, the system does not continue to attempt to process the transaction.		
		Determine if accuracy or completeness of data is maintained throughout the input process by record counts, batch totals, hash totals, or statistical sampling and manual checking.		
		Regarding data transmission over the Internet or any other public network, management should define and implement procedures and protocols to be used to ensure integrity, confidentiality and non-repudiation of sensitive messages.		
Manage facilities	Appropriate physical security and access control measures should be established for information technology facilities, including off-site use of information devices in conformance with the general security policy. Access should be restricted to individuals who have been authorized to gain such access.	Verify that IT organization has appropriate relationship with those responsible for ensuring physical security and safety of information systems assets.		

		Obtain and review procedures followed by receptionists and/or guards at both building entrances and computer rooms.		
		Review policies and procedures pertaining to administration of access devices, issuance of keys, badges or combinations, keys, etc.		
		Determine how entry to the facility is restricted, the extent of each and all layers of access control and whether computer room access is monitored at all times.		
		Obtain a list of all employees with access badges, keys or combinations, and copy for inclusion in the workpapers. Determine access levels for all areas of access including vaults and storage areas or cabinets and identify each employee's access level.		
		Review access lists to determine that only personnel requiring access are authorized to access the computer room and determine whether access to the vault and storage areas is effectively restricted to authorized personnel.		
		Verify that doors accessing all restricted areas are kept in a closed, permanently locked position at all times.		
		Observe computer room entrances during all shifts and non-business hours to determine if only authorized personnel are allowed access.		
		Physically inspect walls, ceiling, floor, windows and doors to determine if they may be easily penetrated.		
	Physical security penetration attempts should be detected and appropriate response procedures should be in place.	Verify evidence of cameras and burglar alarms (indicating where the signal is transmitted).		
		Review procedures for detecting, controlling, recording, and reviewing physical access violations.		
		Determine that all security alarm systems are operational and tested on a regular basis.		
		Obtain and review records of attempted access violations.		
		Sample known incidents and trace through the physical security incident reporting process; verify that reported incidents are resolved.		

	Information services function management should ensure a low profile is kept and the physical identification of the site of its information technology operations is limited.	Survey exterior of building(s) that contain Internet Services Systems. Verify that it is not obvious that such assets are housed therein.		
		Verify that there no windows expose the location of the Internet systems servers or communications equipment to non-information systems personnel.		
	Appropriate procedures are to be in place ensuring that individuals who are not members of the information services function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.	Review procedures for visiting the computer room during business and non-business hours. Verify that records are maintained of access during non- business hours. Examine entrance or sign-in logs or records of access during these times.		
		Review procedures on temporary granting of access to secure areas. If badges/hand-held tokens are used to secure access, reconcile temporary badge repository with sign-out logs. If combinations locks are used, verify that the combination changes		
		Verify that cleaning personnel are escorted or supervised while operating in secure areas.		
		Verify evidence of intrusion alarms		
	Information services function management should assure that emergency response procedures are adequate to respond to environmental events.	Collect documentation of the floor plan. Ensure it is readily available and correctly reflects the location of control- related components. Compare floor plan to walls, windows, ceiling, and floors, examine construction and fire rating.		
		Obtain and review emergency procedures to determine that they are documented, adequate, and posted in a highly visible area. Ascertain that employees are trained in emergency procedures and that fire drills are held.		
		Verify that there no windows expose the location of the Internet systems servers or communications equipment to non-		

		information systems personnel.		
		Verify that emergency alarms, power-off switches, and emergency lights are visible marked, readily accessible, and tested to ensure that they are operational.		
		Determine that personnel have been trained in handling the identified dangers.		
		Determine that hand-held fire fighting devices are readily accessible and highly visible and adequate to protect the data center.		
		Verify evidence of heat, smoke, fire detection devices (indicating where the signal is transmitted).		
		Verify evidence of fire fighting devices. Physically inspect hand-held fire-fighting devices to ascertain that they have been inspected and tested on a regular basis.		
		Verify existence of power off switches. emergency lighting, panic doors, and fire hydrants.		
	Information services function management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g., dust, power, excessive heat and humidity). Specialized equipment and devices to monitor and control the environment should be installed,	Observe the general areas within and outside the computer room (including under the raised floor) to determine if housekeeping is adequate and the computer room is clean and free of dangerous or potentially hazardous materials.		
		Ensure that guard and reception scheduling processes allow adequate coverage of shift change and unexpected absences.		
		Review the floor plan and determine that fire prevention, detection, and suppression devices and computer room and building construction provide adequate protection against fire damage.		
		Determine that the floor tile pullers are readily accessible for emergency use as well as for routine maintenance.		
		Determine whether the computer room is protected by an automatic fire fighting system.		
		Determine if the computer room is subject to damage from water, flood, natural disasters, or any other dangers and identify all known exposures.		
		Review manual procedures designed to protect the computer room from environmental dangers.		
		Verify evidence of temperature measuring devices.		

		Review service and inspection schedules for heat, fire, and smoke detectors.		
		Determine how computer room temperature and humidity control levels are monitored and controlled.		
	Management should assess regularly the need for uninterruptible power supply batteries and generators for critical information technology applications to secure against power failures and fluctuations. When justified, the most appropriate equipment should be installed.	Review procedures for maintaining and testing alternative power supplies.		
		View alternative power test logs and results for conformance to procedures.		
		View evidence of scheduled maintenance for alternative power supplies to ensure that is adequate and current.		
Manage operations	Jobs are processed according to schedule.	Review Internet Systems data flow and process flow to identify key operations processes. Ensure that each has a documented support procedure.		
		Verify that automation enables smooth end-to-end job processing and detects process interruptions.		
		Verify that alerting mechanisms and associated procedures allow operations staff to identify root causes of process interruptions.		
	7x24 operations staff is efficiently and reliably managed.	For each job processed, identify roles and responsibilities with respect to problem identification and escalation.		
		Identify key personnel on call and observe incidents or sample to ensure they are available when needed.		
		Determine if staff hours and rotation schedules are formally managed and well understood.		
		Observe shift changes to verify that incidents in progress are properly managed.		
		Review help desk procedures to ensure that appropriate operations staff are notified of end user situation that may have resulted from unexpected operations failures.		
		Obtain a copy of management operation reports to verify that they accurate reflect current operations status.		
Monitor the process	For the information technology and internal control processes, management should ensure relevant performance indicators (e.g., benchmarks) from both internal and external sources, are being defined, and that data is being collected for the creation	Review management monitoring strategy and associated processes.		

	of management information reports and exception reports regarding these indicators.			
		Determine if system monitoring intervals are adequate to detect performance problems before they impact production.		
		Review procedures to detect inadequate system performance.		
		Review processes to collect accurate and relevant bench-marking data.		
		Determine if monitoring data adequately covers all systems under review.		
		Determine if productivity and integrity metrics are maintained to identify problems in training, procedures, or performance.		
	Services to be delivered by the information services function should be measured (key performance indicators and/or critical success factors) by management and be compared with target levels. Assessments should be performed of the information services function on a continuous basis.	Review periodic network performance and capacity reports.		
		Review the audit trail for a selected set of automated monitoring processes, confirm that processes perform on schedule and that variations in performance are investigated.		
		Verify that the database administrator monitors space and has automated a method to receive an alert if database space is rapidly decreasing.		
		Review database monitoring process to ensure it provide information on volume, response time, and throughput.		
		Confirm that deviations from production job schedules are logged, reviewed, and approved.		
		Confirm that security logs are maintained and appropriately reviewed.		
	At regular intervals management should measure customer satisfaction regarding the services delivered by the information services function to identify shortfalls in service levels and establish improvement objectives.	Verify that planned user workflows and planned administrative workflows exist and are complimentary.		
		Verify that help desk metrics include problem response intervals, resolution response intervals, fault monitoring, trend analysis.		
		Sample help desk cases and verify that recorded information is correct. Sample		

		user experiences with the help desk and verify that recorded information is correct.		
	Management reports should be provided for senior management's review of the organization's progress toward identified goals. Upon review, appropriate management action should be initiated and controlled.	Confirm that the status of management-approved production changes is reported back to the management that approved them.		
		Confirm that statistics on Internet Services prepared for management reports are relevant for their decision- making processes.		
		Confirm that system activity that presents business risk is immediately reported to management.		
		Verify that the management monitoring processes are integrated with incident tracking and problem resolution procedures.		
		Verify that presentations to upper management on the state of Internet Systems activity are timely and accurate.		
Assess internal control adequacy	Management is committed to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis.	Obtain a copy of the information systems control strategy.		
		Identify roles and responsibilities for key internal control responsibilities by job function.		
		Determine how management is appraised of the status of internal controls. Evaluate whether appraisal is accurate.		
		Identify metrics used for reporting on internal controls. Sample to verify accuracy of status report.		
Obtain for independent assurance	Management uses formal methods to evaluate third party services prior to use in the Internet Systems environment.	All contracts for third party services are audited prior to renewal.		
		Data used to audit contracts are predefined and agreed to by vendors.		
		Contract audits are conducted by individuals who are independent from both the vendors and the internal organizations that use the given service.		
		Contract audits are delivered directly to senior management.		
Provide for independent audit	Senior management is cooperative with the audit effort.	Documentation is available upon request.		

		Interviews are granted reasonably soon upon request.		
		Systems are made available for testing when required to conduct an audit test.		
		Issues identified during an audit are discussed openly and frankly.		
		Management understands the role of audit in the company internal control structure.		

Appendix B

SoftServe Internet Services Audit Report

INTERNAL AUDIT INFORMATION TECHNOLOGY REPORT

REPORT DATE: XXX XX, XX

BUSINESS UNIT: Outsourcing

PRIOR REVIEW: No prior system review

OBJECTIVES:

- To determine the adequacy of control procedures and the use of best practices for the Internet Services systems environment.
- Understand and evaluate the key operational processes and workflows for Internet systems operation and deployment.

EXECUTIVE SUMMARY

The current SoftServe Inc. Internet service offering was implemented in November of last year. The implementation of this system was the responsibility of the Outsourcing business unit, though it does provide information to customers of the Deployment and Consulting business units as well. The system is operated at or above industry standard control practices, with one exception, noted below. Based upon the overall control environment and management's commitment to address systems vulnerabilities immediately upon identification, the overall assessment for the Internet Service offering is satisfactory.

SIGNIFICANT OBSERVATIONS AND FINDINGS:

(Management comments/responses noted in italics)

1. User Database Access

The Internet application allows users to access the database via a database login and password that is embedded in the compiled code that is stored both in the source code control system and on several developer desktops. It is possible for any developer or user of a developer desktop to extract this login and password and access the database directly. Direct access would avoid application access controls that prevent users from viewing or changing data to which they are not authorized. This vulnerability is somewhat mitigated by the fact that direct database access is not available from the Internet, so the exposure is limited to users of SoftServe's internal networks.

Our contracts with both outsourcing and deployment users include confidentiality clauses which any disclosure of customer data would breech. If this vulnerability is considered a breech of confidentiality, SoftServe may incur serious liabilities.

This situation occurred because commercial development tools used to create the Internet software hid the database interaction from the application architects. They designed security into the application without awareness of the underlying architecture of the product. The effect is that users who are familiar with the development tool may easily identify files that contain database access passwords.

We recommend that the database access mechanism provided by the commercial development tool be replaced by an authentication mechanism that restricts access to application-authenticated users and that allows database passwords be removed from application code.

Management Response (Mike Manager):

We accept the above assessment. We have scheduled the recommended system changes. We expect that they will be complete by next month. In addition, we have conducted security training on the development software for all application architects.

Reviewers:

_____ _____ _____

Ian Itaud Sue Senior Joe Junior

Distribution:

O. Outcio, CIO, Outsourcing Business Unit
D. Deploycio, CIO, Deployment Business Unit
C. Consultcio, CIO, Consulting Business Unit
P. Presouts, President, Outsourcing Business Unit
P. Presdep, President, Deployment Business Unit
P. Prescon, President, Consulting Business Unit
A. Auddir, Director of Internal Audit
A. Extaudpart, External Audit Partner
S. Softcfo, CFO, SoftServe, Inc.
S. SoftPres, President, SoftServe, Inc.

Glossary

AICPA American Institute of Certified Public Accountants.

Application ControlsControl practices that are performed for a specific set of systems that represent one or more applications of the same systems architecture.

Attestation ServiceA service designed to provide an opinion on a predefined state of affairs.

Audit An activity designed to provide assurance that control objectives are met, and where they are not met, to substantiate risks of control weaknesses and advise management on corrective action.

Audit Objective The purpose of an audit.

Availability: Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

CIO Chief Information Officer (CIO), Chief Technology Officer (CTO), or other high level executives with the ultimate responsibility for systems operations.

CISA Certified Information Systems Auditor.

Compliance: Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.

Chief Accountant A generic term used to describe a person that has primary responsibility for the production of an organization's financial statements. A more correct term for a given country may be Chief Financial Officer or Comptroller.

Confidentiality: Concerns the protection of sensitive information from unauthorised disclosure.

Control: The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

Control FrameworkThe combination of security and internal control policy, organizational structure, roles and responsibilities, and enforcement structure that management uses to establish and maintain control objectives.

Control Objective:High level statement of the desired result or purpose to be achieved by implementing control procedures.

Control Testing Testing designed to ascertain if a given control is in place.

COSO Committee of Sponsoring Organizations, see World Wide Web: <http:// www.coso.org>.

EDPAA Electronic Data Processing Auditors Association.

Effectiveness: Deals with information being relevant and pertinent to the business process, as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency: Concerns the provision of information through the optimal (most productive and economical) use of resources.

General Controls Control practices that are done in the same manner throughout the organization's IT environment.

Integrity: Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

IT Control Objective: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

IT Governance: A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.

FCPA Foreign Corrupt Practices Act.

Fieldwork A generic audit term that refers to any activity performed by auditors outside the confines of their own office that contributes to the completion of an audit program.

GAAP Generally Accepted Accounting Practices.

GAAS Generally Accepted Auditing Standards.

ICS Internal Control Structure, the method by which operational and performance goals are achieved in an efficient and effective manner that is transparent to management.

IS Audit An Information Systems Audit is a service designed to provide assurance that control objectives with respect to information technology are met, and where they are not met, to substantiate risks of control weaknesses and advise management on corrective action.

ISACA Information Systems Audit and Control Association, see World Wide Web: <http://www.isaca.org>.

IT Governor Those who manage the people and processes that plan, organize, monitor, and control the use of information technology.

Management Audit A Management Audit is an assurance service designed to identify performance improvement opportunities in the management process (that is planning, organizing, monitoring, and control).

Regulatory Compliance A state of affairs that meets all applicable regulatory requirements.

Review Area A general description of the subject of an audit.

Risk Assessment A process whereby risks to organizational objectives are identified and ranked according to potential for damage and probability of occurrence.

Scope A technical term in audit that allows a mapping from the definition of the purpose of review to the environment to be reviewed.

Substantive Testing Testing of every member of a set of items in order to verify that each element of the set meets a give criteria.

Statutory Auditor A generic term used to describe a person licensed in a given environment to perform independent audits. A more correct term for a given country may be Certified Public Accountant (CPA), Chartered Accountant, or Independent Auditor.

Structured Programming A methodology in which computer programs are built from reusable components.

Index