AUDITING INFORMATION SYSTEM

BS(LIS)

Code No. 9224 **Units: 1-9**

Department of Library and Information Sciences
Faculty of Social Sciences and Humanities
ALLAMA IQBAL OPEN UNIVERSITY
ISLAMABAD

AUDITING INFORMATION SYSTEM

BS (LIBRARY AND INFORMATION SCIENCES)

Course Code: 9224 **Units: 1-9**

AIOU website: aiou.edu.pk
LIS Dept. website: lis.aiou.edu.pk/
LIS Facebook page: Dept. of Library & Information Sciences, AIOU, Islamabad– Official

Department of Library and Information Sciences
Allama Iqbal Open University, Islamabad

Year of Publication 2023

Quantity 1000

Layout Setting ..... Muhammad Zia Ullah

Incharge Printing ..... Dr. Sarmad Iqbal

Printer..... Allama Iqbal Open University

Publisher ..... Allama Iqbal Open University, Islamabad

COURSE TEAM

Chairman Course team:

Dr Pervaiz Ahmad

Professor/Chairman

Course Development Coordinator

Dr Amjid Khan

Assistant Professor

Compiled by

Dr. Amjid Khan

Reviewed by

Dr. Pervaiz Ahmad
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

FOREWORD

Department of Library and Information Sciences was established in 1985 under the flagship of the Faculty of Social Sciences and Humanities intending to produce trained professional manpower. The department is currently offering seven programs from certificate course to PhD level for fresh and/or continuing students. The department is supporting the mission of AIOU keeping in view the philosophies of distance and online education. The primary focus of its programs is to provide quality education by targeting the educational needs of the masses at their doorstep across the country.

BS 4-year in Library and Information Sciences (LIS) is a competency-based learning program. The primary aim of this program is to produce knowledgeable and ICT-based skilled professionals. The scheme of study for this program is specially designed on the foundational and advanced courses to provide in-depth knowledge and understanding of the areas of specialization in librarianship. It also focuses on general subjects and theories, principles, and methodologies of related LIS and relevant domains.

This new program has a well-defined level of LIS knowledge and includes courses in general education. The students are expected to advance beyond their higher secondary level and mature and deepen their competencies in communication, mathematics, languages, ICT, general science, and an array of topics in social science through analytical and intellectual scholarship. Moreover, the salient features of this program include practice-based learning to provide students with a platform of practical knowledge of the environment and context, they will face in their professional life.

This program intends to enhance students' abilities in planning and controlling library functions. The program will also produce highly skilled professional human resources to serve libraries, resource access centres, documentation centers, archives, museums, information centers, and LIS schools. Further, it will also help students to improve their knowledge and skills of management, research, technology, advocacy, problem-solving, and decision-making relevant to information work in a rapidly changing environment along with integrity and social responsibility. I welcome you all and wish you good luck in your academic exploration at AIOU!

Prof. Dr. Zia Ul-Qayyum

Vice-Chancellor

PREFACE

Auditors have always been responsible for consulting with management to help ensure that adequate internal controls exist within organizations to mitigate major risks to a reasonable level. Auditors identify and quantify risk using professional judgment based on knowledge, education, experience, and even history. This study guide has attempted to view information systems (IS) auditing from a practical viewpoint, applying many existing concepts to a variety of real-world situations, thereby providing readers with useful examples of what they might expect to encounter in audits that they perform or oversee. This study guide is designed to provide readers with information, suggestions, and examples of real-world information systems issues that have been encountered in the business world and to identify issues that are pertinent within the IS auditing field. This book discussed many important IS auditing concepts that are critical to performing effective audits as we move further into the new millennium. These include the basics of computing systems; identification and creation of computing systems inventories; a generic IS audit program; IS policies, standards, and guidelines; auditing of service organizations, including their financial stability and contracts; accounting treatment of computer equipment and hardware; physical and logical security controls; IS operations; control self-assessment (CSA); encryption and cryptographic controls; computer-assisted audit techniques; computer viruses; software piracy; computer forensics; electronic commerce; auditing system development projects; Internet security; and the humanistic aspects of contemporary IS auditing.

The IS auditing theories, checklists, case studies, exhibits, references, and other information discussed in this study guide by no means encompass the entire body of knowledge surrounding the field of IS auditing, nor are they meant to be presented in scientific detail. The concepts are also intended to help readers think about creative approaches to addressing new and traditional risks that their organizations are facing as the technology age rolls on. It is hoped that readers will share their newfound knowledge, thereby helping to advance the body of knowledge encompassed by IS auditing. One final intention is that readers will realize that auditing is a profession that has a wealth of highly skilled and knowledgeable individuals and resources available for the taking. All one must do is take the initiative and begin the fascinating and rewarding journey through the profession of helping organizations control the risks posed by the never-ending supply of new IS technologies being introduced in the marketplace. One of the biggest challenges IS auditors face is keeping knowledge current with rapidly changing technology while still monitoring the controls and security of existing technologies.

Dean,

Faculty of Social Science & Humanities

ACKNOWLEDGMENT

First, I am extremely grateful to the worthy Vice-Chancellor and the worthy Dean, of FSSH for allowing me to prepare this book. Without their support, this task may not be possible. Further, they have consistently been a source of knowledge, encouragement, benignancy, and much more.

I am highly indebted to my parents, spouse, siblings, and children, who allowed me to utilize family time to completion of this work timely. Their continuous prayers kept me consistent throughout this journey. I would also appreciate the cooperation of my departmental colleagues extended to me whenever required. Special thanks to the Academic Planning and Course Production (APCP) and Editing Cell of AIOU for their valued input that paved my path to improve and finish this book per AIOU standards and guidelines. They have been very kind and supportive as well.

I would also like to thank the Print Production Unit (PPU) of AIOU for their support regarding the comprehensive formatting of the manuscript and for designing an impressive cover and title page. Special thanks also owe to AIOU's library for giving me the relevant resources to complete this task in a befitting manner. I am also thankful to ICT officials for uploading this book on the AIOU website. There are many other persons, whose names I could not mention here, but they have been a source of motivation in the whole extent of this pursuit.

Dr Amjid Khan
Assistant Professor, LIS

INTRODUCTION

The course has been designed as easily as possible for distance mode of learning and it will help students in completing his/her required course work. The course is of three credit hours and comprises nine units, each unit starts with an introduction which provides an overall overview of that unit. At the end of every unit the objectives of the unit show student the basic learning purposes. The rationale behind these objectives is that after reading the unit a student should be able to explain, discuss, compare, and analyze the concepts studied in that unit. This study guide is specifically structured for students to acquire the skill of self-learning through studying prescribed reading material. Studying all this material is compulsory for the successful completion of the course. Recommended readings are listed at the end of each unit. A few self-assessment questions and activities have also been put forth for the students. These questions are meant to facilitate students in understanding and self-assessment that how much they have learned.

For this course, a 6-days workshop at the end of a semester will be arranged by the department for learning this course. Participation/attendance in a workshop is compulsory (at least 70%). The tutorial classes/meetings are not formal lectures as given in any formal university. These are meant for group and individual discussion with the tutor to facilitate students learning. So, before going to attend a tutorial, prepare yourself to discuss course contents with your tutor (attendance in tutorial classes/meetings is non-compulsory).

After completing the study of the first 5 units 'Assignment No. 1' is due. The second assignment that is 'Assignment No. 2' is due after the completion of the next 4 units. These two assignments are to be assessed by the relevant tutor/resource person. Students should be very careful while preparing the assignments because these may also be checked with Turnitin for plagiarism.

COURSE STUDY PLAN

As you know the course is offered through distance education, so it is organized in a manner to evolve a self-learning process in absence of formal classroom teaching. Although the students can choose their way of studying the required reading material, but advised to follow the following steps:

Step-1: Thoroughly read a description of the course for clear identification of reading material.

Step 2: Carefully read the way the reading material is to be used.

Step 3: Complete the first quick reading of your required study materials.

Step 4: Carefully make the second reading and note down some of the points in a notebook, which are not clear and need full understanding.

Step 5: Carry out the self-assessment questions with the help of study material and tutor guidance.

Step 6: Revise notes. It is quite possible that many of those points which are not clear and understandable previously become clearer during the process of carrying out self-assessment questions.

Step 7: Make a third and final reading of the study material. At this stage, it is advised to keep in view the homework (assignments). These are compulsory for the successful completion of the course.

Assessment/Evaluation Criteria of Students' Coursework

Multiple criteria have been adopted to assess students' work for this course, which are as follows:

i. Written examination to be assessed by the AIOU Examination Department, at the end of the semester= 70% marks (pass marks 50%). AIOU examination rules will be applied in this regard.

ii. Two assignments and/or equivalent to be assessed by the relevant tutor/resource person= 30% marks (pass marks 50% collectively).

Note: Assignments submission and getting pass marks is compulsory, the student who will not submit assignments or is marked as fail is considered FAIL in the course. He/she will get fresh admission in the course; there is no need to sit in the exam.

Recommended Books

Champlain, J. J. (2003). *Auditing information systems*. John Wiley & Sons.

UNIT-1

BASICS OF COMPUTING SYSTEMS; IDENTIFYING COMPUTER SYSTEMS

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

This unit give the reader a grasp of the basics of computing systems, CPU, history of processing speeds, operating systems, application programs, database management systems, physical security control, logical security controls, and benefits of computing systems inventory. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- Basics of computing systems
- Central processing unit
- History of processing speeds
- Operating system
- Computing memories
- Database management systems
- Physical security control
- Logical security controls

1.1 BASICS OF COMPUTING SYSTEMS

Before performing an audit of a computing system or assessing the adequacy of an audit that was performed on a computing system, there are a few basics that one must understand about how a computing system functions. A computing system is essentially comprised of three basic components:

a. the central processing unit,
b. the operating system, and
c. application programs

Many systems also have a fourth system where the data resides and is managed which is called a database management system. Each of these components is described in the following sections.

1.1.1 Central Processing Unit

A central processing unit (CPU) is essentially a box of interconnected electronic circuits. There are thousands of CPUs in the world today. They include stand-alone microcomputers such as the IBM family of personal computers and their clones, the Apple Macintosh family of microcomputers, mini and mid-range computers such as the IBM AS/400 and the Compaq Alpha family, mainframe computers such as the IBM System 390 series, and even experimental supercomputers.

The brains of these CPUs are computer chips. Among other things, chips determine the speed and efficiency with which computers operate. For computer chips, operating speed is usually measured in terms of megahertz (MHz) and more recently in gigahertz (GHz) and teraflops. One MHz is equivalent to one million operations per second. One GHz is equivalent to one billion operations per second. One teraflop is equivalent to one trillion operations per second. There are hundreds of computer chip manufacturers, both large and small. Some of the more well-known chip manufacturers include IBM, Sun, Intel, Motorola, Hewlett Packard, Advanced Micro Devices, NEC, Hitachi, Compaq, Mitsubishi, and Apple. One of the most widely recognized computer chip manufacturers is Intel, a maker of the Pentium® family of chips, which are installed in many personal computers and file servers. Pentium 4 chips enable personal computers to run at speeds over 2.5 GHz.

1.1.2 History of Processing Speeds

In January 1997, Intel launched the Pentium MMX™ computer chip, which was touted to run existing programs 10 to 20 percent faster than previous same-speed processors. Programs written to take advantage of the new multimedia-enhancing technology reportedly could run 60 percent faster. In July 1997, the Apple PowerBook® 3400 laptop was reportedly capable of running at speeds up to 235 MHz.
Computer chips installed in more sophisticated commercial computers were attaining speeds in the 300 to 500 MHz range in 1997. For example, in May 1997, Intel introduced

the Pentium II®, a sixth-generation processor that can run at 300 MHz and incorporates the MMX technology. This chip was based on the Pentium Pro®, a powerful commercial-use chip. In 1996, Digital introduced its new midrange Alpha® computer. The Alpha chip, which crunches 64 bits of data at a time, is capable of processing at 440 MHz. In October 1996, a small computer chip maker announced that it had developed a chip purported to be able to operate Apple Macintosh software at up to 533 MHz.

In December 1996, a supercomputer developed jointly by Intel and the U.S. Energy Department that could perform at a speed exceeding one teraflop, or one trillion operations per second. This was almost three times faster than the previous supercomputing record held by Hitachi of Japan. The $55 million computer was primarily to be used by government scientists at Sandia Laboratories in Albuquerque, New Mexico, to simulate nuclear weapons tests that are now banned by international treaty.

This application reduced the need to detonate live nuclear explosives to assess their destructive powers. It also eliminated the risk of damage to humans and the environment, and thus avoids the many political ramifications associated with live nuclear testing. The technology can be applied to any commercial applications requiring high-speed calculations. Examples of such applications include weather forecasting and genetic mapping. The tremendous speed of the supercomputer was achieved by clustering 7,264 high-end Pentium Pro computer chips into modules, using a technique called "massively parallel computing." The system eventually included 9,200 computer chips and was able to operate at 1.4 teraflops. Using this technology, Intel expects to be able to configure networks to utilize the processing power of far more chips than before, thereby vastly increasing their computing power. By the year 2000, Intel expected the supercomputer to be able to break the three-teraflop barrier.

Since 1997, computer chip manufacturers have continued to keep pace with Moore's Law, which asserts that computer processing speeds will double every 18 months. Intel cofounder Gordon Moore predicted in 1965 that each new memory chip could perform about twice as many processes as its predecessor, and each new chip would be released within 18 to 24 months of the previous chip.

In June 2002, the National Centers for Environmental Prediction, a division of the National Weather Service, ordered a $224 million IBM computer that will be able to run at 100 teraflops. In April 2002, the Japanese NEC Earth Simulator computer had 5,104 processors that could reach a speed of 35.6 teraflops. This beat the existing computer speed record of 7.2 teraflops achieved by the ASCI White-Pacific computer at the Lawrence Livermore National Laboratory in California using 7,424 processors.

In 2002, IBM built the world's fastest single microchip, which runs at more than 100 GHz. In 2001 Intel devised a new structure for transistors (chips) that eliminated the speed-limiting problems of power consumption and heat. The chips reportedly can operate at one terahertz or one trillion operations per second. Britain purchased a supercomputer made by Sun Microsystems that has a memory equivalent to 11,000 CD-

ROMs and runs at 10 GHz. Intel introduced its two fastest chips, which run at 1.8 and 1.6 GHz, and offered a 2 GHz chip in the third quarter of 2001.

The new transistors are only 20 nanometers, or .02 microns, in size compared to the .18-micron chips in use today. The breakthrough means that silicon will be able to be used to make chips until at least 2007 and will make possible microprocessors containing close to 1 billion transistors running at 20 GHz by that year.

- It also means that Moore's Law will remain on the books until at least 2007.
- Advanced Micro Devices, Inc., introduced two new Athlon chips that run at 1.2 and 1.0 GHz.
- Intel introduced the long-awaited Pentium 4 processor, which runs at 1.7 GHz.
- Intel rolled out its Pentium 3 chip for laptops, which runs at 1 GHz.
- Intel is introducing two Celeron chips that run at 766 MHz and 733 MHz.
- IBM scientists plan to spend five years building the fastest computer in the world.
- The "Blue Gene" computer will be 500 times faster than anything in existence today.
- Apple unveiled new iMac computers that run at 400 MHz and 350 MHz.
- IBM unveiled a new high-speed mainframe computer that runs at 1.6 GHz. It will be used for mapping human genes.
- IBM has developed the world's fastest computer capable of running at 3.9 teraflops to simulate nuclear explosions.

1.1.3 Future of Processing

The potential processing speed of supercomputers, and eventually commercial and consumer computers, is limited only by the amount of space available to house the computers and the size of the materials used to create chips. Conventional technology uses silicon-based chips. However, these chips are projected to reach their maximum size reduced potential by 2010 to 2015.

A newer, promising technology is based on quantum technology. This technology uses individual atoms as semiconductors. It is fascinating to try to comprehend the potential capabilities of robots and other computer-based machines, which, soon, could have multiple high-speed computer chips clustered in a manner that enables processing speeds of more than one quadrillion operations per second or more. It is only a matter of time before many of the science fiction events depicted in productions like *Star Trek* and *Star Wars* are no longer fiction. Teleporting is already being experimented on. As higher- and higher-speed computers materialize in the workplace, auditors will need to understand their potential capabilities and be prepared to evaluate the controls and security over them. Auditors will also need to be able to help organizations maximize the benefits from the processing capabilities of these computers.

1.1.4 Computer Memory

Memory is usually measured in terms of the number of bytes of data that can be stored in memory at any one time. Two primary types of memory are usually referred to concerning computers:

- processing memory, and
- storage memory.

Processing memory is often referred to as random access memory (RAM) or temporary memory. The amount of RAM available in computers is commonly stated in terms of megabytes (MB). As of this writing, new retail home computers were boasting available RAM sizes of up to 512 MB. The more RAM a computer utilizes, the more applications it can process concurrently, thus allowing users to switch from one application to another without having to exit previous applications. Once a computer is turned off or the power is interrupted, most of the information residing in RAM is not retained, hence the term *temporary memory*. Many have found this out the hard way when their systems went down, and they had not saved their work recently. After a few instances of suffering the loss of hours of work because I had not saved, I developed the habit of saving every 5 to 10 minutes to both the hard drive and a diskette or read-writable CD (CD-RW) in an external drive.

Numerous applications can permanently reside in RAM. For example, a security software package exists that resides in RAM and requires the user to enter a password before the computer can proceed with the initialization process. This software can prevent an unauthorized user from initializing a computer by placing an initialization diskette into an external drive, such as the A drive. An unauthorized user could use this technique to initialize a computer, circumvent a less sophisticated sign-on security application that is not resident in RAM, and then access the hard drive from the external drive. Unfortunately, many computer viruses can also reside in RAM. They usually gain residence when an unsuspecting user infects other computers and file servers by infecting a diskette that is accessed by another computer and by travelling through intranets and the Internet. For example, attaching an infected file to an e-mail message can cause the recipient's computer to become infected. To combat viruses, many virus-checking applications have been developed and marketed.

Some are available from computer manufacturers upon the purchase of computer equipment and operating systems while others are available over the counter. The best virus checkers can be set to examine any incoming data files for viruses in their inventory, regardless of source, remove the infected files, and notify the user or system security administrator of any detected viruses. The virus inventory needs to be updated periodically as new viruses are identified. Some virus application developers offer a service that provides subscribers with updated virus inventories periodically (e.g., daily).
Storage memory refers to the number of bytes of data that can be stored on the hard drive of a computer. The phrase *hard drive* is synonymous with the phrases *hard disk, fixed*

disk, and *fixed drive*. Storage memory has increased to the point where it is usually stated in terms of gigabytes (GB).

Unlike RAM, storage memory is retained even after the power is turned off or interrupted. Thus, storage memory is sometimes referred to as permanent memory. However, it is permanent only until the information has been completely deleted. Note that the act of deleting a file does not actually delete the data. It simply removes the file location reference. The data remains on the storage medium until it is overwritten. Since most computers store data sequentially, it can take several weeks, months, or years to overwrite a previously deleted file, depending on the amount of data that has been saved and deleted and the size of the storage medium. Many organizations have a backup data storage program to help ensure data recovery in the event of a disaster.

Depending on the frequency of a rotation and the storage period of the backup media, data can be proliferated indefinitely. For this reason, especially when working with highly sensitive, classified, or confidential information, it is extremely important to adequately secure access to the computer storage media.

Computer forensics companies have recently come into existence to search through the mines of data in existence at virtually all businesses, governments, and other organizations. These forensics firms provide a variety of services. They can be hired by plaintiffs in lawsuits against organizations. After performing the necessary legal proceedings, they can secure a search warrant, which grants judicial authority to obtain control over all the computer resources of an organization, regardless of size, to search for incriminating evidence. Computer forensics firms can also be hired by organizations to assist in developing data storage and retrieval policies and procedures that help minimize or maximize the incidence of data proliferation, depending on the objectives of the organization.

Law enforcement agencies have also utilized the services of computer forensics companies to help recover data from confiscated computer equipment and storage media obtained during raids. The main concept to keep in mind when assessing controls over a computer is that no matter how physically large it is or how fast it operates, all computers function in basically the same manner. Thus, the audit approach and many of the controls that can be applied are generally the same.

1.2 OPERATING SYSTEM

Central processing units are usually connected to various peripheral devices that assist in storing, accessing, and transmitting data and in the production of information output. Examples of peripheral devices include external disk drives, single CD-ROM and CD-RW drives, multiple CD-ROM drives (sometimes called "jukeboxes"), magnetic tape drives, disk packs, printers, routers, bridges, gateways, controllers, visual monitors, keyboards, terminals, and others. These devices are collectively referred to as *computer hardware.*

Operating systems are programs that are required to make hardware devices function. They are usually loaded into computers during the manufacturing process. Operating systems typically include an assortment of utility programs that assist in the functioning, maintenance, and security of the various hardware devices. The operating system and utilities are collectively referred to as *system software*. Examples of common operating systems include DOS, Windows, OS/ 2, NetWare, OSX, Unix, VMS, and OS/390.

Certain features within the system software can be customized by the purchaser. For example, most sophisticated operating systems possess system access control features that enable the purchaser to adequately protect the system against unauthorized access. Manufacturers usually set the system access control parameters to allow virtually unlimited access during initial installation. This is necessary so that the user performing the initial installation can set up other users, configure the system, and customize available system parameter settings. However, because of how wide open newly installed systems are, the system access control features must be properly deployed as soon as possible after installation.

Although computer manufacturers usually assist in the initial installation of complex systems, they tend to concentrate more on making the system operational rather than ensuring that it is adequately secured. Many vendor technicians usually create user identifications (IDs) for themselves, which have the same privileges as a system security administrator. Often, they do not delete the user IDs after they have completed the installation. As a result, the organization is subjected to the risk of unauthorized access by the installing technicians. This is one of the reasons auditors need to participate in new system implementation projects.

1.3 APPLICATION PROGRAMS

Application programs are required to make a CPU and system software perform business functions. Many off-the-shelf application programs have been written to perform general tasks such as word processing (e.g., Word, WordPerfect), spreadsheets (e.g., Excel, Lotus 1 2-3), and data analysis (e.g., Access, Paradox). Many other applications have been written to perform specific business functions in a variety of industries (e.g., loan and deposit applications in financial institutions, credit card applications in card issuing companies, computer design applications in automobile and airplane manufacturing firms, and claims processing applications in insurance companies).

Several enterprise resource planning (ERP) applications exist that help performs common business functions such as financial accounting, accounts payable, human resources, payroll, fixed assets management, and so on. Examples of these ERP applications include PeopleSoft, SAP, Oracle, Baan, J. D. Edwards, and Lawson. Literally, millions of other applications have been developed internally by companies and externally by vendors to perform a myriad of business functions, some of them in multiple languages. Each of these applications may or may not have control features designed to help prevent unauthorized access to them.

1.4 DATABASE MANAGEMENT SYSTEMS

A database management system (DBMS) typically consists of a suite of programs that are used to define, query, secure, and generally manage large volumes of data. Having data located in a separate DBMS offers several benefits, including the flexibility to change applications without affecting the data, the ability to eliminate data redundancy formerly required by non-open applications, and the ability to better secure and monitor the data. Some applications perform tasks that do not require a DBMS. For example, an application that specifically controls the raising and lowering of cooling rods in a nuclear power plant does not need a database. However, data about the raising and lowering needs to be recorded, monitored, and analyzed, most likely by another application. Depending on the amount and complexity of data being recorded, a DBMS may be necessary. Most complex computing applications have some sort of DBMS associated with them. In some cases, applications are written to function with a specific DBMS and to rely solely on the DBMS to implement security. In other cases, applications are written to function with a variety of different DBMSs and have security features within the application software as well as the DBMSs. Examples of common DBMSs include Microsoft SQL Server, Oracle, and IBM DB2.

1.5 PHYSICAL SECURITY CONTROLS

Computer hardware includes the CPU and all peripheral devices. In networked systems, these devices include all bridges, routers, gateways, switches, modems, hubs, telecommunication media, and any other devices involved in the physical transmission of data. These pieces of equipment must be adequately protected against physical damage resulting from natural disasters, such as earthquakes, hurricanes, tornadoes, and floods, as well as other dangers, such as bombings, fires, power surges, theft, vandalism, and unauthorized tampering. Controls that protect against these threats are called *physical security controls.* Examples of physical security controls include various types of locks (e.g., conventional keys, electronic access badges, biometric locks, cypher locks); insurance coverage over hardware and the costs to re-create data; procedures to perform daily backups of the system software, application programs, and data; as well as off-site storage and rotation of the backup media (e.g., magnetic tapes, disks, compact disks [CDs]) to a secure location; and current and tested disaster recovery programs.

1.6 LOGICAL SECURITY CONTROLS

Computing systems must also be adequately protected against unauthorized access and accidental or intentional destruction or alteration of the system software programs, application programs, and data. Protecting against these threats is accomplished through the deployment of logical security controls. Logical security controls are those that restrict the access capabilities of users of the system and prevent unauthorized users from accessing the system. Logical security controls may exist within the operating system, the database management system, the application program, or all three. The number and

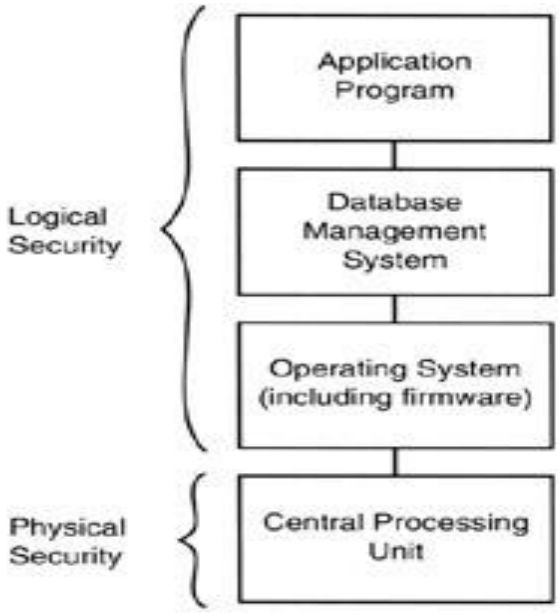
types of logical security controls available vary with each operating system, database management system, and application, and in many types of telecommunication devices. Some are designed with an extensive array of logical security control options and parameters that are available to the system security administrator. These include user IDs, passwords with minimum length requirements and a required number of digits and characters, suspension of user IDs after successive failed sign-on attempts, directory and file access restrictions, time-of-day and day-of-week restrictions, and specific terminal usage restrictions. Other operating systems and applications are designed with very few control options. For these systems, logical security controls often seem to be added as an afterthought, resulting in control settings that are weaker than what is reasonably desirable, even when the maximum available access restrictions have been implemented.

Many systems are programmed with controls that are commensurate with the degree of risk associated with functions performed by the systems. For example, a high-risk wire transfer transaction processing system at a financial institution should have significantly more extensive controls than a lower-risk non-transactional record-keeping system at the same institution. However, be alert to high-risk systems with poor controls. Many high-risk systems have been programmed with inadequate control features or have adequate control features available, but the features are inadequately implemented. Problems can occur when programmers and/or process owners are not aware of one or more significant risks facing the organization during the use of the system.

1.7 Location of Physical and Logical Security Controls

Figure 1.1 visually depicts the concept of a basic computing system and the location of physical and logical security controls. Physical security controls pertain to the central processing unit and associated hardware and peripheral devices. Logical security controls exist at the operating system level and within database management systems and application programs. This basic model can be applied to virtually any type of computing system.

Figure 1.1 Basic Conceptual Model



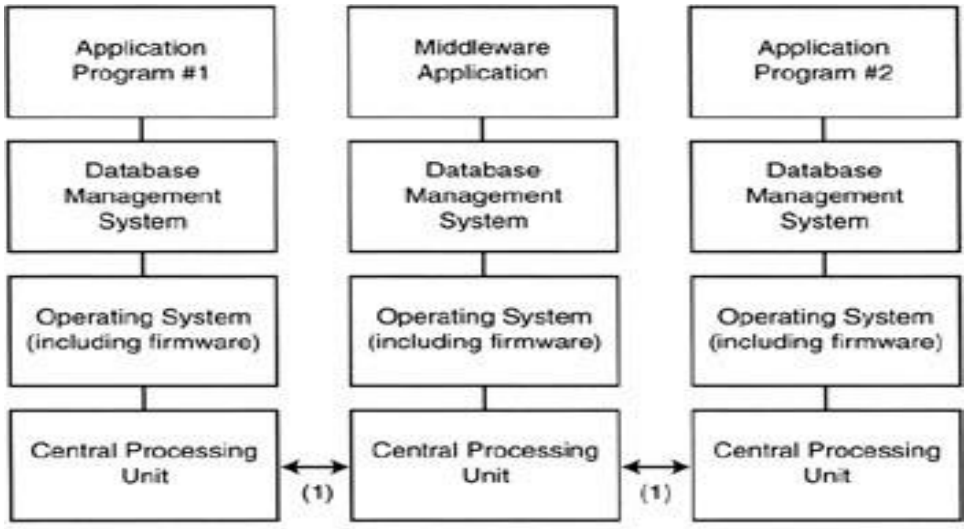
Some other elements of the computing control environment:

Information Protection and Security Policy, Standards, and Procedures
Reporting Structure
IT Operations
Vendor Financial Condition
Vendor SAS 70, TruSecure, SysTrust, WebTrust, TRUSTe, BBBOnline, Other Security Certifications
Vendor License, Maintenance and Support Agreements (software and hardware)
Insurance Policies

Note: This conceptual model is not meant to replace the ISO open systems interconnection (OSI) model. It is a simplified approach meant to help nontechnical auditors to quickly ascertain the adequacy of controls over the most common risks associated with computer systems. See Appendix C for a brief overview of the ISO-OSI model.

For example, Figure 1.2 presents a conceptual model of one way to view the physical and logical security controls over a system that has three applications, each with its CPU. In this configuration, data redundancy can be eliminated if managed properly because applications 1 and 2 can exchange data via the middleware application. The firmware includes memory chips that contain frequently used operating programs and data so they can be processed more rapidly than if the programs had to be loaded and executed in RAM. Unlike RAM, the programs and data are not erased when the power to the CPU is turned off. The firmware typically performs computer processing and thus has logical security controls associated with it.

Figure 1.2 Conceptual Model of Open-Networked System



(1) Includes all telecommunications devices and media that are involved in the transmission of data, such as bridges, routers, gateways, switches, hubs, modems, telecommunications media, etc. Each potentially has some logical security controls associated with it.

Some other elements of the computing control environment:

Information Protection and Security Policy, Standards, and Procedures
Reporting Structure
IT Operations
Vendor Financial Condition
Vendor SAS 70, TruSecure, SysTrust, WebTrust, TRUSTe, BBBOnline, Other Security Certifications
Vendor License, Maintenance and Support Agreements (software and hardware)
Insurance Policies

Note: This conceptual model is not meant to replace the ISO open systems interconnection (OSI) model. It is a simplified approach meant to help nontechnical auditors to quickly ascertain the adequacy of controls over the most common risks associated with computer systems. See Appendix C for a brief overview of the ISO-OSI model.

1.8 IDENTIFYING COMPUTER SYSTEMS

A computing system is generally defined as any computer software application that performs a business function; the supporting database management system if any; the hardware on which it resides and that provides access to it; and the operating system that controls the hardware. Computing systems include hardware devices that reside within an organization or at a vendor site as well as software programs that are written and maintained by internal programmers, purchased from, and maintained by vendors, or reside at third-party processor sites.

Once the "universe" of computing systems in an organization has been identified, the systems must be categorized by criticality; essentially a risk analysis must be

performed on them. The risk analysis could prove to be very time-consuming. The best method for evaluating the risk of the computing systems must be determined. For some, it may be in terms of the total dollar value of items processed by the system, while for others it may be the total number of items processed, total cost or investment in the system, potential losses if the system were corrupted, a combination of these criteria, or some other factors that may be deemed appropriate. The method that makes the most sense for the industry, the size of the organization, and the number and complexity of the computing systems in the organization must be determined. Software packages can assist in performing risk analyses. Although risk analysis software can be useful for obtaining general risk rankings, human judgment must always be exercised to make the final determination as to what systems are the highest risk and should be audited next.

One way to create an inventory is to begin by surveying managers within each work group. If the organization is large, a written survey form may need to be created and sent to the managers. In a small organization, telephoning managers and verbally asking them for the required information may be a more efficient way to complete the survey. As the term *auditor* implies, one can often identify computing systems, especially those being proposed or those that are in the early stages of development, by what one hears during conversations with others in the organization or even through the grapevine.

1.9 BENEFITS OF A COMPUTING SYSTEMS INVENTORY

Once completed, the computing systems inventory can provide several useful benefits. First, as mentioned previously, it will help in assessing the size and complexity of the computing systems environment within the organization. Some computing systems of which one was unaware may be identified. Some of these systems may subject the organization to significant risks due to the relative ease and rapidity with which new systems can be purchased or developed internally at end-user sites. Often managers in end-user areas are too busy or may intentionally neglect to inform an auditing department or other interested parties of the development of new computing systems.

A second benefit of the computing systems inventory is that it can help to identify work areas where the same or similar data is being stored and utilized. In these cases, there may be opportunities for consolidation of data storage resources and data processing resources, potentially resulting in reduced expenses and increased efficiency. A third benefit is that the inventory can help both internal and external audit management in planning what computing systems to examine and in budgeting human resources and the necessary dollars to perform the examinations.

1.10 RISK ASSESSMENT

Now that the computing systems in an organization have been identified, one has the necessary information to begin performing a risk assessment of the IS environment. Additional data regarding the dollar amounts, transaction volume, and other information should be obtained to enable the ranking of the computing systems from most risky to least risky. It is a good idea to record all the computing system demographic information in a spreadsheet, database, or other audit planning application. The computing systems can then be sorted by various criteria, such as process owner, dollar volume, operating system, and application type. Often this can aid in audit efficiency and effectiveness by assisting in determining which audits need to be performed and the order in which they should be performed. As previously mentioned, special over-the-counter software applications are available to assist in the risk assessment process. However, such software is by no means a requirement. An internally developed spreadsheet or database application may be quite sufficient.

1.11 SELF-ASSESSMENT QUESTIONS

Q.1 What are the basics of computing systems? Explain each component with examples.
Q.2 Explain the basic components of computing systems with suitable examples.
Q.3 Describe Central Processing Unit (CPU) with examples.
Q.4 Write a note on the operating system.
Q5. Critically describe physical security control and logical security control with relevant examples.
Q.6 Explain the database management system (DBM) with examples.
Q.8 How would you identify the universe of computer systems in an organization?
Q.7 Describe each of the following:

i. Application programs
ii. Computer memory
iii. Computer system inventory
iv. Operating system

1.12 ACTIVITIES

- Make a list of computer and operating system manufacturers.
- Design a conceptual model of a database management system.

1.13 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised; Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research*, *21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly*, *26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal*, *5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, *14*(1), 43.

UNIT-2

INFORMATION SYSTEMS AUDIT PROGRAM; INFORMATION SYSTEMS SECURITY POLICIES, STANDARDS, AND/OR GUIDELINES

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

The following unit will give an insight overview of the information system audit program and silent features of information systems audit programs. This unit also describes information system security policies, standards, and information security guidelines. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- Information system audit program
- Advantages of audit programs
- Information systems security policies
- Information system security standards
- Information system security guidelines

2.1 INFORMATION SYSTEMS AUDIT PROGRAM

Audit programs are necessary to perform an effective and efficient audit. Audit programs are essentially checklists of the various tests that auditors must perform within the scope of their audits to determine whether key controls intended to mitigate significant risks are functioning as designed. Based on the results of the tests performed, the auditor should be able to determine the adequacy of the controls over a particular process. The audit program is designed to address the primary risks of virtually all computing systems. Therefore, the objective statement and steps in the program are general by design. Computing systems can have many different applications running on them, each with its own unique set of controls. However, the controls surrounding all computing systems are very similar. The IS controls in the audit program have been grouped into four general categories:

a. Environmental controls
b. Physical security controls
c. Logical security controls
d. IS operating controls

2.2 ADVANTAGES OF AUDIT PROGRAMS

- Audit programs can assist audit management in resource planning. For example, management can estimate the total number of hours required to perform an audit based on the expected amount of time required to perform each of the steps in the audit program.

- Audit programs can help promote consistency in tests performed on audits of the same process from one cycle to the next. During planning and preparation for an audit, audit programs used during the previous audit usually can be employed as the basis for the steps to be performed during the current audit. This does not apply in cases in which the process has never been audited before or where the process has changed significantly. In these cases, new audit programs must be created.

- Audit programs can also promote consistency in tests performed on controls that are common to all processes. For example, in many organizations, system security administrators perform additions, changes, and deletions of users and their access capabilities. Department managers are responsible for authorizing the access capabilities granted to their employees by these system security administrators. In these cases, it may be more practical to examine the system access capabilities of users as each process or department is audited rather than trying to examine the access capabilities of all users at one time.

- If an audit department elects to examine user access capabilities on a process or department basis, it would be useful to develop a standard audit program to help ensure that auditors are evaluating such capabilities consistently.

2.3 INFORMATION SYSTEMS SECURITY POLICIES

One of the key elements of the internal control environment within any organization is its information systems (IS) security policy. An IS security policy provides the high-level framework from which all other IS security-related controls are derived. Many of us assume that nearly all organizations have an IS security policy or something that would qualify as such.

Information systems security policies are high-level overall statements describing the general goals of an organization regarding the control and security of its information systems. Policies should specify who is responsible for their implementation. Policies are usually established by management and approved by the board of directors. Because most boards meet only monthly, changes to policies can often take several months to become official. If the change is significant, the board may request additional information or research before it will vote on the change. If the change is relatively minor, there may not be sufficient time in their agenda to address minor policy changes. For these reasons, it is important that the IS security policy not be too specific. For example, the policy should require that the organization provide adequate physical and logical security controls over computer hardware, software, and data to protect them against unauthorized access and accidental or unintentional damage, destruction, or alteration. However, the policy should not specify detailed controls, such as the minimum number of characters required for passwords, or the maximum number of unsuccessful sign-on attempts allowed before suspending a user ID. If this were the case, senior management would be constantly submitting policy change requests to the board. As we all know, often controls that were thought to be strong have been rendered inadequate by advances in technology. At one time, five-character passwords were thought to be sufficient for business applications. With hacking software available at little or no cost on the Internet, passwords of eight or more characters are now required in many organizations. Therefore, it is more practical to include detailed IS control requirements in the IS security standards of an organization. The policy is divided into five sections:

a. Purpose and responsibility
b. System procurement and development
c. Access terminals
d. Equipment and information security
e. Service bureau programs

a. Purpose and responsibility

The Company operates various forms of computing and telecommunications systems throughout its operations. For purposes of this policy, the term "systems" shall refer to all computer operations (mainframe, minis, micros, personal computers, and telecommunications) and any other functional areas in which data is transmitted via an electronic or telecommunications medium. The purpose of the Company's Information Systems Security Policy is to provide the essential guidelines for efficient electronic transaction processing and reporting services, management information systems, and appropriate customer information capabilities for management and the Board of Directors to effectively operate the Company. In addition, this policy is designed to ensure continuous support and improvement of the

computing and telecommunications systems of the Company. It shall be the responsibility of the President or his/her designated individual(s) and Senior Management Committee to manage the Company's computing and telecommunications systems.

The President shall establish an operating structure that optimizes the system's capabilities of the Company consistent with sound business practices. The various systems will be continually monitored to ensure the proper functioning and the ability to meet the current and future needs of the Company. The President and Senior Management Committee shall be responsible for and direct the feasibility studies regarding development, implementation, and system conversions, as well as the continued operation of the Company's computing and telecommunications systems.

b. System procurement and development

The Company's procurement, development, and operation of data processing systems (hardware and software) shall be managed by the President or his/ her designated individuals and the Senior Management Committee. The computing systems of the Company shall be constantly monitored and should a current and/or a future need for change be identified, the Company should follow the system life-cycle evaluation steps outlined on the next page.

- Scope definition—A description of the needs to be addressed
- Requirement definition—A description of the requirements of the end-user and the objective of the new development
- Review of alternative solutions
- System design
- System development
- System testing
- System monitoring

c. Access terminals

Management is authorized to install other dial-up access online terminals as may be required in the operations of the Company.

d. Equipment and information security

Proper security for the computer and telecommunications systems shall be established and maintained as necessary to protect the equipment and related data. The primary intent of protecting these systems from a breach of security shall be to limit unnecessary interruptions in system processing time and to prevent the corruption of Company data. The Company's mainframe computer room, as well as appropriate other computing and telecommunications system facilities as determined by management, shall be supported by an uninterrupted power supply, which will also function as a temporary source of power in the event of a power failure. The physical environment for these system facilities will be adequately protected from fire, smoke, and water. In addition, the Company will maintain and support the proper heating, ventilation, and air conditioning required by the various systems. Access to the systems will also be properly maintained and monitored by security personnel. All systems hardware and the costs of re-creating any lost data will be adequately insured.

- ***Information and Communication Security***

The Company is to maintain integrity and security controls for the protection of all computing and telecommunications systems, which is intended to also address the risks that arise from potential misuse of computing system resources. The establishment of these controls shall include, but not be limited to, the following steps:

- Logical access controls
- An information resource classification method
- Network and local access security
- Retention and disposal of information
- An incident reporting system to analyze errors and develop procedures to prevent future occurrences.
- Measures used to establish and/or enhance such controls should be appropriately justified as to their cost and financial benefit relative to the criticality and sensitivity of the information resources being protected.

- ***Contingency and Recovery*:**

Backup systems support contracts shall be established to protect the Company in the event of an unforeseen breakdown or catastrophe.

The Company is to develop and maintain a plan that addresses the risk that such events can occur. This shall require planning for alternate computing system processing options (facilities, equipment, etc.) and that the necessary procedures be established to successfully achieve each of these alternatives. This is to ensure that the Company can provide for business continuity. Minimum contingency requirements should include, but not be limited to, the following steps:

i. Identification of critical applications to determine their priority for recovery.
ii. Documented backup and recovery plan(s) that include all related or potentially affected information assets (and their probable/potential) effects on any/all operational areas).
iii. Test procedures at least once each year to evaluate the plan's effectiveness on information assets, personnel, and all other potentially affected operational areas.
iv. The Company shall maintain backup data at an off-site location to limit risk and allow for the timely recovery of data should on-site information be destroyed, corrupted, or for whatever reason made unusable.

e. Service bureau programs

The Company's service bureau agreements shall be drafted to require that such bureaus retained by the Company indicate a commitment to developing and maintaining computer application software in such a manner that system capabilities, as specified by the Company, are ensured and that appropriate record-keeping checks and balances are in place. The agreements should detail the level of support the service bureaus will provide with existing programs, new programs developed, and program updates. Consequently, the following steps are designed to facilitate positive interaction with all service bureaus being utilized:

- Programming requests by the Company shall be monitored as to the timeliness of response by the service bureaus, and where timeliness or quality of performance is questionable, the President or his/her designate shall evaluate alternatives for better performance.
- The Company, through its own as well as the service bureaus' verification systems, will ensure that the new system's software is operating correctly before conversions are made to standard operational use.
- The service bureaus' system software supplied will be supported by detailed documentation instructing the Company on operating and error recording procedures.
- In general, this policy is reasonably adequate. However, there are several opportunities where the policy could be changed to increase its overall effectiveness. Each section of the policy that contains an area that could be improved will be critiqued to demonstrate how an auditor could assess the adequacy of a policy and formulate recommendations to improve its overall effectiveness.

2.4 INFORMATION SYSTEMS SECURITY STANDARDS

Information systems security standards are minimum criteria, rules, and procedures established by senior management that must be implemented to help ensure the achievement of the IS security policy. They are implemented by staff (e.g., system security administrators and users) under the direction of management. Information systems security standards should specify the detailed requirements of each IS control. A few examples of detailed controls that should be specified in the standards would be an eight-character minimum password length, a 30-day password expiration period, and a requirement that passwords be composed of at least two alpha and two numeric characters.

Standards should not be specific to any computer platform (i.e., make, model, or operating system). Instead, they should be general enough to apply to all existing and proposed information systems that possess some form of logical and/or physical security. Whenever management deems that the standards need to be changed, the changes can be communicated to staff and implemented without the need for the approval of the board of directors. This enables the organization to react more quickly to technological advances that may have weakened pre-existing standards. About auditing, IS security standards provide a management management-approved benchmark or baseline against which the adequacy of controls applied to individual information systems can be assessed.

2.4.1 Sample Information Systems Security Standards

The following minimum IS security standards have been approved by senior management and are to be applied to applicable information systems within the organization:

1. Upon completion of the initial installation of software, the maiden password shall be changed by the system security administrator.

2. A backup system security administrator shall be designated and trained to ensure the continued operation of the system, even in the absence of the primary system security administrator.
3. System security administrators shall set parameters to require passwords to be a minimum of 8 alpha-numeric, case-sensitive characters in length.
4. Systems shall be designed so that passwords are masked (i.e., invisible) on workstation screens as they are entered by users.
5. Systems shall be designed so that password files are encrypted by a secure algorithm so that nobody, including system security administrators, can view them.
6. System security administrators shall set passwords to automatically expire within 60 days or less.
7. User IDs shall be suspended after three consecutive unsuccessful sign-on attempts.
8. Users shall be required to contact system security administrators to have their user IDs reset. Only system security administrators shall have the capability to reset user IDs.
9. User sessions shall be terminated after five minutes of inactivity.
10. Users shall not be allowed concurrent sign-on sessions.
11. System security administrators shall remove the user IDs of terminated or transferred users immediately upon notification from the user department manager and/or the Human Resources Department. Procedures shall require department managers to notify all applicable system security administrators when users terminate or transfer.
12. Department managers shall be responsible for training users not to share or divulge their passwords to anyone, write them down, post them in their workstations, store them in an electronic file, or perform any other act that could potentially result in their password being divulged.
13. System security administrators shall request user department management to review user access capabilities and certify in writing that the access capabilities of the users in their department are necessary to perform normal duties. This certification shall be performed at least annually, or more often if deemed necessary by senior management.
14. Logical security-related events shall be logged by the system, and the log shall be continuously monitored by system security administrators for potential acts of unauthorized access. Examples of logical security-related events include unsuccessful sign-on attempts, addition/ deletion of users and changes to their access capabilities, resetting of passwords, and system restarts. There are probably many other events that could be logged.
15. Business resumption procedures shall be fully developed, tested, and documented by management in collaboration with system security administrators and other key staff members. The business resumption plan shall provide for complete system backups weekly, complete data backups daily, and rotation of backup media to a secure off-site facility on a three-or-more generation rotation cycle.
16. Adequate insurance coverage shall be maintained over the hardware, operating system, application software, and data. Hardware should be covered at replacement cost. The operating system, application software, and data shall be covered for the costs of re-creation. Lost revenues directly resulting from hardware failure and/or loss of the operating system, application software, and data during covered events shall be fully covered.

17. For custom applications developed by external software vendors, contracts shall specify that the source code shall be held in escrow by an independent third party and that the source code shall be released to the purchaser in the event the vendor ceases to support the software or otherwise violates any "significant" terms of the contract. Other items to be included in vendor contracts shall include the contract period, annual maintenance costs, types of maintenance provided, service level standards (i.e., response time requirements), and so on.
18. Vendor-developed applications acquired in the future should be contractually required to include programming that enables the standards to be deployed upon installation.
19. Confidential information, including passwords, shall be encrypted by a secure algorithm during electronic transmission.
20. System security administrators shall install software that automatically checks for viruses using a current virus pattern file. The virus software parameters should be set to examine all memory sectors of computers, including boot sectors, all permanent storage devices, and all incoming files. The software shall also be set to notify the system security administrator of any viruses identified.
21. User access shall be restricted to normal work hours and days (e.g., 6 A.M. to 6 P.M., Monday through Friday). Overnight and weekend access shall require advance written approval from the management responsible for the system.
22. User access shall be restricted to specific workstations. (*Note*: Each workstation is identified by a unique node number.)
23. The above list of IS security standards is general by design. Depending on the nature of the organization, it will likely be necessary to recommend additional standards that will help strengthen the IS control environment. As with policies, it may be necessary to recommend a different set of standards for each subsidiary, division, or operating unit.

2.5 INFORMATION SYSTEMS SECURITY GUIDELINES

Information systems security guidelines are also established by senior management and are intended to help ensure the achievement of the IS security policy. Guidelines are similar in format to standards in that they provide detailed specifications for individual IS controls. Where they differ from standards is in their implementation. In some firms, management may direct staff to implement only those guidelines that they judge to be pertinent or useful. In others, they may be understood to be the equivalent of standards. Since guidelines are not necessarily required by management to be implemented, they can prove to be somewhat of an anomaly to auditors. For example, in a firm that has IS security guidelines but no standards, an auditor may use the guidelines as a benchmark against which the adequacy of controls of a particular information system can be assessed. When recommending improvements in those controls to line management in charge of the system, using the guidelines as the benchmark, the auditor may encounter resistance to change because line management does not consider the guidelines to be requirements. It is for this reason that the use of the term guidelines is inappropriate when referring to IS security controls. All firms should develop IS security standards that are clearly defined and enforceable. It should not be surprising when one is unable to locate adequate IS security policies, standards, or guidelines within an organization. Based on personal experience

and discussions with numerous colleagues in various professional auditing associations, it appears that many companies do not have any IS security policies, standards, or guidelines. Even in firms that do, the policies, standards, and guidelines are often inadequate or do not address many risks associated with information systems.

2.6 SELF-ASSESSMENT QUESTIONS

Q.1 What is an information system audit program? Highlight the advantages of audit programs with examples.
Q.2 Write a detailed note on information system security policies.
Q.3 Define the term standard. Also, evaluate information systems security standards with examples.
Q.4 Enlist information system security guidelines with examples.

2.7 ACTIVITIES

- Design an information system audit program.
- Suggest policies for information security systems.
- Enlist guidelines for information system security.

2.8 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised, Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research*, *21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly*, *26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal*, *5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, *14*(1), 43.

UNIT-3

Auditing Service Organization Applications; Assessing the Financial Stability of Vendor Organizations, Examining Vendor Organization Contracts, and Examining Accounting Treatment of Computer Equipment and Software

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

Many firms employ the services of external organizations to provide business applications and data processing resources that would otherwise be too expensive or time-consuming to develop and maintain internally. In this unit, the auditing service organizations, and services auditor reports of different countries are discussed with examples. This unit also covers topics on how to use service auditor reports for internal audits and reports of independent auditors. A description of relevant policies and procedures, control objectives by service organization management, and client control considerations are also described in detail in the following unit. Furthermore, this unit also discussed assessing procedures of financial stability of vendor organizations, examining vendor organization contracts, and assessing accounting treatment of computer hardware and software. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- Applications of auditing service organizations
- Service auditor reports of developed countries
- Use of service auditor reports for internal auditors
- Report of independent auditors
- Policies related to service auditors
- Assessing the financial stability of vendor organizations

3.1 AUDITING SERVICE ORGANIZATION APPLICATIONS

Many firms employ the services of external organizations to provide business applications and data processing resources that would otherwise be too expensive or time-consuming to develop and maintain internally. These external organizations are often referred to as service organizations, service bureaus, or third-party processors. Numerous service organizations provide a variety of applications to virtually all sectors of industry and government. These include services for payroll processing, mortgage loan servicing, investment safekeeping, software development and maintenance, automated teller machine (ATM) transaction processing, check processing, electronic bill payment, wire transfers, credit card operations, and trust services.

Service organizations enjoy economies of scale by developing and maintaining applications and computer systems that may be used by hundreds or thousands of client companies. By processing high volumes of client transactions, the cost to process each transaction through a service organization often is significantly less than if each client were to hire a programming and development staff and purchase or lease the computer hardware necessary to process the transactions. As a result of technological advances, changes in laws and regulations, and other business risks, a company might invest significant financial resources in a major computer system only to find it obsolete in a few years. Similarly, a company may hire a programming staff to develop and maintain one or more custom applications internally. Only after years of project delays and application design flaws does the firm realize that it would have been more cost-effective to have contracted with a service organization to provide the application. This is not to say that companies should not maintain internal systems development and maintenance staff and computer systems. Many large organizations are very successful at creating their applications. There are benefits and drawbacks to both alternatives. While service organizations often process transactions at a lower cost than their clients, they must try to maintain applications that meet the needs of all their clients. Some clients may require the service organization to develop customized modules and modifications to the original application to meet unique product and service needs. Service organizations can partially offset these needs by incorporating tables and parameters into their applications.

These tables and parameters can then be customized by each client. However, there will always be clients whose needs cannot be anticipated when the tables and parameters are designed or whose needs are so unique that changing the primary application to meet those needs could adversely affect other clients. In these cases, special modules must be designed and integrated with the primary application at the client site while the primary application is left intact. Thus, service organizations must constantly monitor the changing needs of their clients and update their applications to meet those needs.

If there are many clients with specialized requirements, service organizations often become backlogged and thus are not able to meet the needs of all their clients promptly. They must prioritize their client requests. Clients that are the greatest source of revenue

for the service organization are often given top priority. This places smaller clients at a disadvantage with their competitors who may be utilizing a different service organization or who develop and maintain their applications. Sometimes the backlogs can be months or even years. In the worst cases, service organizations may simply have to reject a client request. Fortunately, most client companies form user groups to discuss their successes and difficulties with the service organization application. If several small firms have the same programming change request, they may be able to form an alliance that is strong enough to leverage their request ahead of a large client. The threat of clients leaving and taking their business to a competing service organization is an effective means of getting programming requests implemented. As with any business, a service organization can survive only if it is managed in such a way that it can satisfy the requirements of its clients efficiently and effectively. The problems are not unique to service organizations.

Many companies maintain an internal staff of application development and maintenance personnel. These companies can create customized applications without relying on outside service organizations. They do not have to compete with other firms to implement specialized programming requests. These benefits often enable companies to tailor their applications to meet the exact needs of their products and services on time. However, the same pitfalls that face service organizations can occur within companies that program their applications. For example, many firms have numerous departments, each utilizing different applications to process their information. When new systems or programming changes to existing systems are necessary, each department submits a request to the information systems (IS) development or maintenance area for action.

Information systems areas are faced with limited resources and, like service organizations, must prioritize the requests of the individual departments. In theory, the requests promising the most financial benefit to the organization are given top priority. Often, however, the departments with the greatest financial or political leverage get their requests completed ahead of other departments. When a company is significantly downsizing, the backlog can reach months or years.

3.2 SERVICE AUDITOR REPORTS

Most major service organizations contract with an independent auditing firm to express an opinion on the adequacy of policies and procedures within the service organization that may affect the internal control environment at the client organization. In some cases, the independent auditor may be contracted to perform additional tests to determine whether such policies and procedures are operating effectively within the service organization. These service auditor reports provide some assurance to clients that adequate controls exist within the service organization to ensure the reliability, integrity, and confidentiality of client customer information. Professional auditing standards about the issuance of service auditor reports in most developed countries are similar but by no means identical. Some standards provide more assurance than others. Therefore, when examining a service auditor report, the reader must be cognizant of the country in which the service organization is domiciled. The following paragraphs examine the status of

professional auditing standards about the different types of service auditor reports issued in the United States, Canada, the United Kingdom, and Australia.

3.2.1 United States

In the United States, a service organization may hire an independent external auditor to express one of two types of opinions on policies and procedures at the service organization that may be relevant to the internal control structure of organizations that utilize its services. The reporting and testing requirements for external auditors who perform such engagements are dictated by Statement on Auditing Standards 70 (SAS 70), issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 is entitled "Service Organizations" and is effective for service auditors' reports dated after March 31, 1993. (*Note:* The SAS 70 name was amended, effective December 1999, from "Reports on the Processing of Transactions by Service Organizations" by SAS 88 entitled "Service Organizations and Reporting on Consistency.") The first type of report expresses, among other things, the auditor's opinion as to whether relevant policies and procedures were placed in operation at the service organization "as of a specific date." This type of report *does not* express an opinion as to the operating effectiveness of such policies and procedures. The second type of report expresses the auditor's opinion as to whether relevant policies and procedures were in place at the service organization *and whether such policies and procedures were operating effectively.* To formulate an opinion under the second type of report, the auditor is required to perform various tests to confirm that the policies and procedures at the service organization are functioning properly. SAS 70 goes on to state that "To be useful to user auditors, the report should ordinarily cover a minimum reporting period of six months." SAS 70 supersedes SAS 44, which was entitled "Special-Purpose Reports on Internal Accounting Control at Service Organizations" and was required for special purpose reports on internal accounting control dated after December 31, 1982. The primary difference between SAS 70 and SAS 44 is that SAS 70 specifies a minimum reporting period of six months. Under SAS 44, a required period was not specified. Rather, the necessary testing period was left to the judgment of the auditor. SAS 44 reports usually covered a period of approximately two to four months, except in cases in which significant control weaknesses were identified.

3.2.2 Canada

The Canadian equivalent of SAS 70 is Section 5900 of the *Handbook of Auditing* published by the Canadian Institute of Chartered Accountants (CICA). Section 5900 is entitled "Opinions on Control Procedures at a Service Organization" and is effective for engagements covering periods on or after July 1, 1987. Like SAS 70, Section 5900 details two types of opinions that external auditors may express. One pertains to the "design and existence of control procedures at a service organization," while the second pertains to the "design, effective operation, and continuity of control procedures at a service organization." The first type of opinion requires auditors to attest only to the design and existence of control procedures "as at a point in time." No opinion is expressed regarding the operating effectiveness of the control procedures. The second

type of opinion requires auditors to perform tests and obtain management representations regarding the effective operation of control procedures "throughout the specified period." Unlike SAS 70, Section 5900 does not specifically recommend a six-month testing period. The period necessary to obtain assurance as to whether control procedures were operating effectively is left to the professional judgment of the external auditor. However, a six-month testing period may be inferred from the example service auditor's report in Section 5900, which states that the auditor "performed tests of the effectiveness of those control procedures for the period from January 1, 19X1 to June 30, 19X1."

3.2.3 The United Kingdom

In September 1994, the Faculty of Information Technology (FIT) of the Institute of Chartered Accountants in England and Wales (ICAEW) issued Technical Release FIT 1/94, which bears the same name as SAS 70, "Reports on the Processing of Transactions by Service Organizations." FIT 1/94 is intended to apply only to matters relating to service organizations that provide data processing services, although some of its principles may also be relevant to other types of services provided by service organizations. FIT 1/94 is quite like SAS 70 and Canada's Section 5900. The auditor may issue an opinion on the policies and procedures of the service organization only or the policies and procedures as well as tests of compliance with the policies and procedures. Control objectives for the service organization are to be specified in the report, including their source. For opinions with tests of compliance, FIT 1/94 specifies that "To be effective for user auditors, the report would normally need to cover a minimum reporting period of six months."

A guidance document like FIT 1/94 was released by the Financial Reporting and Auditing Group (FRAG) of the ICAEW in May of 1994. Technical Release FRAG 21/94, entitled "Reports on Internal Controls of Investment Custodians Made Available to Third Parties," is smaller in scope than FIT 1/94. It focuses primarily on custodial activities related to investment businesses. Other activities of such businesses are not addressed. The report under FRAG 21/94 includes the auditor's opinions on whether "control policies and procedures were suitably designed to achieve the specified control objectives" and that "the related control objectives were achieved during the period. "Unlike FIT 1/94, FRAG 21/ 94 does not require a minimum reporting period. Also, the adequacy of the control objectives is not assessed by the auditor. Appendix III of FRAG 21/94 includes an illustrative example of a management report, which includes a section on control policies and procedures established to ensure that the control objectives are achieved. Among these control policies and procedures, FRAG 21/94 includes a section on the "security and integrity of computer systems" objective.

This section lists 11 control areas:

1. Unauthorized admission to data processing areas

2. Restricted access to operating systems, utility software, applications, communications software, and data
3. Logging and detection of unauthorized system access attempts
4. Data entry accuracy and integrity of information transmitted over networks
5. Reconciliation of data output
6. Definitions and descriptions of all reports
7. Written procedures to ensure the accuracy, completeness, and authorization of all transactions
8. Accurate audit trails
9. Adequate documentation of all data processing systems
10. Adequate archiving and safe storage of records and programs
11. Implementation of adequate contingency procedures

These control areas are comprehensive and can be applied to almost any type of IS control environment. Therefore, they can serve as a useful reference to external auditors.

3.2.4 Australia

Australia did not have an auditing standard applicable to service auditors as of the writing of this book. The Australian Accounting Research Foundation (AARF) has recognized the lack of such a standard as a deficiency and is in the process of drafting an Audit Guidance Statement (AGS) on Outsourcing Entities. The AARF Project Manager responsible for the new AGS on outsourcing entities reported that it focuses on three concepts:

1. Applicable to outsourcing arrangements, including but not limited to service entity arrangements (i.e., service organizations).
2. Encourages "effectiveness" reporting of controls rather than "design-only" reporting
3. Encourages "period-of-time" reporting rather than "point-in-time" reporting

Item 1 is more comprehensive than SAS 70, Section 5900, or FIT 1/94. Items 2 and 3 are consistent with the second type of SAS 70 report, which expresses the auditor's opinion regarding whether relevant policies and procedures were in place at the service organization and whether such policies and procedures were operating effectively. The Australian AGS project manager also stated that the new AGS is based largely on an AARF invitation to comment (IC) document entitled "Reporting on Internal Control,"

which was prepared by the Auditing Standards Board of the AARF in April 1996. Some of the pertinent highlights of the IC document include:

- Reporting on internal controls is considered a specific type of performance auditing and should be read in conjunction with AUS 806, "Performance Auditing," and AUS 808, "Planning and Performance Audits," to obtain a more comprehensive understanding.

- AUS 806 and AUS 808 provide generic principles, practices, and guidance relevant to auditors reporting on internal controls.

- The report on internal controls is a separate engagement from the financial report audit.

Although they may be conducted in conjunction with each other, each requires a separate report.

The IC adopts a broad definition of internal controls, which includes:

1. Effectiveness, efficiency, and economy of operations
2. Reliability of management and financial reporting
3. Compliance with applicable laws and regulations and internal policies.

This definition of internal controls is consistent with the frameworks of the Committee of Sponsoring Organizations (COSO) in the United States, the Criteria of Control Board (CoCo) in Canada, and the Cadbury Committee in the United Kingdom. The IC document is based on the premise that any evaluation of the effectiveness of internal controls is inseparable from a consideration of the objectives to which the internal controls are directed and the risks that threaten the achievement of those objectives. Criteria that consider these objectives and risks must be identified before a meaningful opinion about effectiveness can be expressed. Without such criteria, an auditor's report would be open to widely divergent and subjective interpretations of individual users.

The tests of operating effectiveness should be performed over a period that is adequate to determine that the internal controls are operating effectively. The period over which the auditor would perform tests of operating effectiveness is a matter of judgment. Based on the foregoing information, it is reasonable to expect that the AARF Audit Guidance Statement on Outsourcing Entities will provide as much or more guidance to external auditors who prepare reports on the internal control environments of Australian service organizations as do SAS 70, Section 5900, and FIT 1/94. As part of the AGS, it would also be reasonably expected that internal controls over information systems within service organizations will be adequately addressed.

In January 1997, the Auditing Standards Board of the AARF issued AGS 1026 entitled "Superannuation Funds—Auditor Reports on Externally Managed Assets." AGS 1026 is very like the FRAG 21/94 document in the United Kingdom in that it provides some guidance on IS controls, albeit only for a specific type of entity. AGS 1026 is directed primarily at superannuation (pension) fund auditors and is limited to an explanation and application of existing standards to circumstances in which superannuation fund auditors may need to obtain necessary audit evidence concerning externally managed assets

through reports issued by the auditor of an external manager. The guidance is intended to provide a clearer indication of the needs of superannuation fund trustees and auditors and seeks to achieve greater consistency in their requests for reports by the auditors of external managers.

The report under AGS 1026 includes the auditor's opinions on whether the external superannuation fund manager maintained effective internal controls for the assets under management as of the period ending date, based on the criteria set out in a Management Report on Internal Controls, which is attached to the audit report. AGS 1026 does not specify a minimum reporting period, and the adequacy of management's control criteria is not required to be assessed by the auditor.

Like FRAG 21/94, the AGS 1026 includes an illustrative example of a Management Report on Internal Controls, which includes a section on control policies and procedures established to ensure that the control objectives are achieved. Among these control policies and procedures, AGS 1026 includes a section on the objective entitled "Security and Integrity of Computer Systems." This section lists 10 control areas, most of which are specified in FRAG 21/94:

1. Unauthorized admission to data processing areas
2. Restricted access to operating systems, utility software, applications, communications software, and data.
3. Logging and detection of unauthorized system access attempts
4. Data entry accuracy and integrity of information transmitted over networks
5. Written procedures to ensure the accuracy, completeness, and authorization of all transactions.
6. Accurate audit trails
7. Adequate documentation of all data processing systems
8. Adequate archiving and safe storage of records and programs
9. The formal process for testing new programs before they are released
10. Implementation of adequate contingency procedures

Item 9 is a control area not included in the FRAG 21/94. The formal process for testing new programs before they are released is a control area worthy of specific mention. This control area is applicable not only in the context of superannuation funds but for all IS control environments. Another difference between AGS 1026 and FRAG 21/94 is that the AGS excludes the two control areas about the reconciliation of data output and definitions and descriptions of all reports (control areas 5 and 6 under FRAG 21/94). It appears that these items were excluded because they are more operational rather than specifically about the

security and integrity of computer information systems. Therefore, their exclusion should not be considered a significant detriment to the guidance of AGS 1026.

Like FRAG 21/94, the control areas of AGS 1026 are quite comprehensive and can serve as a useful reference and be applied by auditors and interested parties to almost any type of IS control environment. Internal auditors and other interested parties who utilize SAS 70, Section 5900, FIT 1/94, and similar reports should be alert to the fact that even if an external auditor expresses an unqualified or unreserved opinion as to the operating effectiveness of relevant policies and procedures at a service organization, there may exist relevant policies and procedures upon which the external auditor was not hired to express an opinion. SAS 70 states, "The management of the service organization specifies whether all or selected applications and control objectives will be covered by the tests of operating effectiveness." Therefore, it is important to carefully examine the report to understand the areas tested and to determine whether an organization should request additional assurance from the service organization regarding the existence and operating effectiveness of policies and procedures that were not tested in the original service auditor's report.

3.3 USE OF SERVICE AUDITOR REPORTS FOR INTERNAL AUDITS

Once an organization has determined that it will contract with a service organization, one of the first steps that the project development team at the client organization should perform is to examine a copy of the most recent service auditor's report from each of the bidding service organizations. This examination should take place before any contract is entered into with the service organization. Significant control weaknesses in a service auditor's report could signal that the service organization cannot provide client organizations with an adequate level of service and information protection. If a service organization does not have a service auditor's report prepared, the client organization should seriously consider dropping that service organization from consideration. The lack of a service auditor's report may also signal that internal controls at the service organization could significantly jeopardize client operations. The internal control environment can change over time at a service organization, as with any organization. Therefore, even after a service organization has been contracted and its services have been deployed, process owners and internal auditors at the client organization should examine each service auditor's report that is prepared. Although professional auditing standards do not require the preparation of a service auditor's report for all service organizations, most reputable service organizations have one prepared annually or at least biannually. To help defray a portion of the costs of hiring service auditors to prepare the reports, some service organizations charge client organizations a fee for each copy of the service auditor's report. The internal audit department should obtain a copy of the service auditor's report for each service organization utilized by the client organization on an annual basis or whenever the reports are prepared.

Service auditor reports can be quite lengthy (up to 100 pages or more) and consist of several sections. Although professional standards do not specify how service auditor reports are to be organized, they generally include four pieces of information:

1. Report of independent auditors.
2. Description of relevant policies and procedures (provided by client organization management)
    a. General description of operations, including an organization chart
    b. Description of control environment elements
    c. Description of transaction flow, including flow charts
    d. Application overviews
    e. Program change procedures
    f. Regulatory compliance information (if applicable)
3. Control objectives as specified by client organization management and results of service auditor's tests of the operating effectiveness of the control objectives.
4. Client control considerations

3.4 REPORT OF INDEPENDENT AUDITORS

The independent auditor's report includes an opinion statement on the adequacy of policies and procedures and if contracted by the service organization, an opinion on whether the policies and procedures were operating with sufficient effectiveness during the specified period. Internal auditors at client organizations should examine the opinion closely. If the opinion is "qualified" due to one or more significant control weaknesses at the service organization, the internal auditor should determine whether the weaknesses significantly affect the internal control environment at the client organization. If so, the internal auditor should recommend that management communicate their concern to the service organization and determine whether the service organization has implemented necessary changes to resolve the control weaknesses. If the necessary changes have not been implemented, the internal auditor should recommend that management consider changing to another service vendor that does not have any significant control weaknesses that adversely affect the internal control environment at its client organizations. If the original service organization states that the control weaknesses have been corrected, the internal auditor should perform alternative tests to confirm the changes. The internal auditor should also

confirm that the same control weaknesses are not mentioned in the next service auditor's report. The existence of perpetual control weaknesses within a service organization could be an indication that its overall control environment is weak, thereby increasing the risk that transactions could be improperly processed; service could be interrupted; data could be lost, damaged, or divulged to unauthorized parties; and the service organization could suffer a significant enough loss to drive it out of business.

3.5 DESCRIPTION OF RELEVANT POLICIES AND PROCEDURES AND OTHER INFORMATION

Internal auditors need to read this section of a service auditor's report to gain a better understanding of the service organization and its control environment. Quite often this information can provide more complete information about the service organization and its applications than the process owner at the client organization. This section commonly includes a general description of operations, a description of control environment elements, and a description of the flow of transactions. The general description of operations usually consists of a narrative overview of the corporate structure of the service organization, an overview of corporate operations, and a general description of each applicable application. An organization chart is often included, or it may be provided in an appendix.

Control environment elements are those that should be in place at the service organization to provide reasonable assurance that client organization transactions and data are processed in a timely, accurate, and secure manner. Some service auditor reports describe the functions of key departments supporting the overall control environment. Examples of such key departments include Human Resources, Internal Audit, Client Support, Product Delivery, Research and Development, and Product Management. Other service auditor reports instead may describe the policies and procedures surrounding specific control objectives specified by the management of the service organization.

The description of the flow of transactions is a high-level narrative of how the application processes transactions and generates output reports and other documents for the client organizations. Flow charts may be included in this section or an appendix. Application overviews are narrative descriptions of the various services or functions that each application performs. In some cases, complex primary applications are supported by one or more secondary applications. If so, overviews of these secondary applications would also be provided. Program change procedures at the service organization exist to help ensure that changes have been properly authorized, documented, tested, and placed into production. The procedures may be described in narrative form with an accompanying flow chart or may simply be included as a flow chart in an appendix. Depending on the industry to which the service organization supplies applications, a description of policies

and procedures that help ensure regulatory compliance may be provided. The format will vary with the nature of the laws or regulations being described.

3.6 Control objectives as specified by service organization Management

Control objectives are specified by the service organization's management. However, service auditors play a significant role in consulting with management to ensure that the control objectives specified address the primary risks associated with the service organization's operations. Following each control objective is a detailed description of the policies and procedures purported to be in place to ensure that the control objective is attained.

Management of the service organization also provides this information. For service auditor reports that include the auditor's opinion on the operating effectiveness of the policies and procedures placed in operation, the service auditor specifies the tests performed to gain reasonable, but not absolute, assurance as to their effectiveness. These tests typically include inquiries with management and staff of the service organization, sample tests of individual transactions, examinations of system access controls, assessment of segregation of duties, observation of service organization operations, and so on.

3.7 CLIENT CONTROL CONSIDERATIONS

From the perspective of the client organization, the most important information contained in a service auditor's report is the client control considerations. Client control considerations are procedures that the service organization recommends that each client organization implement. These controls complement the controls at the service organization to enhance the level of control over client organization transactions and data. The controls at the client organization and the service organization comprise the overall control environment for the process being evaluated. Within a service auditor's report, client control considerations are sometimes described immediately after each description of policies and procedures and tests performed. Client control considerations may also be grouped in a separate section or a matrix.

When performing an audit of a process that utilizes a service organization, the internal auditor should examine the service auditor's report and confirm that each client control consideration has been implemented at the client organization. If not, the auditor should determine the reason the client control considerations were not implemented, assess the potential risks if the controls continue to be ignored, and then make appropriate recommendations based on the information they have gathered.

3.8 ALTERNATIVES TO SAS 70-TYPE AUDITS

With the proliferation of the Internet and e-commerce, the need arose for alternatives to the traditional SAS 70-type audit. Traditional SAS 70-type audits are typically large in scope, are time-consuming, and are more appropriate for large organizations that perform high-volume transaction processing for multiple commercial clients. They are designed to provide detailed information and assurance to auditors of client organizations about controls at the service organization that might affect the financial statements of client organizations. The detailed information includes a description of the IS environment, the testing procedures performed by the service auditor, and the results of the tests. But many service providers, such as small application service providers or website hosting companies, cannot afford SAS 70-type audits or hire an internal IS audit staff. In other cases, non-service provider organizations engaged in e-commerce or other Internet-based commercial activities want independent assurance that their internal systems are reliable and secure, and they want to be able to communicate their secure status to their customers and shareholders to alleviate their security concerns. Some organizations simply want independent assurance that their systems are reliable and secure, beyond what there is security team or even their internal IS auditors are reporting. To respond to these needs, several different types of "certifications" have been developed. Most allow the organizations that meet the certification standards to post an electronic certification or seal on their websites.

The following sections briefly describe five of the more common certifications: TruSecure, SysTrust, WebTrust, BBBOnline, and TRUSTe.

a. TruSecure®

TruSecure Corporation (formerly ICSA and originally known as NCSA) is a worldwide leader in security assurance solutions for Internet-connected organizations. TruSecure was one of the first organizations to offer a website certification service. The primary criteria for the TruSecure certification are:

- Use of adequate physical and logical security mechanisms that address the client's desired "security posture." The security mechanisms include written and implemented access control, antivirus, firewall, backup, and redundancy policies and procedures.

- Documented use of standard access controls, encryption mechanisms, and informed consent of data usage that ensure confidentiality of all back-end transactions and session traffic.

- TruSecure-evaluated site documentation, on-site verification, remote testing, and random spot-checking for annual compliance.

One unique aspect of the TruSecure certification is that it provides a small amount of insurance for certified websites in the event of a security breach. For more information about the TruSecure certification, see their website at www.trusecure.com.

b. SysTrustSM

SysTrust is a service jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) that enables qualified public accountants with the necessary IS skills to assure that a client's system is reliable. SysTrust Version 1.0 was released in 1999, and Version 2.0 was issued in 2000. SysTrust has 4 principles and 58 criteria organized:

Availability. The system is available for operation and uses at times outlined in service-level statements or agreements. This principle requires testing 12 detailed criteria that are grouped into 3 categories.

Security. The system is protected against unauthorized physical and logical access. This principle requires testing 19 detailed criteria that are grouped into 3 categories.

Integrity. System processing is complete, accurate, timely, and authorized. This principle requires testing of 14 detailed criteria that are grouped into 3 categories.

Maintainability. The system can be updated when required in a manner that continues to provide for system availability, security, and integrity. This principle requires testing of 13 detailed criteria that are grouped into 3 categories.

The SysTrust principles and criteria can be applied to all types of systems. SysTrust defines a system as an infrastructure of hardware, software, people, procedures, and data that produce information in a business context. As with SAS 70-type audits, the auditor issues a SysTrust opinion letter. SysTrust opinions may be unqualified or qualified. Contrary to SAS 70-type audits, client organizations do not receive details about the IS environment, testing procedures, and results of testing. For more information about the SysTrust service, see the AICPA website (*www.aicpa.org*) or the CICA website (*www.cica.ca*). Also, Boritz et al. have published an excellent article introducing the new SysTrust assurance service.

c. WebTrustSM

WebTrust is a family of services jointly developed by the AICPA and CICA that enables qualified public accountants with the necessary IS skills to assure that client websites that conduct business-to-consumer and business-to-business electronic commerce transactions meet standards for one or more of various principles. An unqualified opinion letter must be earned from the auditor before the WebTrust seal can be displayed on the client's website.

WebTrust Version 1.0 was released in 1997 with the first website earning the seal in the spring of 1998. Version 2.0 was issued in 1999, and Version 3.0 in 2000. Version 3.0 enables auditors to issue an opinion and corresponding seal on individual principles or combinations of principles. An entity must be able to demonstrate five WebTrust 3.0 principles. The detailed criteria within each principle are organized into four broad areas: disclosures, policies, procedures, and monitoring.

Online Privacy Principle. The entity discloses its privacy practices, complies with such privacy practices, and maintains effective controls to provide reasonable assurance that personally identifiable information obtained because of electronic commerce is protected in conformity with its disclosed privacy practices.

Security Principle. The entity discloses its key security practices, complies with such security practices, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security practices.

Business Practices/Transaction Integrity Principle. The entity discloses its business practices for electronic commerce, executes transactions in conformity with such practices and maintains effective controls to provide reasonable assurance that electronic commerce transactions are processed completely, accurately, and in conformity with its disclosed business practices.

Availability Principle. The entity discloses its availability practices, complies with such availability practices, and maintains effective controls to provide reasonable assurance that electronic commerce systems and data are available in conformity with its disclosed availability practices.

Confidentiality Principle. The entity discloses its confidentiality practices, complies with such confidentiality practices, and maintains effective controls to provide reasonable assurance that access to information obtained because of electronic commerce and designated as confidential is restricted to authorized individuals, groups of individuals, or entities in conformity with its disclosed confidentiality practices. In addition to these certifications, certification authorities (CAs) can earn a specialized WebTrust seal, which has three principles:

- *Business Practices Disclosure*. The CA discloses its key and certificate life-cycle management business and information privacy practices and provides its services following its disclosed practices.

- *Service Integrity*. The CA maintains effective controls to provide reasonable assurance that subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and that the integrity of keys and certificates it manages is established and protected throughout their life cycles.

- *Environmental Controls.* The CA maintains effective controls to provide reasonable assurance that subscriber and relying on party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure; the continuity of key and certificate management operations is maintained; and CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity. For more information about the WebTrust family of services, see the AICPA website (*www.aicpa.org*) or the CICA website (*www.cica.ca*).

d. BBBOnline®

BBBOnline offers two website certifications, one for reliability and one for privacy. The following are the general requirements of each program:

- **BBBOnline Reliability Program Requirements**

Become a member of the Better Business Bureau (BBB) where the company is headquartered. Provide the BBB with information regarding company ownership and management and the street address and telephone number at which it does business, which may be verified by the BBB during a visit to the company's physical premises. Be in business for a minimum of one year (an exception can be made if a new business is a spinoff or a division of an existing business, which is known to and has a positive track record with the BBB). Have a satisfactory complaint-handling record with the BBB.

Agree to participate in the BBB's advertising self-regulation program and to correct or withdraw online advertising when challenged by the BBB and found not to be substantiated or not in compliance with children's advertising guidelines. (The BBB does not preclear or preapprove online advertising. Its local and national advertising review programs are described on the BBB's website, and complaints about online advertising brought by consumers, competitors, or public officials may be filed online with the BBB.) Agree to abide by the BBB Code of Online Business Practices and to co-operate with any BBB request for modification of a website to bring it into accordance with the code. Respond promptly to all consumer complaints. Agree to dispute resolution, at the consumer's request, for unresolved disputes involving consumer products or services. For more information about the BBBOnline certifications, see the BBBOnline website at *www.bbbonline.com*.

e. TRUSTe™

TRUSTe is an independent, nonprofit privacy organization whose mission is to build users' trust and confidence in the Internet and, in doing so, accelerate the growth of the Internet industry. It was founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium, which act as independent, unbiased trust entities. The TRUSTe privacy program attempts to bridge the gap between users' concerns over privacy and websites' desire for self-regulated information disclosure standards. TRUSTe issues two different "trust marks."

f. TRUSTe (Standard)

Members' websites must adhere to established privacy principles and agree to comply with ongoing TRUSTe oversight and consumer resolution procedures. Privacy principles embody fair information practices approved by the U.S. Department of Commerce, the Federal Trade Commission, and prominent industry-represented organizations and associations. The principles include:

- Adoption and implementation of a privacy policy that considers consumer anxiety over sharing personal information online.
- Notice and disclosure of information collection and use practices.
- Choice and consent, allow users to exercise control over their information.
- Data security, quality, and access measures to help protect the security and accuracy of personally identifiable information.

All websites that bear the TRUSTe Trustmark must disclose their information collection and privacy practices in a straightforward privacy statement, generally a link from the home page. More than one Trustmark may be displayed if personal information privacy practices vary within the site.

g. TRUSTe children's privacy seal requirements

Websites directed at children under 13 must meet all regular program requirements and must also *not* perform the following:

- Collect online contact information from a child under 13 without prior verifiable parental consent or direct parental notification of the nature and intended use of this information, which shall include an opportunity for the parent to prevent the use of the information and participation in the activity. Where prior parental consent is not obtained, online contact information shall be used only to directly respond to the child's request and shall not be used to re-contact the child for other purposes.
- Collect personally identifiable offline contact information from children under 13 without prior verifiable parental consent.
- Distribute to third parties any personally identifiable information collected from a child under 13 without prior verifiable parental consent.
- Give the ability to children under 13 to publicly post or otherwise distribute personally identifiable contact information without prior verifiable parental consent and make best efforts to prohibit a child from posting any contact information.
- Entice a child under 13 by the prospect of a special game, prize, or other activity to divulge more information than is needed to participate in such activity.

The site must also place prominent notice where personally identifiable information is collected, requesting the child to ask a parent for permission to answer the questions. For more information about the TRUSTe certification, see the Electronic Frontier Foundation website at *www.eff.org*.

3.9 ASSESSING THE FINANCIAL STABILITY OF VENDOR ORGANIZATIONS

Service organizations and application vendors provide services that are often critical to the success of their client organizations. Any service disruptions could significantly impair the ability of client organizations to serve the needs of their customers. If a disruption lasts for an extended period, the client organization could begin to lose customers and eventually suffer significant revenue losses. Service disruptions could be the result of poor operating procedures, outside competition, or poor management decisions at the vendor organization. Eventually, these problems will surface in their financial statements. One of the first steps that the project development team at the client organization should perform after the decision has been made to utilize a service organization is to examine a copy of the most recent service auditor's report from each of the bidding service organizations. Such an examination should take place before any contract is entered into with the service organization. Another step the project development team should perform before signing a contract with a service organization or application vendor is to analyze the financial statements of each prospective vendor organization to obtain reasonable assurance that it is in sound financial condition for the foreseeable future. The project development team will have to employ the services of a qualified individual who can analyze financial statements. Examples of qualified persons include the chief financial officer (CFO), controller, an appointed subordinate who has sufficient education and experience in accounting and finance, or an independent certified public accountant (CPA).

As is the case with poorly operating internal policies and procedures, poor financial strength and performance could be indicators that the vendor organization may have difficulty providing the level of service and information protection expected by the client organization. It is beyond the scope of this book to discuss the many aspects of financial statements, the types of opinions independent auditors may express on them, and how to analyze them. However, the following discussion provides a general overview of the types of financial statements and independent auditor opinions issued in the United States under generally accepted auditing standards promulgated by the American Institute of Certified Public Accountants (AICPA). Note that there are some differences in financial statements and independent auditor opinions in other countries; however, the purpose and intent of independently audited financial statements are the same, regardless of where the vendor organization or its independent auditor resides. Vendor organizations may submit one of several types of financial statements with their contract proposals. These include audited, reviewed, compiled, or internally prepared financial statements.

For *audited* financial statements, an independent auditor expresses a written opinion as to whether the financial statements accurately represent the financial condition of the organization, in all material respects, in conformity with generally accepted accounting principles (GAAP). For reviewed and compiled financial statements, an independent auditor does not express such an opinion.

For *reviewed* financial statements, an independent auditor provides only limited assurance that the financial statements are free of material misstatement because the scope of the tests they performed was significantly less than they would perform during an audit. For *compiled* financial statements, an independent auditor states that the information contained in the financial statements is the representation of management and that the auditor does not provide any form of assurance over them.

Internally prepared financial statements are prepared directly by the management of an organization and have not been examined by an independent external auditor. The most preferable type of financial statement to evaluate the financial strength and performance of a vendor organization would be the *audited* financial statements for the most recently completed fiscal year, along with any interim (e.g., quarterly) financial statements prepared since the vendor organization's fiscal year-end. Interim financial statements alone are insufficient since they are usually prepared internally by the vendor organization and are unaudited. They are useful as a supplement to the most recent audited financial statements since they provide a general reference as to the recent financial performance of the vendor organization. Audited financial statements are the most desirable because they include the opinion of an independent auditor as to whether the financial statements are free of material misstatement. An independent auditor can express various opinions in audited financial statements. These include unqualified, qualified, adverse, or disclaimer.

An *unqualified opinion* states that the financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with GAAP. Financial statements on which the independent auditor expressed an unqualified opinion can provide the client organization with a reasonable degree of comfort that there are no material misstatements in the financial information contained in the statements. The project development team can then begin the process of evaluating the financial performance of the vendor organization based on its historical earnings, equity, cash flow, and various other factors. If the client organization suffers a significant loss as a result of relying on audited financial statements with an unqualified opinion, it may have some recourse toward the firm or individual who performed the audit if it can prove that its losses were the result of relying on the independent auditor's opinion. Therefore, it is also a good idea for the project development team at the client organization to document the review of independent auditor financial statements and include the documentation as part of the permanent project files.

A *qualified opinion* states that, except for the effects of matters to which the qualification relates, the financial statements present fairly, in all material respects, the financial

position, results of operations, and cash flows of the entity in conformity with GAAP. Financial statements upon which the auditor has issued a *qualified* opinion indicate that the auditor identified one or more areas in the financial statements where there could be a material misstatement. For example, the auditor may not have been allowed to perform tests to confirm that fixed assets such as computer hardware were accurately reported. If a prospective vendor organization submits audited financial statements containing a qualified opinion, the project development team at the client organization should carefully evaluate the nature of the qualification and determine whether the reasons for the qualified statement are significant enough to warrant disqualifying the prospective vendor organization from further consideration. As with the unqualified opinion, it would be prudent for the project development team to carefully document their analysis of the financial statements and their degree of reliance on the "unqualified portion" of the financial statements.

An *adverse opinion* states that the financial statements do not present fairly the financialposition, results of operations, or cash flows of the entity in conformity with GAAP. An adverse opinion could be issued, for example, if revenues at a company were significantly overstated because they were being recognized on a cash basis instead of an accrual basis or because the method of accrual did not conform to GAAP.

A disclaimer of opinion states that the auditor does not express an opinion on the financial statements. An auditor usually issues a disclaimer of opinion when circumstances prevent the performance of an audit of sufficient scope. This situation can occur, for example, when a company does not make available necessary records; the records have been lost or destroyed, or the auditor was not allowed to perform sufficient tests. If a prospective vendor organization submits audited financial statements containing an adverse opinion or a disclaimer of opinion, the project development team at the client organization should seriously consider dropping that vendor organization from further consideration. The project development team should give the vendor organization further consideration only if it can provide strong evidence that the issues leading to the adverse or disclaimed opinion have been resolved and the evidence can be corroborated by an independent party.

If a prospective vendor organization submits only reviewed, compiled, or internally prepared financial statements, the project development team at the client organization should also seriously consider dropping that vendor organization from further consideration, especially if the product or service the client organization is developing is mission critical. Although the information in unaudited financial statements may be perfectly accurate, the client organization would be taking a risk that there could be some material misstatement. Such a mistake could critically wound the client organization's ability to successfully launch its product or service. Another obvious step that the project development team should perform before entering a contract with the vendor organization is to contact a reasonable number of the vendor organization's past and present clients. Each past and present client surveyed should be asked to provide an assessment of the prospective service organization's level of service, product quality, and

response to special needs. Candid references from past and present clients can often provide important intangible information about a vendor organization that cannot be gleaned from a service auditor's report or independently audited financial statements.

Once a vendor organization has been contracted and service has been implemented, client organizations should monitor the financial condition of the vendor organization on an annual basis. Audited financial statements should be obtained by the client organization and reviewed by the process owners, the Internal Audit Department, or other designated areas. If the financial statements show a deteriorating financial condition, the client organization should communicate its concerns to management at the vendor organization. If the financial deterioration continues, the client organization should consider formulating one or more contingency plans of action, each depending on the criticality of the vendor organization's financial deterioration. For example, if the vendor organization's independent auditor issues an opinion that states that the service organization's ability to continue as a "going concern" is unlikely due to the outcome of recent litigation, the client organization should immediately develop plans to secure an alternative vendor organization. However, if the vendor organization is experiencing reductions in net income or even negative earnings, the client organization may not necessarily need to begin locating another vendor organization. The core operating earnings of the vendor organization may be sound, while net income was negatively impacted by a one-time charge (e.g., due to costs of corporate restructuring or divestiture of a subsidiary). The degree of concern can be determined only through close communication with management at the vendor organization and a careful analysis of the financial statements by qualified individuals. Even if a vendor organization has independently audited financial statements that express an unqualified opinion and indicate excellent historical financial performance and, in the case of a service organization, a service auditor's report that does not specify any reservations regarding the operating effectiveness of internal controls, it is still possible that an organization could suddenly experience significant operational and financial difficulties and not be able to provide adequate service to its clients. In some cases, this could cause clients to suffer significant losses.

3.10 EXAMINING VENDOR ORGANIZATION CONTRACTS

In any significant business transaction, a written contract is usually drafted and signed by authorized representatives of each party. The contract should specify the responsibilities of each party. Even if all parties involved have every intention of completing their end of the bargain as agreed upon in various discussions with each other, a contract helps ensure that there are no misunderstandings as to what actions each party is expected to perform, at what time they are expected to be performed, what services or payments will be received when the actions have been satisfactorily performed, and when the services or payments will be received. As an added incentive, most contracts also include a section specifying the consequences or penalties if one or more of the parties fails to perform as required by the terms of the contract.

The success of the products and services of most organizations is highly dependent on the timely, accurate, and secure functioning of computer systems and related applications, whether they are maintained internally or provided by a vendor. Thus, when a vendor supplies a computer system and/or application to a client organization, a significant business transaction has taken place and thus should be documented by a written contract. The following paragraphs attempt to identify the critical items that all auditors should be cognizant of and that should be specified in contracts between client organizations and vendor organizations.

Many parts of business contracts are included to address local and national laws and regulations. For example, in the United States, the Uniform Commercial Code (UCC) was developed in the mid-1900s to provide consistency among business transactions between parties residing in different states. Each state government has adopted the UCC as a baseline and then added additional provisions based on their interpretations of commercial law. For example, in the State of Washington, businesses operate under the auspices of the Revised Code of Washington (RCW). In addition, each city, county, or other municipality may have its unique laws or regulations that apply to the client and vendor organizations conducting business there. Although many contracts may appear to be routine, it is a good idea for the client organization to have all contracts reviewed by its legal counsel. Even after an attorney has "blessed" a contract, an internal auditor should still examine it during an audit to assess whether the terms of the contract adequately address the current operational, financial, regulatory, and information systems (IS) security needs of the client organization and whether the provisions of the contract have been carried out. Most contracts between client organizations and IS vendor organizations include these sections:

- The effective date of the agreement.
- Names of the parties to the agreement (i.e., the client organization and vendor organization).
- Definitions of unique or special terms used in the contract.
- Purchase or lease the price of any computer equipment, system software, and application hardware, including delivery, installation, and testing.
- Payment terms, including any down payment or advance, plus any other periodic payments (e.g., monthly, quarterly, or annual).
- Licenses to use the system software and application software. The contract should specify the terms or expiration dates of the licenses (i.e., for what period the software may be used), and the number of concurrent users authorized by the licenses.

- Any warranties by the vendors. For example, the vendor should warrant that the equipment will function properly upon completion of installation.
- Costs of training client organization staff on how to operate the new applications and computer equipment.
- Ongoing maintenance services provided (e.g., the normal hours during which service technicians are available, the expected response times, the premiums charged for after-hours response times, and so on) and the costs for such services.
- Maintenance services are not provided.
- Requirements of each party to terminate the contract (e.g., 30 days' prior written notice must be given by the terminating party).
- Penalties or liabilities to either party for nonperformance of the contract.
- Additional programming and/or support agreements, addenda, and modifications or clarifications often become part of the overall contract, in conjunction with the original contract.
- Approval page.

When performing an audit of a vendor application, an auditor should examine the contract between the client and vendor organizations to ensure that it has been executed by authorized representatives from both organizations. Authorized representatives are typically officers of an organization, such as the president, vice president, and treasurer. The auditor should also determine whether the contract is current (i.e., has not lapsed), addresses current service needs, does not contain wording that could be detrimental to the client organization, and does not omit wording that could pose a risk to the client organization. IS security standards should require that the contract specify that a copy of the programming source code of the current version of the software be stored in escrow by an independent third party so it is available to the company in the event the vendor goes out of business. Additional sections should be added to tailor each contract to the process being supported by the application. The number of additional sections is limited only by the imagination of the attorneys for the client and vendor organizations.

3.11 EXAMINING ACCOUNTING TREATMENT OF COMPUTER HARDWARE AND SOFTWARE

Internal auditors should examine the proper accounting for computer hardware, software, maintenance, and other costs to determine whether such costs have been properly recorded on the financial statements. For example, computer equipment and software should be capitalized and amortized over their estimated useful lives. Prepaid

maintenance costs should be classified as assets and expensed only when the costs applicable to the period in question have been realized. If equipment and/ or maintenance is billed monthly, the costs should be expensed as incurred. The audit steps described in this section are not necessarily the type of steps a specialized information systems auditor would perform. If an organization is small and has only one or two internal auditors, those persons will likely have a background in accounting, finance, or industrial operations. This type of internal auditor will be more likely to audit the accounting treatment of costs associated with computer equipment and software than would a specialized IS auditor.

If an organization has a large Internal Audit Department, these steps would likely be performed by one or more financial or operational auditors. If the organization uses an integrated audit approach whereby a team of auditors with expertise in various disciplines performs an audit of an entire process, an examination of the accounting treatment of computer equipment and software may be performed within the overall scope of the integrated audit. If an integrated audit approach is not used, the accounting treatment of computer equipment and software may be examined completely independently of an audit of the IS-related controls of the same computer equipment and software. In any event, management of the client organization, whether it is in the Accounting Department or the user department, is responsible for ensuring that the costs associated with the computer equipment and applications are properly accounted for, following promulgated accounting standards of the country in which the client organization resides.

3.12 SELF-ASSESSMENT QUESTIONS

Q.1 Describe auditing service organization applications with examples.

Q.2 Write a note on the various applications of auditing service organizations.

Q.3 How to write service auditor reports? Explain with examples.

Q.4 Write a detailed note on the service auditor reports of the USA, Canada, UK, and Australia.

Q.4 How to assess the financial stability of vendor organizations? Discuss.

Q.5 Explain the following:

- Control objectives of service organization management
- Examining vendor organization contract
- SAS 70-Type Audit
- Report of independent auditors

3.13 ACTIVITIES

Sketch a draft of auditing service organization applications.

3.14 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised; Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research*, *21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly*, *26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal*, *5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, *14*(1), 43.

UNIT-4

PHYSICAL SECURITY; LOGICAL SECURITY

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

Physical controls are the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. This unit cover topics on physical security, logical security, physical security, and security guards. This unit also describes general emergency and detection controls, heating, ventilation and cooling systems and insurance coverage, information systems business resumption programs, remote access controls, system security administration, wire transfer fraud, etc. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- Physical security and logical security
- Physical security and security guards
- General emergency and detection controls
- Heating, ventilation, and cooling systems
- Insurance coverage
- Information systems business resumption programs
- Remote access controls
- System security administration
- Wire transfer fraud

4.1 PHYSICAL SECURITY

Physical controls are the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. Physical security controls over computer hardware form the foundation of an organization's information systems (IS) control environment. Damage to central processing units (CPUs) and peripheral devices in any organization can be the result of a multitude of natural and human hazards. Earthquakes are a common occurrence along the West Coast of the United States, especially in California. Hurricanes are so common along the southeastern coast of the United States that they are assigned personal first names.

Tornadoes tear through the central plains of the United States regularly, especially during the summer months. Floods caused by heavy rains can happen anywhere but are a fact of life in the fall and winter along many river basins in the Midwest, central plains, and northwest regions of the United States. Severe rainfall can also cause mudslides as the water undermines the soil supporting hills and cliffs. Every winter, blizzards and severe colds paralyze the north-central and north-eastern United States, often resulting in the need to shut down business activity to minimize human casualties. Wildfires caused by lightning (and humans) have been all too frequent in California. They ravaged Colorado and Arizona in the summer of 2002. Volcanic eruptions are less common but can result in horrific destruction. The 1980 eruption of Mount Saint Helens in Washington state created such an enormous blast that some of its volcanic ash settled on the other side of the world. Trees in the blast zone were flattened like toothpicks, river basins surrounding the volcano were flooded within minutes, and the cloud of ash over eastern Washington state turned day into night. There are hundreds of dormant volcanoes along the entire Pacific Ocean rim that could erupt at any time. Kilauea and Mauna Loa are active volcanoes in Hawaii. Mount Pinatubo in the Philippines erupted fiercely in 1991 after being dormant for six centuries. Human hazards can be just as destructive as natural disasters. Bombings are unfortunately a common occurrence in many countries. The 1995 bombing that levelled the Federal Building in Oklahoma City was the most devastating in U.S. history. In 1993, a massive explosion ripped apart the World Trade Center in New York City, causing significant destruction. These events both paled in comparison to the destruction caused by September 11, 2001, jet-plane-turned-missile attacks on the World Trade Center and the Pentagon. Theft is another human hazard that is becoming more significant because computers are becoming smaller and more portable, while the amount and criticality of data they are capable of storing are increasing.

In the fall of 1996, a desktop computer was stolen from VISA International's San Mateo, California, data processing center. This was no ordinary desktop computer. Information on over 300,000 credit card accounts from VISA, MasterCard, American Express, and Diners Club was stored, unencrypted, on the hard drive. Some issuers, like Citibank, cancelled the cards in question and issued new ones. Others elected to keep the theft quiet so as not to inconvenience cardholders. These issuers chose to monitor the accounts in question for unusual activity. VISA agreed to reimburse affected card issuers for the costs

of replacing the cards. This theft could cost VISA an estimated $6 million. The insurance industry reported that over 200,000 laptop computers were stolen in 1995, an alarming 39 percent increase over 1994. One of the reasons for their attractiveness is that thieves can render laptops virtually anonymous by simply reformatting their hard drives. As a result, stolen laptops can command up to 50 percent of their retail price on the black market.

4.2 PHYSICAL LOCKS

The first line of defense in physical security is usually accomplished through the deployment of various types of locks on doors to any rooms that house computer and telecommunications equipment. These rooms include the main computer room, wiring closets, and rooms where file servers, gateways, routers, and other devices are located. *Conventional keys* can still be one of the most effective means of controlling access to restricted rooms. It is imperative that a highly trusted member of management, preferably the organization's security officer or designated subordinate, be responsible for issuing all keys, contracting with vendors to install new and replacement locks and make replacement keys, maintaining an inventory of all keys and the individuals to whom the keys are issued, and ensuring that all spare keys are properly secured. If keys are not properly controlled, conventional locks can provide only a false sense of security. For example, unauthorized access to computer equipment could be gained by custodians, former employees, transferred employees who no longer require access as part of their normal duties and former security guards.

Vendors can manufacture various types of keys. In many buildings, vendors create separate keys for each door. They are also able to make "master" keys that can open all the doors in a certain area, floor, or building, even though each door lock requires a unique "regular" key. In cases in which there are multiple locations, vendors are sometimes contracted to make "grand master" keys that can open all the locks in all facilities. It is very important to have an inventory of who has been assigned the master and grand master keys and to ensure that the people who possess such keys are highly trusted.

Electronic access badge systems provide two distinct advantages over conventional keys. First, electronic access badges eliminate the need to have to issue conventional keys to all employees. Rather they can be issued electronic access badges that provide them with the access they need. Whenever someone terminates, transfers, or loses his or her badge, it is simply deactivated on the electronic access badge system, thereby preventing any further access to previously authorized doors. Even if the badge is not returned, there is no need to consider rekeying all the locks in a facility. In addition, when the use of previously lost or stolen badges is attempted, their activity can be recorded, possibly leading to the recovery of the badges. The second advantage is that electronic badge access can be restricted to certain times of the day or night. Certain door locks can be programmed to remain locked during specified hours (e.g., after normal business hours). If after-hours access is allowed, such access by employees can be monitored and recorded. The

following discussion is a brief description of how a typical electronic badge access application function. Electronic access badge locks are activated when the holder of an electronic access badge places it on or near a badge reader plate. The badge reader "reads" the authorization information electronically encoded on a computer chip inside the badge and transmits it to the electronic badge access application program, which usually resides on a microcomputer or file server in a centrally controlled location. If the badge information is included in the table of authorized badges in the application program, a command is returned to open the electronic access badge lock. With this type of application, each lock, badge reader plate, central microcomputer, or file server, and, in some cases, multiple remote microcomputers or file servers are usually connected via a network of dedicated electrical wiring within facilities and dedicated phone lines between facilities.

Despite their advantages over conventional key locks, electronic access badge locks can sometimes be circumvented with relative ease. Often overlooked is the fact that many doors to rooms housing computer equipment have both an electronic access badge lock and a conventional key lock. Persons holding the keys can simply unlock the door manually and walk in, thus avoiding the audit trail that is available with the electronic access badge system.

For this reason, it is important to examine the key inventory in conjunction with the electronic access badge system (and any other types of physical locks) when assessing the adequacy of physical security at a data centre. Another way to bypass electronic access badge system controls is when people lend their cards to others. The badge borrower could access areas that only the badge lender should be accessing. A third potential control concern is that electronic access badges can be mistakenly programmed by the system security administrator to provide access that was not authorized or intended. A fourth risk is that the electronic access badge application could contain a programming flaw that unintentionally allows unauthorized access.

4.3 SECURITY GUARDS

Security guards are an important component of an organization's overall physical security program. Although the guards are not police, they are a deterrent to theft, danger in the workplace, and other illegal and unauthorized activities. They can also assist in reducing the incidence of piggybacking into data centers and in the monitoring of controls such as video cameras. Furthermore, the incident reports they prepare can be crucial evidence in cases of criminal prosecution and employee misconduct. For organizations that utilize the services of an outside security guard company, the responsibilities of the security guard company should be specified in a contract with the organization being protected. The contract should specify these key items: Term (e.g., from January 1, 20XX to December 31, 20XX) and cost.

Security guard company shall subject all guards to police background checks. Training and performance requirements of security officers, including excellent skills in

observation and writing. Attention to detail in observations is particularly important because security guards are often required to complete incident logs and incident reports. This is where writing (and spelling) come into play. Incident logs are used to record routine events that guards observe while making their normal rounds. The events are recorded as to time and location on the premises. Individually, the events recorded may not seem to be very important, but collectively, accurately recorded events can provide a glimpse of how a more significant event began to unfold. Incident reports are for significant events. If these events are poorly described, their credibility can be more easily questioned. If the description is difficult to understand, poor spelling can make incident reports even more difficult to read, thereby compounding their lack of credibility. For safety reasons, many security guards are required to be certified in first aid and cardiopulmonary resuscitation (CPR).

The contract should refer to a separate procedure manual. Day-to-day responsibilities should not be specified in the contract. This would result in a situation in which each time there was a change in procedure, an officer of the organization and the security guard company would need to review, approve, and sign a new contract. Instead, a separate procedures manual should be developed by the manager in charge of security at the facility and agreed on by the first-line manager of the guard service company. The contract should refer to the fact that the procedures in the manual will be followed. Routine changes to procedures should be approved by the organization's security manager and the first-line manager of the security company. The contract should be revised only in cases in which there are significant revisions, or the liability of the organization or security guard company has changed significantly.

Liability of the security guard company and indemnification to the organization if damages are caused by security guards. For example, the contract could specify that the security guard company will maintain a certain amount of liability insurance and name the organization as the beneficiary. Proof of such insurance should be obtained from the security guard company's insurance company. Termination requirements, including the number of days required for written notice to be given to either party before terminating the contract. Signatures of the president or other designated officer of the organization and the security guard company. This list is by no means comprehensive. It highlights some of the minimum requirements of a contract between an organization and a security guard company. Additional items that tailor the contract to the unique needs of the organization and the security guard company should be included. If the security guards are employees of the organization, the procedures manual would effectively constitute the contract between the security department and the rest of the organization. Internal security guards should still be held to the same, if not higher, performance standards as external guards. Again, minimum job requirements should include excellent observation and writing skills.

4.4 VIDEO SURVEILLANCE CAMERAS

Video surveillance cameras are an additional control that can act as an effective deterrent to unauthorized activities and provide critical evidence in criminal prosecution and employee misconduct. Video surveillance cameras are usually positioned in strategic locations that afford full views of the doors and/or equipment they are designed to protect. The video system should be designed so that the day, date, and time appear on the recording. In addition, monitors should be installed in the guard station. One monitor for each video camera would be optimal. However, in many facilities, there are more video cameras than there is space available for monitors in the guard station. These systems are designed so that the views appearing on the monitors rotate among the various video cameras periodically (e.g., every 30 seconds). Security guard procedures should specify that they are to observe the activity in the monitors regularly. For video tape systems, procedures should also be included in the security guard manual to ensure that videotapes are replaced before they run out. Full tapes should be stored for a reasonable time in a secure off-site location.

Newer digital video surveillance systems should be programmed to save the data images on the hard drive. Nightly backups of the hard drive should be performed, and the backup tapes, CD-RWs, or other digital storage devices should be stored at a secure off-site storage facility for a predetermined, operationally practical time commensurate with the risk of the areas being monitored. In some more sophisticated systems, data images can be electronically transmitted to the remote storage facility in a real-time mode so that nightly backup procedures are not necessary.

4.5 GENERAL EMERGENCY AND DETECTION CONTROLS

Alarms can be triggered by smoke, fire, or several other specific actions (e.g., forcibly opening a restricted door). Alarms should be installed at strategic locations throughout a facility for both safety and security reasons. They should be electronically monitored continuously. Fire alarms are typically monitored by both security guards and the local fire department. Physical access alarms are normally monitored by security guards and, depending on the application, the local law enforcement agency. Alarms should also notify security management within the organization. The security guard procedures manual should specify whom the guards should notify, depending on the nature and type of alarm. Heat-activated overhead sprinkler systems are required in most facilities. In the case of data centers, they may or may not be located above computer equipment, depending on the local fire code and the wishes of management. Overhead sprinkler systems should be installed even in areas where CPUs and other equipment are located for four reasons:

- Employee safety would be maximized.

- Fire damage can be contained in one area rather than being allowed to grow and spread, thereby risking the loss of the entire facility.
- Most equipment should be insured (see the Insurance Coverage section for more details), so losses from water damage should not be a major concern.
- If the organization has an effective business resumption plan, business operations should be able to be restored within a reasonable time despite water damage to computer equipment at the original data center or other location.

Many data centers used to be equipped with fire prevention systems that released pressurized halon gas in the event of a fire. Halon gas rapidly removes oxygen from the air, thus suppressing a fire. Halon dissipates quickly, leaves no residue, and is "nontoxic." Because of its inert properties, it does not damage equipment. Unfortunately, halon has some significant side effects. Halon damages the ozone layer of the atmosphere. Also, prolonged exposure can be hazardous to humans. For these reasons, halon gas is heavily taxed in some cities and jurisdictions. Therefore, the installation and maintenance of halon fire prevention systems are being phased out. Fire extinguishers are a simple but necessary component of the overall fire prevention control environment. They should be strategically located around the facility, especially in areas where the risk of fire is greatest. Alarms, sprinkler systems, and fire extinguishers are periodically inspected by local fire departments to ensure compliance with fire codes. A master key to all the doors in a facility is commonly located in a locking key box on the outside of a facility. The key box should be accessible only by the fire department. Building blueprints should be on file with the local fire department and/or located in a restricted area that is accessible by the fire department.

4.6 HEATING, VENTILATION, AND COOLING SYSTEMS

Computers survive best in a cool, dry, dust-free environment. Many computers do not require special HVAC equipment. For example, laptop and desktop computers function very well in a typical office or household room. These small computers are cooled by internal fans and do not require any special dust filters. The larger the computer, the more likely it is to require special cooling and dust removal equipment. Large mainframe computers generate significant amounts of heat, thus requiring special air-conditioning systems to maintain temperatures within manufacturer-specified ranges. Many mainframes also require special dust removal equipment due to the significant amount of air turbulence they create. The comfort requirements of the people operating the equipment must not be forgotten. Computer rooms should not be so cold that staff members can see their breath and must wear arctic clothing to be able to function. This type of atmosphere can lead to other hazards, for example, space heaters placed on the floor underneath computer consoles to warm the toes of the operators. Unless designed to supply power to a space heater for extended periods, the electrical wiring could short-

circuit and start a fire. Faulty or poorly maintained ventilation systems can lead to poor health for the staff. Failure to perform routine maintenance of ventilation systems is one of the most overlooked procedures in many companies. Companies that do not routinely maintain their ventilation systems may save a few dollars on paper, but they pay much more in terms of lost productivity when employees are sick and must miss work. As with household heating filters, the filters of commercial facilities should be changed regularly. The ducting should also be inspected and cleaned if necessary. If there are overhead vents with significant amounts of soot around them or with dust protruding from the grates, one should inquire as to when the last time the ventilation system was cleaned. The response might be surprising. The role of an information systems auditor should be to ensure that the HVAC systems receive maintenance regularly as required by the manufacturers. The person or persons in charge of the computer facility and equipment should maintain a log of all equipment and facility vendors, the types of maintenance that are required, and the approximate times during the year that such maintenance is to occur. The auditor should confirm that the log has been updated periodically during the year as the various maintenance procedures are completed. The auditor should also examine the contracts with each vendor to ensure that they are current and that they specify the types of maintenance that are to be performed, the frequency of such maintenance, and the cost. The auditor should then confirm that the maintenance procedures are included in the maintenance log.

4.7 INSURANCE COVERAGE

Insurance should be maintained to cover computer hardware and software at replacement cost and the costs to re-create lost data. Some policies may even cover lost revenues that are directly attributable to computer hardware or software failures. However, coverage for lost revenues may be costly and can be difficult to prove. Most insurance policies specify that coverage applies so long as certain procedures are implemented. For example, the policy may require that the company implement daily, weekly, or monthly backup procedures for software and data and that the data should be stored at a secure off-site location. The policy may also specify that all covered equipment must have routine maintenance procedures performed according to the manufacturer's specifications. Neither of these conditions should be a problem since the company should already have these procedures in place. Deductibles should be set at reasonable levels so that premiums are not excessive. The insurance policy should be examined to ensure that it is current and that it covers all computer hardware, software, and data at replacement costs. It should also be confirmed that the amount of coverage is adequate so that the company is not paying for too much or too little insurance. This can be accomplished by examining the procedures used by the insurance manager to determine the amount of coverage necessary and then testing the sources of the information. For example, the insurance manager may receive inventory listings of capitalized computer equipment and software costs from the Accounting Department. Using this historical cost information, the insurance manager can then adjust the required coverage upward to arrive at an anticipated replacement cost. A member of the audit staff should test the reliability of the

inventory listings because the acquisition and disposal of some equipment may not be recorded or may be improperly recorded.

4.8 PERIODIC BACKUPS

As mentioned in the Insurance Coverage section, procedures should be in place to perform periodic (daily, weekly, monthly) backups of the system software, application programs, and data as well as storage and rotation of the backup media (e.g., magnetic tapes, disks, compact disks [CDs]) to a secure off-site location. Daily backups are usually necessary only for data since the application programs and system software do not change significantly. Full backups of the entire system, including system software, application programs, and data should be performed weekly or monthly, depending on the number and types of changes that have been made. Full system backups should also be performed on completion of a major upgrade or significant changes to the operational and security parameters of a system. Logs should be maintained to document that backups have been performed and that the backup media have been transported to the off-site location. The auditor should visit the offsite storage facility to evaluate the adequacy of its physical security controls. If the off-site storage facility is a vendor, the contract should be examined to ensure that the vendor agrees to reimburse the client organization for any losses or damages that occur because of the backup media being lost or stolen while under the control of the vendor. Most off-site storage vendors require each client organization to supply a list of authorized individuals who are allowed access to the organization's storage containers. The auditor should examine the list to ensure that the listed personnel are correct and that transferred or terminated employees have been removed.

4.9 EMERGENCY POWER AND UNINTERRUPTIBLE POWER SUPPLY Systems

An *emergency power system* and an *uninterruptible power supply system* should be designed for every information processing facility. An emergency power system consists of a generator and the necessary hardware to provide limited electrical power to critical operational areas within a facility. In the event of a power loss, the emergency power system should activate automatically. A UPS system consists of an arrangement of batteries and supporting hardware components that are configured to provide smooth, continuous power to computer equipment. The UPS system acts as a buffer between the outside power source and the computer equipment, so that power surges and spikes are minimized. Also, in the event of primary power loss, a UPS system continues to supply electricity to the computer equipment until the emergency power system can fully activate. During an audit of physical security at one information processing center, a description of the emergency power system and UPS system was prepared, and key aspects of the systems were tested. They were well-designed and supplied with modern, reliable equipment.

4.10 BUSINESS RESUMPTION PROGRAMS

Every organization should have a current and tested business resumption program (BRP). Such plans are sometimes referred to as disaster recovery programs, but this phraseology infers that the program applies only to disasters. Since some BRP procedures may be implemented in events less severe than a disaster, the phrase *business resumption program* is more appropriate. Before describing the contents of a BRP, it is important to note that a BRP does not have to be the size of an encyclopedia. If it is too large, it can be difficult to maintain, and management may let it collect dust. The BRP should be as brief, concise, and easy to read as possible, while still retaining the key procedures necessary to ensure that all steps are carried out in a timely and appropriate manner. A BRP should include, at a minimum:

- List of key contact personnel throughout the organization, including contact phone numbers (home, work, cell phone, pager) and home addresses.
- Primary and secondary headquarters sites where key management is to convene if a disaster has rendered the main headquarters location inoperable.
- Identify and rank operational areas in terms of criticality and risk. The high-risk processes should be the first ones to be made functional in the event of a disaster. Data processing areas are usually at or near the top of the list of critical operational areas since so many other areas rely on data processing resources. Key aspects of a data processing BRP are discussed later in this section.
- Brief description of events that should trigger the BRP. This section should include initial BRP procedures as well as procedures for escalating the BRP, depending on the severity of the situation.
- Concise descriptions of the actions that will take place in each of the operational areas. These narrative descriptions may also include drawings and schematics of the facility.
- Often forgotten in the planning for disasters is the potential psychological impact of the disaster on the ability of employees to perform their duties. September 11, 2001, terrorist attacks were a clear example of the devastating psychological impact of this type of disaster. During disaster recovery training, it should be communicated to all staff that their priority is to be sure that their family members are safe. If employees fear for the safety of their families, they will be mostly ineffective at performing their job duties. In addition, if employees have witnessed or experienced severe trauma

during a disaster, some are going to need counselling and other assistance. The BRP should provide for these needs.

Once the BRP has been established, the organization must provide training for management and key personnel in charge of each operational area to ensure that they understand their roles and the sequence in which they are to carry out their business resumption duties. On completion of training, periodic tests of the BRP should be conducted. Initially the organization should conduct limited walkthrough tests to identify and resolve any inconsistencies or administrative difficulties. Next, the organization should plan limited tests of the BRP, beginning with the previously identified high-risk areas. At some point, the organization should be proactive and schedule a full mock disaster. Many companies do not perform such trials because of the inconvenience to employees and customers and the cost. Although full mock disasters can be very costly, committing the resources to stage them periodically (e.g., annually) should be viewed as paying an insurance premium for an event that, it is hoped, will never happen. In the event of a disaster, the organization's potential exposure will have been minimized. After completing training and testing, the organization must be committed to maintaining the plan. This means that the plan should be updated on an annual basis or more often when significant changes have occurred in operational areas. The recent terrorist attacks have taught us some additional lessons for BRPs. Alternatives must be provided for each key BRP assumption. For example, most of us take for granted that backup storage tapes and key personnel could be quickly flown to an alternative processing site. If all airplanes are grounded, this assumption is invalid. Even the assumption that ground transportation could be used was invalid near New York City shortly after the terrorist attacks. Many BRPs also assume that cell phones will be the primary mode of communication during a disaster. Shortly after the Nisqually earthquake in Washington state on February 28, 2001, cell phones were virtually useless as frequencies were jammed with people trying to call loved ones. Traffic became gridlocked within hours. Therefore, as part of the annual BRP maintenance process, all key assumptions should be questioned and at least one if not two alternative sets of processes should be developed for each key assumption, including transportation, communications, staffing, and processing facilities.

4.11 KEY ASPECTS OF AN INFORMATION SYSTEMS BUSINESS RESUMPTION PROGRAM (BRP)

For full-blown information processing disasters, an organization's BRP should provide alternate information processing sites. Hot sites, cold sites, vendor sites, and reciprocal sites are four commonly deployed alternative information processing sites. The type of site selected depends on the type of computing system platform (i.e., computer hardware and operating system), available financial resources, and desired time to full information processing capability at the alternative site. For each type of site, computer equipment must be compatible with the primary computer system, and backup tapes must be readily available so that the computers have the most current system software, application

programs, and data. Most organizations have multiple IS platforms. Thus, they will likely have separate IS BRPs. Each BRP may utilize a hot site, cold site, the third-party site, reciprocal site, or some variation of these sites in the event of a business interruption.

A *hot site* is an information processing facility that is fully equipped and configured with lights, electricity, air-conditioning equipment, computer equipment, and supplies such that it can be fully operational in less than 24 hours. The primary advantage of a hot site is its fast start-up time. This can be especially critical to large companies whose customers require immediate service. Each day that a data processing center is not functioning can cost a large organization millions of dollars in lost revenues. A hot site's primary disadvantage is cost. Maintaining a hot site requires the organization to lease or purchase a building, pay for maintenance of the facility (including property taxes if the facility is purchased), and continuously upgrade and test computer equipment to ensure that it will function properly if it needs to be placed in service.

A *cold site* is a facility that is equipped only with the basic infrastructure necessary to operate the primary information processing system. The infrastructure includes lights, electrical wiring, air conditioning, and supplies but does not include computer equipment. A cold site plan provides for the organization to receive the necessary computer equipment from a vendor or alternative supplier within a predetermined period. Because the equipment must be transported from the vendor, installed, and tested before being placed in operation, a cold site can take several weeks to become operational. The main advantage of a cold site over a hot site is that it is cheaper to maintain. There is no computer equipment to continuously upgrade and test. The disadvantages include a relatively slow return to operations and the costs of leasing or purchasing the facility.

A *vendor site* is an information processing facility that is provided by a vendor that specializes in providing such facilities. Advantages include a fast return to operations and the elimination of the need to acquire and maintain a facility and related equipment. Disadvantages include a relatively high cost that the vendor may charge and the potential risk that the vendor's site is not maintained at full compatibility with the client organization's information processing system. As with any vendor, the contract should be specific regarding the responsibilities of the vendor and the client organization. It should also specify the vendor's liability if information processing capacity is not restored within the required time frame.

A *reciprocal site* is an information processing facility located within another organization. Two organizations form an agreement in which each agrees to allow the other to utilize it IS resources if one or the other experiences a business interruption. The agreement should be documented in writing. The agreement should specify the rights and responsibilities of each organization and should provide for periodic testing by both organizations. It is very important that reciprocal sites not be in the same geographic area. Otherwise, in the event of a regional catastrophe, both sites may be rendered inoperative. The primary advantage of a reciprocal site is that there is little or no cost. One disadvantage is the risk of the two organizations not keeping their computing platforms compatible. Another disadvantage is the

potential difficulty in enforcing the agreement if one organization cannot grant the other full IS processing resources. The organization called on to provide alternative IS processing resources could claim that doing so would prevent it from being able to meet its own information processing needs. Therefore, the written agreement must specify the rights and responsibilities of each organization and that management of each organization fully understand the implications of the agreement.

4.12 BACKUP SYSTEM SECURITY ADMINISTRATOR

The movie *Jurassic Park*, based on the novel by Michael Crichton, provides an excellent example of how not to administer security over a high-risk system. In the movie, Jurassic Park is a giant, computer-controlled tropical theme park with Tyrannosaurus rexes, velociraptors, and numerous other live dinosaurs as its main attractions. Any IS auditor who saw the movie should remember the part where the system programmer was bribed into stealing several dinosaur embryos. To facilitate his theft and getaway, he had programmed the system to unlock secured doors to the research facility where the embryos were located while the primary console terminal for the system displayed what appeared to be typical processing. The system was locked to prevent anyone from accessing the system without the appropriate password. To complicate matters further, a severe tropical storm was battering the park. The resulting power outages enabled some of the predatory dinosaurs to escape and attack the humans. The embryo theft and escape of dinosaurs were possible because the data processing facility suffered from a severe lack of internal controls. Complete control over tens of millions of dollars' worth of research facilities and dinosaurs was granted to a single individual—a classic example of inadequate segregation of duties. There was no trained backup system security administrator, no BRP, and no procedures to back up software and data to enable the system to be restored in the event of a system restart. After the system lockout was discovered, the system supervisor did not know how to resolve the situation other than to completely turn off the power to the system and then restart it from scratch. As a result, all the customized system parameter settings were wiped out. Fortunately, the young granddaughter of Jurassic Park's owner was able to operate the system and get it functioning, albeit at a less-than-optimal level of performance. The theft of the embryos and all the problems that followed could have been avoided had the owner of the park and the system security administrator implemented many of the IS security controls described in this book. Unfortunately, situations like the one just described are not restricted to the movies. Granting complete control over a computer system to one individual is one of the most common control weaknesses in the real world. Management of many organizations fails to recognize the need and urgency to designate and adequately train a backup system security administrator. As a result, they are subjecting their organizations to the risk that one person can perform unauthorized activities as well as the risk that a system may experience problems that cannot be resolved. For example, the system security administrator could be involved in an accident, must leave work unexpectedly, or may be at a location where he or she cannot be reached. Thus, the organization might not be able to restore operations adequately promptly.

4.13 LOGICAL SECURITY

The initial key to protecting an information system from unauthorized access lies in the design and programming of logical security controls into the system, whether it is an operating system, a database management system (DBMS), or an application program. Before logical security controls can be designed, the project design team must first be aware of the significant risks to which the system may be exposed. The degree of risk will have an impact on the types of logical security controls that need to be designed into the system as well as the number of controls and their relative strength. High-risk systems would warrant the time and resources to design a greater number of robust logical security controls than low-risk systems.

4.14 LOGICAL SECURITY DESIGN

Identification of the significant risks facing a system can best be accomplished through a formal risk assessment process. Because many internal and external auditors prepare risk assessment documents as a standard part of their audit process, they can be an excellent resource to a system design team for assistance in performing a formal risk assessment. Since members of a design team usually include representatives from all significantly impacted areas of the organization who are experts in their respective fields, the team will likely be able to identify most of the significant business risks. However, auditors are often aware of risks that a design team may not have considered. For example, one of the most difficult risks to control is the performance of unauthorized activities by a system security administrator. By definition, a system security administrator needs to be able to add, delete, and change users and their access capabilities, monitor, and regulate system activities, control system security parameters, review system security and operational logs, and perform various other unrestricted tasks. (*Note*: In large organizations, some of these tasks may be segregated.) To accomplish these tasks, a system security administrator requires virtually unrestricted access within the system. Most design team members do not think twice about the fact that the system security administrator essentially will have free rein in the system. In these cases, it is the responsibility of the auditor to make the rest of the design team aware of the risks posed by the system security administrator.

The challenge facing the design team is whether the risk of a system security administrator performing unrestricted activities outweighs the costs of designing controls to limit what functions a system security administrator can perform.

Two techniques can be designed into a system to control system security administrator activities:

- Program the system to require a second system security administrator to confirm any additions, changes, and deletions of user IDs and their access capabilities and to make changes to the system operating and security parameters. This control would effectively prevent one system security administrator from performing unauthorized activities. However, the disadvantage of this control is that requiring two system

security administrators to bless every security-related change to the system could cause significant operational delays if two system security administrators are not available when a situation requiring immediate action arises.

- Program the system to log all potential system security-related events and implement procedures whereby the log is reviewed regularly for unusual or unauthorized activity, preferably by the manager of the system security administrator. Loggable events include additions, deletions, and changes to user IDs and their access capabilities (including changes to the system user ID), system reinitializations, changes to the system operating and security parameters, software upgrades, unsuccessful sign-on attempts, resetting of user IDs when users forget their password, and any other activity that could affect system security. Logging these events would provide an audit trail of the activities of system security administrators, other users, and hackers who are attempting to infiltrate a system.

The system should also be programmed so that a system security administrator cannot delete or change the log file (i.e., the log file should be read-only), even at the operating system level. In this way, the system security administrator cannot remove audit trail evidence of unauthorized activities from the log. The system should be further programmed to automatically archive the log file periodically (e.g., monthly) and then purge the archived files after a reasonable time (e.g., annually, or less often, depending on the criticality of the information). Alternatively, log files can be recorded on permanent storage devices such as compact disks (CDs) via a WORM (write-once-read-many) drive. System security administrators should not have physical access to the CDs in the WORM drive. If system security administrators know that their activities are being automatically recorded and then reviewed by their superiors, they are much less likely to perform unauthorized activities.

Although logging can be a deterrent to performing unauthorized activities, it is not a preventive control. Rather, logging is a detective control that will identify a potential violation after it has already taken place. Another consequence of logging system security-related activities is that it requires a certain amount of system processing capacity and disk storage space. If the volume of activity is very high, this "overhead" can degrade system performance. To circumvent this problem, the system could be designed with parameters that enable the system security administrator to reduce, but not eliminate, the period that log files are archived. Additionally, the system could be programmed so that the log records only the riskiest types of system-security-related events (e.g., adding users with system administration capabilities, and reinitialization of the system). The third problem with logging is that it is difficult to prevent a system security administrator from being able to access and delete a log file, or any other file, at the operating system level. It might be possible to disguise the log file or files so that they are difficult to locate, but an experienced system security administrator might still be able to locate them.

4.15 BRINGING A NEW SYSTEM TO LIFE

After programming and installation have been completed, a system security administrator or installation technician initializes an execution program to activate the system for the first time. The system should be programmed to recognize a *system user ID* and *maiden password.* The system user ID and maiden password should be specified in the system documentation in the event the system needs to he reinitialized later. The system should be programmed such that, on entering the system user ID and maiden password, the system security administrator is required to enter a new password comprised of *eight or more alphanumeric, case-sensitive characters.* By allowing combinations of numbers and case-sensitive letters to be used in a password, the number of possible character combinations is significantly increased. A longer minimum password length requirement for the system user ID should be programmed into high-risk systems.

Password characters should not appear on the terminal screen as they are entered by the system security administrator. This control is called *password masking.* Password masking makes it difficult for a passer-by or observer to steal another user's password and then perform unauthorized activities. The system should also be programmed so that passwords cannot be viewed by the system security administrator from within the application, database management system (if applicable), or at the operating system level. To accomplish this, the password file should be encrypted, using a relatively secure encryption algorithm. Adequately encrypted files are much more difficult to examine and change as compared to unencrypted files. User IDs and passwords should remain in their encrypted state as they are transmitted through any telecommunication network. The system user ID should be programmed to have system security administration capabilities to enable the system security administrator to enter customizable operations and security parameters and to create user IDs for other users of the system. When additional user IDs are created, the system should grant them read-only access capabilities as a default, as opposed to granting universal access capability. This design control ensures that additional effort must be performed before a new user ID can be dangerous. The system should be programmed to enable the system security administrator to assign a maiden password of at least eight characters to each new user ID. When the user signs on for the first time, the system should prompt the user to change his or her password. In this way, the system security administrator is prevented from knowing the passwords of other users (assuming that the password file has been adequately encrypted).

The number and types of customizable operation parameters will vary greatly, depending on the type of application and the user requirements specified during the design stage. The number and types of customizable system security parameters will also vary by application, depending on the risk of the applications and the financial and human resources available during system design and development. System security parameters should be customizable on a system-wide basis and an individual-user basis. Five common customizable systemwide security parameters include:

1. *Minimum password length.* The system should reject any user attempts to enter passwords with fewer characters than the parameter setting. For most commercial

business systems, a minimum password length of eight characters is sufficient. However, if the system in question supports a highly risky process, more characters will be warranted, even into the 20-plus range. With long passwords, passphrases are usually necessary. A *passphrase* is simply a statement that is typed instead of just a single word. Passphrases can be highly effective because they require an unauthorized user to guess a concept statement rather than just a single word. They are also effective against dictionary "cracking" software. Some systems have a parameter that enables system security administrators to require users to include one or more numbers or special characters in their passwords. *Password expiration period.* When the password expiration period has elapsed, the system should prompt each user to enter the old password as well as a new password two consecutive times. For most commercial applications, a password expiration period of 60 days is sufficient. Again, in the case of a highly risky system, more frequent changes of passwords may be necessary. Keep in mind that if the system enables users to enter a new password, and then immediately change their password back to their old password, the effectiveness of frequent password changes is eliminated.

2. *The number of consecutive unsuccessful sign-on attempts allowed before suspending a user ID*. If the number of unsuccessful consecutive sign-on attempts has been reached, the system should suspend the user ID. Suspension means that the user ID is unusable until a system security administrator resets the user ID back to active status. This is an excellent control to prevent a hacker or hacking system from trying to sign on an unlimited number of times. In most cases, suspending user IDs after three consecutive unsuccessful sign-on attempts is sufficient for operational and security purposes.

3. *Time of day and day of the week that users can sign on*. The system should reject any user attempts to access the system during times of the day or days of the week that are outside the parameter settings. This control helps prevent unauthorized access attempts during nonbusiness hours by persons who have physical access to a facility (e.g., a custodian or security guard).

4. *A period of inactivity is allowed before a user is automatically signed off*. When a user ID has been inactive for the period specified in the parameters, the system should automatically save and close any files that are still active, terminate the application, and sign off the user. This control reduces the risk of unauthorized access when users leave their workstations and forget or choose not to sign off. The most appropriate session time-out period must be determined based on a balance between operational and security needs. Initially, a session time-out period of 10 minutes or less should have been recommended.

5. The system should be programmed to allow these same system security parameters to be separately specified on an individual user ID basis by the system security administrator. If no separate system security parameters are designated for a particular user ID, the default system security parameters should apply. The system

should apply any individual user ID parameters in preference over the system's default parameters. This logic enables the system security administrator to accommodate users who have unique access requirements without changing the access restrictions of all users. For example, in the case of a user who wishes to work over a weekend on a special project, the system security administrator would assign an individual user ID access parameter for this person. Another example would be when a backup system security administrator's user ID is created. The primary system security administrator may wish to set the minimum password length for this user ID at a higher minimum number of characters than the standard for other non-system security administrator user IDs. The five system security parameters should apply to all non-system security administrator user IDs. Parameters, 1, 3, and 4 however, should not apply to the system user ID.

The system should be programmed so that the system-wide and individual minimum password-length parameters do not apply to the system user ID. The reason is that a new system security administrator who is unfamiliar with the need for minimum-password-length controls could intentionally or inadvertently set the parameter to an undesirably low minimum, such as three characters. The password for the system user ID could then be changed to only three characters, thus exposing the system to a significantly higher risk of unauthorized access. This could also happen in the case of a lazy system security administrator. Having a separate, unchangeable programming requirement that the password for the system user ID is at least eight mixed alphanumeric characters long eliminates the possibility of a password that is too short or simple being assigned to the system user ID and thus considerably reduces the risk of unauthorized access. The parameter concerning the number of consecutive unsuccessful sign-on attempts allowed before suspending a user ID should also not apply to the system user ID. If it did, then someone who attempted to hack the password for the system user ID could cause it to become suspended after only a few tries. This would be a highly undesirable situation in the event the system security administrator had not created a backup system user ID and needed to perform functions that no other user ID could perform. If the system is programmed so that the system user ID is not protected by the automatic suspension control, the need to program the system with an unchangeable minimum password length for the system user ID of eight or more mixed alphanumeric characters becomes even more critical.

The time-of-day and day-of-week parameters should not apply to the system user ID because the system security administrator could require access at any time of the day or week. If a critical problem were to arise during a time when the system user ID was restricted, the organization could suffer significant damage to system programs and data. This could be like having a time lock on a bank vault and then having a fire break out inside the vault. One would not be able to open the time lock and would have to hope that the oxygen ran out before the money was burned up. Parameters 1, 3, and 4 should still apply to backup system security administrator user IDs that were created using the system user ID. Although backup system security administrator user IDs are usually granted access equivalent to the system user ID, they have nonetheless created user IDs,

which can be erased by the system user ID or a different backup system security administrator's user ID, and which could be deleted in the event the system is reinitialized. This brings up another key design issue.

The system should be programmed so that the system user ID cannot be deleted. For instance, one of the backup system security administrators could inadvertently or intentionally attempt to delete the system user ID. If such a request were allowed, critical operation of the system would be dependent on the system access parameters applicable to backup system security administrator user IDs. If the parameters were improperly conceived, as in the case of time-of-day and day-of-week parameters, the system may not be accessible in the event of a problem during off hours.

The granularity of system access controls refers to the degree of specificity with which system access parameters can be controlled. In the design stage of a system, the granularity should be determined. Keep in mind that there is a trade-off between granularity and cost, in terms of increased dollars and programming time and system overhead once the system has been implemented. In addition to the above typical types of logical security controls, other, more detailed controls may be designed into a system. These four logical security controls would add to the granularity of control provided to the system security administrator:

Passwords could be screened to prevent users from entering easily guessed passwords. For example, the system could be programmed with a changeable parameter as to the maximum number of consecutive characters that would be allowed. Thus, passwords such as "aaaaaa" or "111111" could be prevented.

1. The system could be programmed to require a minimum of two numbers and two non-alphabetic characters in the password, thus making passwords more difficult to guess.
2. The system could be programmed to prevent a user from entering a password that he or she had recently used. To accomplish this control, the system would need to record, in an encrypted format, a predetermined number of previous passwords of all user IDs (e.g., 10). A parameter could then be created that allows the system security administrator the flexibility to set the number of previous "generations" of passwords the system will not allow users to reuse.
3. The system could be programmed to allow only certain user IDs to sign on from specific workstations. For example, user IDs assigned to computer operations personnel could not sign on from workstations in the programming department, and vice versa. Each device (workstation, terminal, printer, gateway, etc.) on the system is assigned a unique "node" number by which the system can identify it. To implement workstation restrictions, the system security administrator would assign specific signs on nodes or node ranges to each user ID. An attempt by a user to sign on to a node number different from his or her authorized node number or outside the authorized range would be rejected.
4. The system should be programmed to apply granularity controls 1, 2, and 3 to all user IDs, including the system user ID. However, granularity control 4 should apply to all

user IDs except the system user ID, which should be allowed to sign on from any workstation to troubleshoot and maintain system security efficiently and effectively. An additional granularity control programmed into some systems is a system access parameter that can be set to allow concurrent sign-on sessions by users. A *concurrent sign-on session* is when the same user ID is allowed to be signed on from two or more workstations simultaneously. From an operational viewpoint, this feature can be very useful. For example, a system security administrator may be signed on at his or her normal workstation and may be in the middle of performing a lengthy interactive database query. An emergency problem may arise, thereby requiring the system security administrator to perform some sort of immediate action (e.g., the company president forgot his or her password and it needs to be reset immediately). Rather than terminating a lengthy interactive job and then having to restart it from the beginning, it is more efficient for the system security administrator to go to another workstation to perform the reset operation.

However, this type of activity can present significant control weaknesses. In this example, the system security administrator may need to use a workstation in another room or location within the facility. While the system security administrator is away, the interactive job could finish, thereby freeing the system security administrator's sign-on session at the original workstation. An unauthorized user could then proceed to access the system and perform unauthorized system security administration functions (e.g., create an unauthorized user ID with system security administrator capabilities for use later). If three or more concurrent sessions are allowed, the potential for this type of unauthorized access increases drastically.

Therefore, end users should not be granted concurrent sign-on capabilities because of the number of potential security weaknesses that could arise in the end-user environment. If warranted by operational need, only system security administrators and possibly a very select few other users may need the concurrent sign-on capability. If so, no more than two concurrent sessions should be allowed, and their activities should be logged and reviewed. The most secure situation would be to design and program a system so that concurrent sign-on sessions are not allowed and are not even an optional system security parameter. To address the problem of having to terminate an interactive program or query that takes many minutes to complete, the system security administrator or user in question should submit his or her job for "batch" processing. A *batch program* is submitted by the user and executed by the system when data processing resources are available. Submitting jobs in batches frees the user ID to perform other interactive functions without having to wait for the job to complete.

Even if a system is designed so that concurrent sign-on sessions are not even an option, system security administrators can circumvent the design control by simply creating multiple user IDs for the same user. The risks of one user having two or more user IDs are the same as for the same user having the concurrent sign-on capability. Therefore, this practice should be strongly discouraged. The logical security controls just described ingan optimal system design situation. However, in the real world, some of the controls

will not have been designed into systems. Some of the controls likely exist, but they affect the system user ID in a manner that could result in an increased risk of unauthorized access via the system user ID. For example, the minimum-password-length parameter may be set to a low level and may apply to the system user ID as well as all other users. Additional granularity controls that may or may not affect the system user ID will likely be encountered. In each case, assess the overall risk of the process affected by the system and then determine whether the lack of certain controls or the way they have been designed, is significant enough to warrant a recommendation to reprogram the applicable part of the system. In some cases, the identified weaknesses can be overcome partly or completely by the proper deployment of system security-related controls.

4.16 USER IDS AND PASSWORDS

As can be seen from the preceding illustration of logical security controls in a newly installed system, *user IDs in conjunction with passwords form one of the most common and critical types of logical security control*. Hence, user IDs and passwords are deployed in virtually every computer system requiring at least some form of security. Without them, almost anyone could access an information system and perform unauthorized transactions; gain unauthorized access to information; damage data and programs; release viruses; add, change, and delete users and user access capabilities; make unauthorized changes to system operations and security parameters; and perform a myriad of other undesirable activities. Unfortunately, the mere presence of user IDs and passwords does not ensure that an information system is adequately secure. All logical security controls, including those over user IDs and passwords, must be carefully designed and properly administered to be effective.

4.17 REMOTE ACCESS CONTROLS

In the early days of computing, system security administrators were typically the only users who required the ability to sign on to a system remotely. Computer processing was centralized, and users typically signed on using dumb terminals. Today more and more users are requiring the ability to sign on remotely using laptops, personal digital assistants (PDAs), and some kinds of cell phones. They typically require access to the organization network and, from there, access to various applications. Remote access facilitates numerous efficiencies and enables more timely communications and completion of work, but it also significantly increases the risk to an organization's network of computing systems to unauthorized access, viruses, and other operational challenges. To help mitigate these risks, several remote access control technologies have been developed. The most common remote access controls include dedicated leased lines, automatic dial-back, secure sockets layer (SSL) sessions, multifactor authentication, and virtual private networks (VPNs). In some situations, a combination of one or more of these controls is deployed. Each of these controls is discussed briefly here. Most rely on some sort of encryption technology.

Dedicated leased lines are telephone connections that are private in the sense that the leasing telecommunications company does not allow external parties to access them. Data transported between computers across a dedicated leased line is not encrypted by default because there is less risk of interception. Depending on the nature of the information being exchanged, a separate encryption control may need to be implemented. Dedicated leased lines are expensive but provide enhanced performance since there is less external traffic and there is a reduced need to encrypt all internal traffic. A remote user should still be required to authenticate to the network using a user ID and password at a minimum.

Automatic dial-back is a control in which the remote user's computer modem dials a phone number dedicated to remote network sign-on. The remote computer provides enough identification information such that the authenticating system can automatically terminate the original call and dial the authorized phone number in its database for that remote computer. This control helps prevent unauthorized users from attempting to access the organization's network, even if they know the remote network sign-on phone number. The authenticating computer will dial only preauthorized phone numbers in its database. After successful dial-back, a remote user should still be required to authenticate to the network using a user ID and password at a minimum. Depending on the nature of the sign-on session, data traffic may or may not need to be encrypted.

The secure sockets layer is a protocol used to provide encrypted Internet sessions between remote computers and the network server. It normally runs on port 443 of the network server and uses public key encryption to establish a trusted connection. Once the connection has been established, all data exchanged between the remote computer and the network server is symmetrically encrypted. The strength of the encryption depends on the symmetric key length (typically 128 bits) supported by the remote computer's browser and the network server. The constant data encryption utilizes enough central processing unit (CPU) processing capacity to degrade the performance of the remote computer and the network server. While SSL encrypts data between the remote computer and the network, it does not provide proof that an authorized remote user initiated the session. A remote user should still be required to authenticate to the network using a user ID and password at a minimum.

Multifactor authentication is the implementation of two or more controls before granting access to a user. *Two-factor authentication* is typically applied to remote users. It requires the user first to authenticate to a challenge-response server and then to authenticate to the network server with their network user ID and password. To authenticate to the challenge response server, a user must possess a token device. During the authentication process, the user is challenged to enter a single-use randomly generated number. The number is obtained from the token device, which is synchronized with the challenge-response server upon issuance. To access the token, the user must first enter a PIN. Three common products providing this type of internal information technology control include SecurID® by RSA Security Corporation, Defender® by Symantec Corporation, and CRYPTOCard® by CRYPTOCard Corporation. An example of three-factor authentication would be to require the user to present a biometric possession (e.g., finger,

palm, retina, iris, voice, etc.) in addition to the two-factor authentication process. Applicable hardware and software would need to be implemented at both the client end and on the network server.

Virtual private networks enable secure Internet sessions between remote computers and the network server, much like SSL. Unlike SSL, VPNs typically require special hardware and software. A VPN gateway server commonly protects the network server, and the remote computer must have the corresponding VPN client application to establish a secure channel (sometimes referred to as a tunnel) for electronic data interchange or exchange. Internet Protocol Security (IPSec) has emerged as the dominant protocol standard for implementing VPNs. Internet Protocol Security was developed by the Internet Engineering Task Force (IETF), which is a group of scientists and other technical experts who provide support on technical issues related to the Internet and who help develop Internet standards. The three security goals of IPSec are to provide:

1. Mechanisms for authentication, to reliably verify the identity of the sender Mechanisms for integrity, to reliably determine that data has not been modified during transit from its source to its destination.
2. Mechanisms for confidentiality, are to transmit data that can be used only by its intended recipient and not by any unauthorized interceptor.
3. These goals are achieved primarily using encryption and digital certificates. By taking advantage of the existing Internet infrastructure throughout the world, properly deployed VPNs can provide significant cost savings, efficiencies, and other benefits for organizations. For example:
4. Remote users can access their organizational networks without the costs of long-distance phone calls or the need for the organization to pay for an 800 number.
5. Site-to-site connections no longer require expensive dedicated leased telephone lines.
6. Access connections can be made virtually anywhere in the world.
7. VPNs can be constructed and dismantled in a relatively short period.
8. VPNs can be designed with complex proprietary encryption and authentication controls so that the look and feel of each organization's internal network are presented to remote individual users and users at each organization or commercial partner site.
9. VPNs are more secure than applications that rely on the secure sockets layer protocol for security.

These benefits can be summarized and quantified in this way: "Using the Internet as a backbone, a VPN can securely and cost-effectively connect all of a company's offices, telecommuters, mobile workers, customers, partners and suppliers. Forester Research estimates that companies can achieve savings of up to 60 percent using Internet-based VPNs instead of private networks and corporate modem banks." But VPNs also present several challenges. Christopher King has identified eight challenges:

1. VPN devices must possess a mutually agreeable method of securing data (typically digital certificates). The challenge is that there is currently not standard protocol for requesting, validating, and cross-certifying digital certificates.

2. VPNs must be designed so they provide high availability to users. VPNs must be designed to handle the computationally intensive modern encryption products while also providing high-speed data processing.
3. VPNs must be able to quickly transport high volumes of data among users via the Internet. The challenge is that sometimes the Internet contains bottlenecks that prevent or delay data from reaching its destination.
4. The organization's internal network must be configured so that the VPN gateway device does not compromise other security mechanisms, such as the firewall.
5. The electronic addressing and routing of VPN devices must be carefully designed to ensure that the same private address number sequences are not assigned to two or more different networks.
6. Vendor software for VPNs often is difficult to administer and manage.
7. Different VPN software products that are labelled IPSec compliant may not necessarily work together.

4.18 SYSTEM SECURITY ADMINISTRATION

System security administration is the process through which an information system is protected against unauthorized access and accidental or intentional destruction or alteration. How the available logical security controls are administered after the system has been implemented is equally as critical as the design of the logical security controls. Very likely most systems encountered in the real world have less-than-optimal logical security design, thereby elevating the urgency to strengthen other available controls. In some cases, weaknesses in the logical security design of a system can be controlled sufficiently through the proper deployment of other available logical security controls. In other cases, the weaknesses cannot be adequately controlled. If not, then monitoring controls and procedures should be implemented to identify potential system violations promptly until the system can be redesigned and programmed to prevent such weaknesses. Essential security-related functions performed by a system security administrator include the creation of user IDs and assignment of their associated system access capabilities, the deployment of system security parameters, and monitoring of the system to help prevent and detect potential instances of unauthorized system usage. When a user ID is first created on a system, the system security administrator should grant the user only those access capabilities authorized by the data owner, system owner, or another appropriate management person. The system security administrator should perform this action only on receipt of authorization in writing or via a secure electronic communication message.

Sometimes a vendor technician enters the system user ID and maiden password during installation. Since the installation technician usually does not have any ongoing purpose for accessing a system after the installation has been completed successfully, the system security administrator should make sure to change the password of the system user ID so that no one else knows it. If the technician still requires access for specific purposes, the system security administrator should create a separate user ID for the technician but grant only the necessary access capabilities, excluding any system administration access

capabilities. No outside vendor user IDs should be granted system security administrator access capabilities. Department managers should be responsible for training users not to share or divulge their passwords to anyone, write them down, post them in their workstations, store them in an electronic file, or perform any other act that could potentially result in their password's being divulged. However, all areas of the organization should stress the importance of exercising confidentiality over passwords to protect information systems. There should be a company policy statement and specific standards about such confidentiality. System security administrators should carry out the policy and standards. Internal auditors should help ensure that the policy and standards have been adequately implemented. The policy and standards should be communicated to employees as part of a new employee training program. In addition, quick reference reminder cards and periodic reminders in company newsletters and electronic mail should be prepared and distributed by the system security administration department. These communication media should be updated regularly (e.g., quarterly, or semi-annually). A procedure should be implemented whereby the access capabilities of users are reviewed periodically (e.g., annually). In theory, management should perform periodic access capability reviews in the user areas. Implementation of this procedure is very difficult. The main reason that the effectiveness of a periodic review is limited is that, in most cases, management personnel called upon to review and approve the staff system access capabilities do not understand what all the access capabilities mean.

Management must be educated in what the complex system access security matrices, tables, specific functions, rights, and attributes enable the users to do on the system. Such education could be accomplished through formal training courses performed by system security administrators or IS auditors familiar with system access security over the platforms in question. Further complicating the matter is the fact that there are numerous computer systems accessible by staff within a department. For example, when a typical user comes to work in the morning, he may check his voice mail box, sign on to the network and check electronic mail, check his Internet e-mail, sign on to the mainframe to check the status of reports or other work, and then sign on to several restricted access network applications to perform various business and audit tasks. By the end of the day, the user may have accessed 10 or more independently administered computer systems. Other users with the same manager may also sign on to 10 or more systems during the day, but they may not be the same 10 systems that the other user accessed.

In a department of 15 or 20 employees, the combined number of different systems accessed during the day could be 50 or more. Thus, training management to understand system access capabilities in all systems becomes an enormous undertaking. Should the department manager be expected to understand and approve the system access capabilities of all department employees to all systems? This is a question whose answer will vary by organization. It will depend on the nature of the systems being accessed, the degree of control exercised by the system security administrators of each system, the system and/or data owners of each system, and by end-user management. The organization's size and corporate culture will also play a role in determining the degree to which access to various information systems is administered and monitored. The realistic

answer to this dilemma is that monitoring of system access capabilities is a joint organization-wide effort. Management is ultimately responsible for the activities of their staff. However, system security administrators are responsible for protecting system resources from unauthorized access and damage. Therefore, they must advise management as to why certain access capabilities should not be granted. Internal auditors must also assist in the overall process by evaluating the reasoning behind the system access capabilities granted, including the abilities of the system security administrators themselves.

Another procedure that system security administrators should perform is to immediately remove the user IDs of terminated or transferred users. Procedures should be established that require department managers and/or the Human Resources Department to notify all applicable system security administrators when employees terminate or transfer. Such notification should take place within one day or less of the transfer or termination to reduce the risk of unauthorized actions by the terminated or transferred employee before having his or her system access revoked. Telephone calls are the quickest way to notify system security administrators of terminations and transfers. Telephone notification usually must be followed up with a written memo. An alternative notification means e-mail. E-mail is very timely, and, if the e-mail system and originating user ID are properly secured, the e-mail message can serve as the documented authorization mechanism.

4.19 WIRE TRANSFER FRAUD

Many types of fraud, such as loan fraud, can be costly to financial institutions. Some loan fraud schemes take months or years to reach significant proportions, while others require the perpetrator to expend a great deal of effort in preparing false documents to prevent detection while trying to carry on their normal duties. Even when a fraudulent loan has been executed, the task of withdrawing the funds by cash or check is difficult to accomplish without being noticed. Losses from wire transfer fraud, on the other hand, can occur instantaneously. Sometimes wire fraud can occur with little or no planning. For example, wire fraud can occur from an opportunistic wire transfer operator who notices that another operator has left his or her workstation without signing off. What makes wires so risky is that, to the delight of perpetrators, the funds are immediately available for withdrawal.

4.20 OPERATIONAL PROCEDURES

The most critical operational flaw pertained to inadequate segregation of duties. Financial institutions process enormous dollar amounts through their wire transfer systems. According to the National Organization of Clearing Houses, in 1996 the average wire transfer transaction size was $3 million on Fedwire, the Federal Reserve Bank's national wire transfer the system, and $6 million on CHIPS (Clearing House Interbank Payment System). In 1996, daily turnover was 5 times bank capital for Fedwire and 76 times reserve accounts for CHIPS. In total, daily turnover for wire transfer systems exceeded

bank reserves by $600 billion. Because of the tremendous financial volume of wire transfers, the goal of wire transfer controls at each financial institution should be to ensure that no one person can perform a wire transfer alone. In other words, wire transfer controls should enforce the segregation of duties. Without such segregation, financial institutions are subjecting themselves to the largest risk of loss among all the activities they perform. A single unauthorized wire can wipe out a financial institution's earnings for an entire year. Each day, financial institutions wire funds among themselves that can exceed the total amount of all their assets.

In the financial institution being audited, the wire transfer application was called Feline II. Feline II was supplied by the U.S. Federal Reserve Bank. It is a microcomputer-based application that is installed at thousands of financial institutions throughout the United States. The application was designed to perform two of the three steps necessary to transact an outgoing wire. The three steps of a wire transfer are initiation, verification, and transmission.

Initiation is when a wire operator enters wire information (routing number of the destination financial institution, the recipient's account number, the dollar amount, and so on) into Fedline II.

Verification is when a second wire transfer operator with a different user ID from the initiating user ID confirms that the initiated wire instructions were accurately entered into Feline II.

Transmission is when the wire instructions are electronically transmitted to Fedwire, the Federal Reserve's host wire transfer system. Fedwire debits the sending financial institution's account at the Federal Reserve and credits the receiving financial institution's account at the Federal Reserve. The receiving financial institution then credits the beneficiary's account.

Fedline II enables initiation and verification to take place at a financial institution. However, the transmission of a wire transfer requires a user at the financial institution to be signed on to Fedline II and then to sign on to the Federal Reserve's host wire transfer system, Fedwire. Then and only then can transmission of the wire take place. The fact that a user must be authorized on two systems is the key to ensuring that one person cannot perform a wire alone. Unfortunately, if operational and logical security controls are not properly implemented, one person could easily perform an unauthorized wire. In fact, during the audit in question, it was found that two users had the system access capability to perform unauthorized wires alone. Furthermore, this problem was not unique to the financial institution being audited. A Federal Reserve system security administrator stated that this condition existed at almost all the over 10,000 U.S. financial institutions with Fedline II. Ensuring adequate segregation of duties within a wire process that utilizes Fedline II requires three controls:

1. The Fedline II verification parameter must be set to require verification by a user other

ethen the one who initiated the wire.

2. Any Fedline II users with system security administrator access capabilities should not be authorized users on Fedwire. In other words, they should not be able to transmit wires.
3. Any Fedline II users with system security administrator access capabilities should not be designated as the authorized "security contact" with the Federal Reserve Bank. The security contact is the person who notifies the Fedwire system security administrator to add and delete users. The security contact is authorized in writing by the financial institution's treasurer, assistant treasurer, or another authorized signer on the financial institution's account at the Federal Reserve.
4. Control 1 is critical to ensure that wire transfer operators cannot initiate and verify a wire-alone. It is acceptable for wire operators to transmit alone because they cannot do so until Fedline II has confirmed that the wire instructions were verified by a different user.

Controls 2 and 3 are critical in that they prevent one-person wires even if the Fedline II system security administrators have circumvented the Fedline II verification controls. Fedline II system security administrators could circumvent the verification controls in two ways. First, they could simply change the verification rule to not require a different user ID to verify any initiated wire instructions. Alternatively, Fedline II system administrators could create one or more phoney user IDs. One could be used to initiate a wire, and the other could be used to verify the falsely initiated wire. The financial institution in question did not have control 2 or 3 in place. Two users had system security administration capabilities and were also authorized users on Fedwire. In addition, one of the two system security administrators was the financial institution's designated security contact. Based on inquiries with the Federal Reserve system security administrator, it was found that the Federal Reserve does not require that the financial institution's security contact be someone other than the Fedline II system security administrator. Furthermore, no such recommendation by the Federal Reserve was in the Fedline II system documentation.

When auditing a wire transfer system, remember to evaluate the procedures that segregate duties as well as the people who have system security administrator access capabilities, regardless of whether they use them. A user may procedurally not be a system security administrator or designated backup but could have the same system access capabilities. If that person is also authorized to transmit wires via Fedwire, then he or she could perform an unauthorized wire alone.

4.21 SYSTEM SECURITY ADMINISTRATION

Fedline II was designed with logical security controls, which, if properly deployed, could provide reasonable assurance that outgoing wire transfers were entered by one person. Unfortunately, it was found that logical security controls were not properly deployed. Some of the control weaknesses noted include:

- A Fedwire user ID and password for transmitting wire information to the Federal Reserve were shared by various users in the department. In addition, terminated personnel knew the user ID and password because they had not been changed for several months. Furthermore, the user ID and password had been included in the written procedures of the department.
- Fedline II user IDs existed for four transferred users and two users who no longer required access as part of their normal duties. One user never changed her password after her initial sign-on. She was still using the standard initial password of "pass1234" (the system did not force password change). Seven users shared the same Fedwire user ID and password. Seven users were assigned various access capabilities that were not required as part of their normal duties.

A large bank in the Eastern United States incurred a $1.5 million loss to a former manager at a large international public accounting firm. When the manager learned that the bank had eliminated its information security function during downsizing, he resigned from the public accounting firm and started his consulting firm, specializing in data security and integrity. Using social engineering, the consultant obtained secret computer codes directly from a senior management information systems (MIS) officer. Using these codes, he initiated a $4.3 million wire transfer from a commercial customer's concentration account to an account he opened in Switzerland. By the time the fraud was discovered the next day, the consultant had already flown to Switzerland and withdrawn the equivalent of $4 million ($300,000 in currency, $2 million in bearer bonds, and $1.7 million in manager's checks). After nearly a year on the run outside the United States, the consultant was apprehended by customs agents as he tried to return to the United States. By then he had spent $1.3 million but still had $2.7 million in his possession. Through a plea bargain, the consultant confessed to one count of wire fraud, which was punishable by a fine of $1,000 and/or five years in prison. In exchange for consulting with authorities as to how he perpetrated the scheme, the courts did not fine the consultant and he was sentenced to only 30 months in a minimum-security prison.

This article points out the need for employees at all levels of an organization to be adequately trained not to share sensitive information with anyone unless they are certain that the requesting party is authorized. A Bloomberg news release reported that a Russian computer expert and his wife were charged in the United States with breaking into Citibank's cash management system and, from June to October 1994, transferring $10 million to accounts he and at least four others had set up in Finland, Russia, Germany, the Netherlands, the United States, Israel, and Switzerland. Citibank's cash management system is used by customers to shift funds from their Citibank accounts to their accounts at other banks. According to a Citibank official, all but $400,000 of the money the ring withdrew was recovered and client funds were never at risk (in other words, Citibank absorbed the loss). The ring breached Citibank's internal control system by using the identification numbers and passwords of employees of the three Citibank customers that were victimized. The customers were themselves banks, two from Argentina and one from Indonesia. The charges did not specify how the passwords and identification numbers were compromised by the ring. Security analysts not involved in the case speculated that the ring could have gotten help from "renegade" employees at Citibank or

the victimized banks. One security analyst revealed that bank frauds often involve people who have access to secret passwords or confidential information and that the amount of crime committed by insiders is far greater than that from outsiders.

According to a Wall Street Journal report covering the same wire transfer fraud story, the Russian "hacker" exploited a method by which employees of Citicorp corporate Clients can access accounts and transfer funds from them. This type of access is guarded by multitiered authentication. Some have suggested that knowing the system well enough to penetrate its security may have been impossible without information coming from a Citicorp employee. The fact that this fraud was believed to have been perpetrated with the assistance of one or more bank employees demonstrates the need for information systems to be designed so that employees cannot access customer passwords. Readers should note that fraud in all types of organizations, not just banks, can occur from employees who have access to secret passwords and confidential information. Therefore, systems should be designed so that passwords are encrypted and no one, including a system security administrator, can view them. The design should also include an unalterable audit trail so that if a system security administrator were to reset a customer's password and perform unauthorized transactions, the action could be irrefutably traced to the offending system security administrator, thereby incriminating him or her. Bloomberg reported yet another wire transfer breach at a financial institution. United States authorities charged a former employee of Amsterdam-based ABN Amro Bank NV with 11 counts of embezzling a total of $1.9 million between March 1991 and September 1993. The former employee, who was an assistant vice president at the bank's San Francisco office, stole the money by arranging wire transfers of funds from ABN Amro Bank accounts in San Francisco to an ABN Amro Bank account in New York and then on to an account she controlled at another bank in San Francisco.

ATM Vendor's Adjustment Request Application: Several design flaws and system security administration weaknesses were identified in this application, which resulted in an increased risk of unauthorized access. The design flaws were that passwords could be as short as two characters, the system security administrator could view user passwords from within the application, and a password expiration feature was lacking. The system security administration weaknesses included two employees who had transferred to other areas of the company but still had valid user IDs on the system; one user had three different valid user IDs, one of which had system security administrator access capabilities even though such access was not part of his normal duties; and one valid user ID existed for an employee who had been terminated several months earlier.

ATM Vendor's Replacement Card/PIN Application: As with the previous application, weaknesses were found in both system security design and administration. The design issues were that passwords could be as short as four characters and a password expiration feature was not available. The system security administration control weaknesses included the fact that five users were granted system access capability, which enabled them to purge the audit log file of system security-related events and perform application

screen design functions. In addition, the original system diskettes were stored in the user documentation manual instead of in a locked location.

ATM Vendor's Hotcarding Application: System security design flaws and administration weaknesses were also evident in this system. The design flaws included passwords that could be as short as zero characters and the lack of a password expiration feature. Control weaknesses that could have been avoided with proper system security administration procedures included the fact that one user had system security administrator access capabilities that were not required as part of her normal duties, the system security administrator had a 20-minute session time-out parameter setting instead of 5 minutes like the other users, and all user IDs were named after department positions rather than usernames. This last control weakness was operationally workable so long as the position names were unique, and passwords were not shared by multiple users. But the practice of assigning the user's actual name to user IDs provides a better audit trail.

Summary of ATM Vendor Applications:, from the number and types of design flaws described for each of the three applications, system security was not a primary consideration during the design phase of their development. The ATM Department compounded the system security design flaws by failing to implement adequate system security administration procedures. It was recommended that the management of the ATM Department send a letter to the ATM switching service vendor, requesting that each of the identified security design flaws be corrected in future releases of the ATM applications. It was also recommended that ATM Department management resolve the identified control weaknesses and implement procedures to help ensure that similar control weaknesses do not occur again.

4.22 SELF-ASSESSMENT QUESTIONS

Q.1 Define security and describe physical security, logical security, and security guards with suitable examples.

Q.2 Explain general emergency and detection controls with relevant examples.

Q.3 Design and describe a logical security system with examples.

Q.4 Describe each of the following:

i. Heating, ventilation, and cooling systems
ii. Business resumption program
iii. Information System Business Resumption Program
iv. Backup System Security administration
v. Wire transfer fraud
vi. Remote access control

4.23 ACTIVITIES

Design a conceptual model of the logical security system.

4.24 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised; Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research, 21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly, 26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal, 5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica, 14*(1), 43.

UNIT-5

Information Systems Operations; Control Self-Assessment and an Application in an Information Systems Environment

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

This unit briefly discusses how to audit information systems (IS) operations from a broad perspective. It also includes examples of a variety of real-world internal control weaknesses and inefficiencies about IS operations. Some of the computer operations control discussed in this unit are closely related to physical security controls. This unit also describes business operations, internal database balancing and monitoring, control self-assessment, internal control framework (COSO) etc. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- Information systems operations
- Computer operations
- Production job scheduling and monitoring
- Business operations
- Internal database balancing and monitoring
- Control self-assessment
- Internal control framework

5.1 INFORMATION SYSTEMS OPERATIONS

Information systems operations include internal controls at data processing facilities as well as those in place in end-user environments, which are designed to help an organization's operational processes function as efficiently and effectively as possible within the constraints imposed by the economic, financial, political, legal, and regulatory environments. Because all operations throughout an organization are interdependent, auditors should not view IS operations as separate functions from the other operations within an organization. They are all essentially part of the same large "information system." They form one comprehensive input, processing, and output engine working toward achieving the organization's long-range strategic objectives. Therefore, when examining IS operations, auditors should consider the overall impacts of inefficiencies and ineffective procedures on the organization's ability to achieve its long-term objectives. With the proliferation of distributed data processing systems in recent years, IS operations of various scales have materialized at multiple locations within most organizations. Computers and related peripheral hardware devices can exist centrally, as at a large data centre, as well as at every physical location in a company, as in the case of a wide-area-network (WAN) that enables all processes within an organization to electronically exchange information. Within these IS operations, each functional area is responsible for conducting its processes in a responsibly controlled manner. Because of how widespread IS operations are, all auditors should be familiar with the approaches that are necessary to assess their adequacy. To provide a high-level approach, IS operations within an organization can be divided into two interrelated components: computer operations and business operations.

5.2 COMPUTER OPERATIONS

Computer operations consist of those IS processes that ensure that input data is processed efficiently and effectively to support the strategic objectives and business operations of an organization. A typical computer operations audit should include assessments of internal controls that ensure that:
Production jobs are completed promptly and production capacity is sufficient to meet short- and long-range processing needs Output media are distributed in a timely, accurate, and secure manner Backup and recovery procedures adequately protect data and programs against accidental or intentional loss or destruction Maintenance procedures adequately protect computer hardware against failure Computer hardware, software, and data are insured at replacement cost Problem management procedures ensure that system problems are documented andresolved in a timely and effective manner

5.3 PRODUCTION JOB SCHEDULING AND MONITORING

Automated job scheduling and initiation software can significantly enhance operational efficiency by automatically initiating the next scheduled production program immediately upon completion of the previous program. Each job should be assigned a priority number (e.g., one through nine, with one having the highest priority), which enables the job-scheduling software to initiate programs with the highest priorities first.

While computer operators still need to monitor the program queue for abnormal program failures and may occasionally need to alter the sequence of program initiation, this kind of software significantly reduces the need for computer operators to manually initiate each program, thereby freeing them to perform other duties. Automated job-scheduling software also reduces the risk that a computer operator may run a program out of sequence or forget to run one altogether.

When a program is run out of sequence or not run at all, subsequent data output may not be correct because it is dependent on updated data from the program that should have been completed previously. To monitor the effectiveness of the automated job-scheduling software, management of the computer operations area should receive a system-generated daily production report indicating the start and end times of each job, preferably with a comparison to the planned production schedule, and any job that abnormally terminated. This information provides management with a tool to independently assess whether jobs are being completed on time and following the preapproved schedule. Problems may identify a need to alter the sequence in which jobs are scheduled to utilize system processing capabilities more efficiently. Management can also observe whether many jobs are abnormally terminating. Such activity could indicate a system programming problem or the need to expand the production capacity of the system hardware. Other monitoring controls that should exist include periodically examining the amount of available disk storage and the dynamic system capacity utilization. Examining the amount of available disk storage space is like checking the amount of disk space available on the hard drive of a personal computer. Dynamic system capacity utilization is more difficult to determine. This monitoring control involves tracking the percentage of total system processing capacity that is used over a specific time, such as one day, one week, one month, or one year. It is preferable for a system to automatically log this information and generate management reports for the desired periods. This information can assist management in scheduling system maintenance, planning production schedules, and identifying when the system is reaching a capacity utilization level that requires upgrading the system to accommodate higher volumes of data processing. Some more sophisticated systems can be programmed to page or e-mail a system administrator if a predetermined processing capacity or data storage threshold is exceeded.

5.4 OUTPUT MEDIA DISTRIBUTION

Many productions jobs result in the creation of electronic output files. These output files are stored in a temporary queue sometimes referred to as a SPOOL, which stands for "simultaneous peripheral operation online." Output files in the SPOOL can be printed, copied to another directory, or both, depending on the requirements of the data owners. These activities should be performed by an output distribution area promptly so that the data owners can effectively utilize the information. Output files should also be purged from the SPOOL regularly, typically within one or two days, to free up disk storage space. Physical output media (paper printouts, microfiche, and microfilm) should be

strictly controlled to ensure that unauthorized personnel are not able to view or acquire sensitive information. Similarly, logical access to the SPOOL files should be granted only to necessary computer operations staff and system security administrators. This is an important control because an unauthorized user with access to the SPOOL could quickly view, copy, and possibly alter a wide variety of data files containing sensitive information.

5.5 BACKUP AND RECOVERY PROCEDURES

Every organization should have a business resumption plan. As part of the plan, procedures should exist to adequately protect data and programs against accidental or intentional loss or destruction. The primary controls to provide this protection are to perform periodically (daily, weekly, monthly) backups of the system software, application programs, and data as well as storage and rotation of the backup media such as magnetic tapes, disks, and compact disks (CDs) to a Secure off-site location.

Daily backups are usually necessary only for data since the application programs and system software do not change significantly. Full backups of the entire system, including system software, application programs, and data, should be performed weekly or monthly, depending on the number and types of changes that have been made. Full system backups should also be performed on completion of a major upgrade or significant changes to the operational and security parameters of a system. Furthermore, management should ensure that tests are performed to confirm that system operations can be fully restored using the backup media. This is one test that is often overlooked.

5.6 MAINTENANCE PROCEDURES

All computer hardware should be serviced according to the manufacturer's recommendations as specified in the contract with the hardware vendor. Maintenance procedures should adequately protect computer hardware against failure over the expected useful life of the equipment. In most instances, proper maintenance is also a requirement for the manufacturer's warranties on the equipment's performance to remain in effect. For this reason, every organization must maintain accurate records of all maintenance performed. Depending on the type of equipment deployed in an organization, vendor technicians or subcontractors may need to perform the necessary maintenance services. If so, the costs and availability of routine and nonroutine maintenance procedures should be documented in the contract with the vendor or subcontractor. Before allowing maintenance services to be performed by in-house technicians, management should review the contract terms to ensure that any warranties will not be invalidated if nonvendor technicians perform the maintenance. The contract may allow nonvendor technicians to perform the maintenance but require them to be certified experts in the technology being maintained for the warranty to remain in effect.

5.7 INSURANCE

Every organization should purchase insurance in an amount that adequately covers all computer hardware and software at replacement cost, the costs to recreate any lost data, and possibly the value of lost revenues that are the direct result of computer hardware or software failures. The insurance policy may require that routine maintenance procedure specified by the computer manufacturers be performed for coverage to remain in effect. The policy may also specify that daily, weekly, and monthly software and data backups be created and stored at a secure off-site location. Deductibles should be set at levels that provide a reasonable balance between annual premiums and the overall coverage amount.

5.8 PROBLEM MANAGEMENT

The number and types of system problems that arise should be carefully logged to help ensure that system problems are documented and resolved in a timely and effective manner. Some organizations maintain a central Help Desk Department that fields various user telephone inquiries, including those about system problems. Other organizations may require the process owners of each system to field and resolve their system problems. In either case, all system problems should be logged, preferably in an electronic format that facilitates management review and that can be provided to system vendors for use in troubleshooting the causes of any problems. Types of information that should be logged include the date and time the problem was reported; a description of the problem; the name, title, department, e-mail address, and telephone number of the individual reporting the problem; and the action steps taken by the person fielding the report. Actions may include resolving the problem over the phone, referring the problem to a technician, or escalating the problem to a manager. Follow-up procedures should exist whereby a designated person in the problem resolution area or help desk tracks each action step taken after the initial report and records it in the log until the problem has been resolved. Even minor system problems should be noted in the log since a high incidence of minor problems may be a precursor to more serious problems. If a particular problem cannot be resolved, the reason should be recorded in the log. Periodically, (e.g., weekly), a management report of system problems should be prepared. The report should classify problems as type and severity to enable management to determine the frequency and urgency of the problems that occurred over the period under review. Unresolved problems should be highlighted, especially those that have not been corrected for an extended period. The report should be reviewed by management in affected areas. Significant problem trends and other related system performance issues should be communicated to vendors, technicians, and other appropriate parties.

5.9 BUSINESS OPERATIONS

Business operations consist of all other functions within an organization besides those in the computer operations area. Business operations areas typically provide input data to the computer operations area and utilize the resulting output in their daily processes.

Business operations audits should include assessments of the adequacy of internal controls about all significant aspects of the process under consideration. The number and types of internal controls in a business operation will vary greatly depending on the type of business or process being audited. In the operating environments of almost every organization, there are many end-users of IS controls. These controls must function in tandem with traditional centralized computer operations controls to adequately protect the organization against unauthorized system access and to help ensure that business operations are being carried out efficiently and effectively.

In other words, internal controls in centralized computer operations areas complement those in business operating units and vice versa. Neither can function effectively without the other. As mentioned at the beginning of this chapter, computer operations and business operations together comprise the IS operations of an organization. An organization's internal control environment is indeed only as strong as its weakest component. Information systems control existing in business operating environments can pertain to each of the three basic electronic data processing categories: input, processing, and output. But there are other controls impacting information systems that are critical to the effective functioning of business operations. Several examples of business operations control likely to be encountered are presented next.

5.10 EDIT AND REASONABLENESS CHECKS

To help prevent invalid data from being entered into a system, many systems are programmed with automated *edit and reasonableness checks.* For example, edit checks can prevent letters from being entered into a field that should only have numbers or vice versa. Edit checks can also prevent invalid codes from being entered into a particular field and can prevent dates or amounts outside of predetermined ranges from being entered. Some systems require a second data entry person to rekey some or all of the data that was key entered by the original data entry person and will accept the data only if both sets of data are the same. Alternatively, edit checks can be a detective in nature. In other words, edit controls can be manual or after the fact.

For example, a system may generate a data entry report that must be compared to the original input documents to identify any errors, or a system may accept and attempt to process all the data originally entered and generate exception reports in which key-entered data did not meet prescribed standards or filters. The recipient of the exception reports must then enter the necessary corrections to the original data. Detective IS controls are usually less efficient and effective than preventive controls because they require additional action and thus slow down the overall process.

5.11 INTEGRITY/COMPLETENESS CHECKS

When large volumes of data are electronically imported from or exported to other systems, data integrity and completeness controls can provide reasonable assurance that

the recipient has received all the data intact, without any alterations or missing information. *Control totals* are the most common form of integrity/completeness check. The sender provides the recipient with control totals, such as the total number of records in the data file and the total dollar amount of the records. When the recipient processes the data, the total number and dollar amount of items received can be compared with those provided by the sender to determine whether there could be missing or altered records. However, control totals may not identify instances in which records have been altered in a field other than the amount. For example, a destination account number or customer name may be changed to that of an unauthorized account. In this case, the total number and dollar amount of the original records would not be changed and thus would not be identified by basic control totals.

5.12 HASH TOTALS

Hash totals are a common form of integrity/completeness control that can reduce exposure to altered records. A hash total is simply a number that is calculated based on a key field that does not normally have numeric calculations performed on it. For example, a simple hash total formula may add the account numbers or invoice numbers of every record in a data file. An alteration to even one of the account or invoice numbers would cause the hash total to change. When the recipient rehashes the data received, the total would not agree with the hash total supplied by the sender, thus alerting the recipient to a possible unauthorized change or unintentional scrambling of data during the transmission process. More complex hash totals that utilize arithmetic algorithms to calculate variations and combinations of multiple fields can be designed. The results may even be encrypted before transmission or transport. The basic objective is the same as with simple hash totals.

5.13 SEGREGATION OF DUTIES

When examining a business operation or traditional centralized IS processes such as computer operations, systems development, and program change control, one of the most critical internal control objectives is the segregation of duties. Duties must be properly segregated to adequately protect an organization from unauthorized access to information, loss of physical or financial assets, and a myriad of other potential risks. Segregation of duties can therefore exist in data entry areas, data processing areas, and in business operating areas in which processing output is utilized. Segregation of duties can be most effectively enforced through the proper deployment and administration of system access capabilities. (See Chapter 8 for a complete discussion of system access controls.) Implementation of strong procedural controls is equally as critical but more difficult to enforce because of the increased possibility of human error or distraction. As will be seen in some of the examples later in this chapter, the segregation of duties is where business operations often falter.

5.14 EFFICIENCY/EFFECTIVENESS CONTROLS

Within any business operation, there are almost always opportunities to enhance efficiency and effectiveness by automating manual procedures. Management may often overlook obvious opportunities because they are preoccupied with meeting ongoing deadlines and dealing with day-to-day operational issues. Ironically, if management were to automate some of their most difficult and time-consuming processes, they would enhance their ability to meet deadlines and reduce the severity of the operational difficulties that are causing them the most grief.

5.15 INTERNAL DATABASE BALANCING AND MONITORING

Management reports and other information that are derived from internally generated databases are only as reliable as the data from which they originate. Many organizations create *extract databases* for use in preparing various types of specialized reports. Extract databases, which are essentially copies of original production databases, enable multiple end-user areas to prepare customized reports and perform various database analyses and other operations without impacting the production operations. Extract databases thus make the information available to a greater number of users within an organization who, through their analyses, can help their organization more effectively attain its objectives. Security over the information must be tight to ensure that the information is not compromised. An additional, perhaps more critical concern is that the extract program creates an accurate database. Otherwise, information and analysis results derived from the extracted database may be incomplete or meaningless, possibly resulting in material misstatements of information or poor strategic decisions.

5.16 INADEQUATESUPPORTOFEND-USER APPLICATIONS

Customized computer application programs are being developed at an alarming rate in end-user areas. Many of these applications are created by individuals who have a limited amount of technical training. As a result, documentation as to the logic and design of the applications is usually limited or non-existent. Then, when the developer transfers or terminates, so does all the knowledge about how to support the application. Some end-user applications are relatively simple and can easily be re-created and even improved when the developer leaves. There are also many highly complex applications upon which end-user organizations have become highly dependent. If the developer transferred or terminated and a problem arose, management could be seen frantically trying to contact the previous developer. The resulting impacts on the business operations could have been avoided had management required the developer to take the time to document the application from the very beginning so that another person with reasonable knowledge about the development language or software could support the application.

5.17 EFFICIENCY AND EFFECTIVENESS OF INFORMATION SYSTEMS IN BUSINESS OPERATIONS

Auditors should always be on the lookout for opportunities to recommend the automation of previously manual procedures to increase operational efficiency. Management is often so concerned with day-to-day operations that they overlook automation opportunities. In some cases, management may not be aware of new technologies that would enable an operation to be automated with relative ease. In other cases, management in business units may look to the Internal Audit Department to assist in being heard by management of the IS development process. Internal auditors can reinforce a business operation's justification for a programming request to automate a procedure. This is not to say that an operation should automate simply for the sake of automating. There must be concrete evidence that the benefits of automation will outweigh the costs of designing and programming the system.

The same arguments can be made for effectiveness opportunities. Sometimes a process may already be automated, or a system may be providing automated information, but the quality of the service or product could be enhanced through a change in the automation process. For example, customers may be receiving automated transaction statements or invoices, but the information on the documents may be unclear or confusing. In this case, a change in the type or clarity of information provided would make the statements and invoices more effective for customers. Quite often, efficiency improvements concurrently provide enhancements to the effectiveness of an operation.

5.18 CONTROL SELF-ASSESSMENT AND AN APPLICATION IN AN INFORMATION SYSTEMS ENVIRONMENT

Control Self-Assessment (CSA) is a leading-edge process in which *auditors* facilitate a group of *staff members* who have expertise in a specific process, to identify opportunities for internal control enhancement of critical operating areas designated by *management.* The CSA process is usually accomplished during *workshops.* Note in the definition that the words *auditors*, *staff members*, and *management* have been *italicized.* The reason is to emphasize that a CSA workshop can be successful only through the combined positive efforts of each of these three groups of individuals, or *players.* If any one of the players does not adequately perform his or her role, constructive ideas to enhance the internal control environment will not be as effective as they otherwise could have been. Other keywords in the CSA definition are *facilitating, identifying,* and *critical.* Each keyword relates to the role that each of the three groups of CSA players must perform. Successful CSA depends on auditors effectively facilitating a lively, open, honest, and constructive session. Without effective facilitation, a CSA workshop can easily wander into irrelevant topics or negative discussions about problems with other individuals or departments that do not pertain to the objectives of the workshop. This can result in wasting valuable time and resources. Staff members are also essential to the success of a CSA workshop because they have a detailed working knowledge of the process being evaluated. With their detailed knowledge, they are in the best position to identify which internal controls

are working well, which ones are not working well, and how internal controls could be most effectively improved. Management's role is to designate those operating areas that are critical to the success of the process being evaluated, whether it is a department, operating unit, or higher-level organization. Management is also instrumental in the implementation of the internal control enhancements identified by their staff members.

5.19 HISTORY OF CONTROL SELF-ASSESSMENT

The CSA concept was originated in the late 1980s by Bruce McCuaig, then at Gulf Canada Resources, a subsidiary of Gulf Corporation. Another CSA pioneer at Gulf, Paul Makosz, assisted McCuaig in developing CSA into a process that could be used to measure soft controls, which traditional audit techniques could not measure. These soft controls include things like management's integrity, honesty, trust, willingness to circumvent controls, and overall employee morale. Collectively, these attributes comprise an organization's corporate culture, which is often derived from the tone at the top. This phrase refers to the fact that unwritten accepted corporate standards of conduct take their cue from the behaviour and actions of the leaders of an organization; key officers such as the chairman, chief executive officer (CEO), president, and other senior executives. The reason for wanting to measure soft controls is that soft control failure has often been attributed to the demise of many failed organizations. Soft control failure coupled with a rapidly increasing interest rate environment was almost entirely responsible for the near extinction of the savings and loan industry in the United States. Because of his early experimentation and continuing enhancements to CSA approaches, as well as his efforts to promote CSA, Makosz is now considered by many to be "the father of CSA." Both McCuaig and Makosz have left Gulf Canada Resources and established successful consulting practices that specialize in CSA. By the early 1990s, a few other organizations began implementing CSA. For example, in 1991, Jim Mitchell, the general auditor of MAPCO, Inc., a Fortune 500 energy corporation headquartered in Tulsa, Oklahoma, became interested in CSA and put it into practice in 1992. By 1996, CSA was one of MAPCO's three major audit methods, and about 30 percent of MAPCO's audit resources were devoted to CSA. MAPCO was so successful with its CSA program that two of its former CSA managers published an article that described their approach.

During the mid-1990s, interest in CSA began taking the auditing world by storm. The Institute of Internal Auditors (IIA) hosted its first CSA conference in Orlando in 1995. This conference was so successful, the IIA hosted a second CSA conference in Toronto in 1996 and a third in Las Vegas in 1997. Based on the enormous popularity of CSA, the IIA now hosts annual CSA conferences and training seminars. By 1996, all the Big Six (now Big Four) accounting firms had begun to offer CSA consulting services, although their degrees of commitment varied. Deloitte & Touche, LLP, had been the most aggressive CSA proponent among the Big Six in terms of the number of CSA consultants they hired and their visibility and participation at CSA conferences. Deloitte and Touche also invested significant financial resources in hiring CSA experts and marketing CSA services. Some of their experts were hired directly from firms like MAPCO, Inc., which pioneered CSA. Deloitte & Touche was also the most visible at the 1996 CSA

conference. Other Big Six firms represented at the conference included Ernst & Young, LLP; KPMG, LLP; and Arthur Andersen, LLP. The remaining Big Six firms, Coopers & Lybrand, LLP, and Price Waterhouse had also begun to offer CSA services. In January 1997, the IIA launched its Control Self-Assessment Center. The objective of the center is to offer guidance and training opportunities to individuals engaged in the practice of CSA. Some of the services provided by the center include *The CSA Sentinel*, a triannual electronic newsletter; professional guidance on CSA implementation; a series of CSA seminars culminating in CSA qualification; reduced prices on IIA products related to CSA; and an annual directory of CSA Center participants. By 1997, many major organizations around the world had implemented CSA programs to varying degrees. However, these CSA pioneering organizations represented a vast minority of all the organizations in the world. Many organizations had been considering implementing CSA, but relatively few had implemented CSA, even to a limited extent. The reason was that implementing CSA requires a major commitment from all parts of the organization, including the Internal Audit Department as well as all levels of management.

5.20 KEYS TO A SUCCESSFUL PROGRAM

Control Self-Assessment is still in an early growth stage in its evolution. Relatively few organizations have taken the plunge and committed of time and resources necessary to develop and implement an effective CSA process. As with any new business venture, there are risks involved with the implementation of CSA. The purpose of this section is to help reduce those risks so that the CSA program can be successful and to identify six key elements of a successful CSA program. The most important part of any CSA program is the need to obtain the encouragement and support of senior management. Without their backing, lower levels of management will not be anywhere near as likely to take the process seriously. Without serious participation, a CSA program could be viewed as a waste of time. Senior executives and others who support and promote CSA are fondly referred to as "champions" by those in the CSA arena. Senior management support must be earned through effective demonstrations of the potential for significant gains in operational efficiency and effectiveness, and reductions in exposure to financial, regulatory, and other significant risks. These demonstrations can be supported by success stories at various companies that have implemented successful CSA programs (e.g., MAPCO, Inc.). Articles written about CSA (see the previous section) may need to be referred to, and senior management may have to be better educated on the objectives of internal controls. This brings up the second key to a successful CSA program. To effectively sell CSA to senior management and to effectively facilitate a CSA workshop, auditors must be intimately familiar with the objectives of internal controls. There are several contemporary national and international models, or frameworks, of internal control. Six of the most well-known frameworks include COSO (United States, 1992); CoCo (Canada, 1995); Cadbury (Great Britain, 1994); COBIT (ISACA, 1996, 1998, 2000); SAC (IIA, 1977, 1991,1994) and eSAC (IIA, 2001); and SASs 55/78/94 (AICPA, effective 1990, 1997, 2001). A detailed understanding of these frameworks is pertinent to audits of all processes, including IS processes, in every country in the world. A brief discussion of each of these models follows.

5.21 INTERNAL CONTROL FRAMEWORKS COSO

The formal name of this report is *Internal Control-Integrated Framework*. It was published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in September 1992. The official name of the Treadway Commission was the National Commission on Fraudulent Financial Reporting, which was established in 1985 through the joint sponsorship of five U.S. organizations: American Institute of Certified Public Accountants, American Accounting Association, Financial Executives Institute, Institute of Internal Auditors, and Institute of Management Accountants (formerly the National Association of Accountants). The Treadway Commission, which was named after its first chairman, James Treadway, was charged with identifying the primary causes of fraudulent financial reporting, which had been proliferating in the United States during the 1970s and 1980s. The Commission was also responsible for providing recommendations to reduce the incidence of such fraud.

The Treadway Commission's 1987 report recognized that weak internal controls were the primary contributing factor to many fraudulent financial reporting cases. The report stressed the importance of the control environment, codes of conduct, audit committee oversight, an active and objective internal audit function, management reports on the effectiveness of internal control, and the need to develop a common definition and framework of internal control. The evolutionary process of developing a generally accepted definition and framework of internal control was finally realized in 1992 with the publication of the COSO report.

COSO defines internal control as:

A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

One of the key aspects of this definition is that internal control can provide only reasonable, but not absolute, assurance as to the achievement of the objectives. The report goes on to state that each of the above internal control objectives consists of five interrelated components, which are derived from the way management runs a business:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring

Another key concept of COSO is that management is responsible for an entity's internal control system, and the CEO should assume ownership of the control system. This concept is further supported by the fact that U.S. federal sentencing guidelines

complement the COSO framework. Whereas COSO defines what constitutes effective internal controls, the U.S. federal sentencing guidelines specify penalties for failure to maintain an effective system of internal controls. Senior management of organizations subjected to these penalties is ultimately responsible. A 1997 article provides an excellent comparison between COSO and the United States federal sentencing guidelines. For more details about COSO, please refer to the complete four-volume COSO report, which is available from the American Institute of Certified Public Accountants. The four volumes are *Executive Summary, Framework, Reporting to External Parties*, and *Evaluation Tools*.

5.22 CoCo

The formal name of this report is *Guidance on Control*. It was published by the Criteria of Control Board (CoCo) of the Canadian Institute of Chartered Accountants (CICA) in November 1995. CoCo is responsible for issuing guidance on designing, assessing, and reporting on the control systems of organizations. The CoCo guidance builds on the understanding of control set out in COSO. Like COSO, it defines control and specifies criteria for effective control. The CoCo control framework is intended to be used by people throughout an organization to develop, assess, and change control. CoCo defines control as "those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives." It defines three categories of objectives:

1. Effectiveness and efficiency of operations
2. Reliability of internal and external reporting
3. Compliance with applicable laws and regulations and internal policies

This definition is very similar to COSO, but the CoCo *Guidance on Control* presents additional concepts not contained in the COSO framework. Appendix 1 of the *Guidance on Control* provides an excellent comparison of COSO versus CoCo. Some of the key differences specified in that appendix are:

- Within the scope of control, CoCo includes objective setting, strategic planning, risk management, and corrective actions, while it excludes decision-making.
- CoCo explicitly states that control includes the identification and mitigation of the risks of failure to maintain an organization's ability to identify and exploit opportunities, and failure to maintain the organization's resilience.
- CoCo includes control criteria about mutual trust between people and the periodic challenge of assumptions.
- CoCo's concept of monitoring includes monitoring the operating performance of the Organization.
- CoCo judges the effectiveness of an internal control system about specific objectives (such as customer service levels), not a category of objectives (such as efficiency and effectiveness of operations).

5.23 COCO CRITERIA OF CONTROL REGROUPED INTO COSO COMPONENTS

Control Environment

B1 Shared ethical values, including integrity, should be established. communicated and practised throughout the organization.

B2 Human resource policies and practices should be consistent with an organization's ethical values and the achievement of its objectives.

B3 Authority, responsibility and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people

B4 An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives

C1 People should have the necessary knowledge, skills, and tools to support the achievement of the organization's objectives

Risk Assessment

A1 Objectives should be established and communicated

A2 The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed

A5 Objectives and related plans should include measurable performance targets and indicators

D1 External and internal environments should be monitored to obtain information that may signal a need to re-evaluate the organization's objectives or control

Control Activities

A3 Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated, and practised so that people understand what is expected of them and the scope of their freedom to act

C4 The decisions and actions of different parts of the organization should be coordinated.

C5 Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the interrelatedness of control elements.

Information and Communication

C2 Communication processes should support the organization's values and the achievement of its objectives

C3 Sufficient and relevant information should be identified and communicated promptly to enable people to perform their assigned responsibilities

A4 Plans to guide efforts in achieving the organization's objectives should be established and communicated

D4 Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified

Monitoring

D2 Performance should be monitored against the targets and indicators identified in the organization's objectives and plans

D3 The assumptions behind an organization's objectives should be periodically challenged

D5 Follow-up procedures should be established and performed to ensure appropriate change or action occurs

D6 Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable

5.24 CADBURY

The formal name of this report is *Internal Control and Financial Reporting*. It was published in December 1994 by the Committee of the Financial Aspects of Corporate Governance (Cadbury Committee) of the Institute of Chartered Accountants in England and Wales (ICAEW). Like CoCo, the Cadbury report builds on the understanding of internal control set out in COSO. Cadbury initially defines internal control as:

The whole system of controls, financial and otherwise, was established to provide reasonable assurance of:

- effective and efficient operations
- internal financial control
- compliance with laws and regulations

Cadbury goes on to define internal *financial* control as:

The internal controls established to provide reasonable assurance of:

- the safeguarding of assets against unauthorized use of disposition: and
- the maintenance of proper accounting records and the reliability of financial information used within the business or for publication.

The reason for the more specific internal financial control definition is that Cadbury requires that the board of directors of every company incorporated in the United Kingdom published a statement about their system of internal *financial* control. The statement must, at a minimum:

- Acknowledge that the directors are responsible for internal financial control.
- Provide an explanation that the system can provide only reasonable, not absolute, assurance against material misstatement or loss.
- Describe key procedures that the directors have established to help ensure effective internal financial control.
- Confirm that the directors have reviewed the effectiveness of the system of internal financial control.

Cadbury encourages but does not require, directors to state their opinion on the effectiveness of the system of internal financial control.

Cadbury's criteria for assessing the effectiveness of internal financial control fall into the five COSO-derived categories:

- Control environment
- Identification and evaluation of risks and control objectives

- Information and communication
- Control procedures
- Monitoring and corrective action

5.25 COBIT

COBIT, which stands for Control Objectives for Information and Related Technology, was published by the Information Systems Audit and Control Foundation in 1996 and updated in1998 and 2000. COBIT is a comprehensive internal control framework specifically about internal control issues associated with information technology (IT). COBIT's mission is to "research, develop, publicize, and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors." COBIT defines control as "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." This definition is very similar to the other frameworks previously discussed. Contrary to what some readers may have thought, the objectives of IS auditing are essentially the same as financial, operational, and other branches of auditing. The difference lies in the body of knowledge and the tools necessary to accomplish the objectives.

COBIT consists of six volumes: *Executive Summary*, *Framework*, *Control Objectives*, *Audit Guidelines*, *Management Guidelines*, and *Implementation Tool Set*. The COBIT package also comes with a diskette of the six volumes in ASCII format and a CD-Rom of the PowerPoint slides in the *Implementation Tool Set*. COBIT is an internationally developed, comprehensive IT evaluation tool that envelops virtually every major generally accepted standard in the world about controls and IT. Included for consideration during its development were standards from numerous organizations, including the International Organization for Standardization (ISO); Electronic Data Interchange for Administration, Commerce, and Trade (EDIFACT); Council of Europe; Organization for Economic Cooperation and Development (OECD); ISACA; Information Technology Security Evaluation Criteria (ITSEC); Trusted Computer Security Evaluation Criteria (TCSEC); COSO; United States General Accounting Office (GAO); International Federation of Accountants (IFAC); IIA; American Institute of Certified Public Accountants (AICPA); CICA; European Security Forum (ESF); Infosec Business Advisory Group (IBAG); National Institute of Standards and Technology (NIST); and the Department of Trade and Industry (DTI) of the United Kingdom.

5.26 SAC AND ESAC

The Systems Auditability and Control (SAC) report is intended to provide "sound guidance on control and audit of information systems and technology. The report focuses on the business perspective of information technology and the risks associated with planning, implementing, and using automation." SAC emphasizes management's responsibility to identify, understand, and assess the risks associated with the integration

of technology in an organization and to oversee and control the organization's use of technology. The SAC report was originally published by the IIA in 1977. It was the first internal control framework about IT. Due to the enormous changes in IT since 1977, an updated and extended AC report was published in 1991 and was then further revised in 1994. SAC defines the system of internal control as those processes, functions, activities, subsystems, procedures, and organization of human resources that provide reasonable assurance that the goals and objectives of the organization are achieved and ensure that risk is reduced to an acceptable level.

The SAC report consists of 14 modules: Executive Summary, Audit and Control Environment, Using Information Technology in Auditing, Managing Computer Resources, Managing Information and Developing Systems, Business Systems, End-User and Departmental Computing, Telecommunications, Security, Contingency Planning, Emerging Technologies, Index, Advanced Technology Supplement, and a case study.

5.27 SASs 55/78/94

The AICPA's Statements on Auditing Standards (SAS) 55, 78, and 94 pertain to the independent auditor's consideration of internal control in an audit of financial statements by generally accepted auditing standards. SAS 55, which was effective for audits of financial statements for periods beginning on or after January 1, 1990, used a non-COSO definition of internal control. SAS 78, which was effective for audits of financial statements for periods beginning on or after January 1, 1997, amended SAS 55 to include the COSO internal control definition and model of internal control. SAS 94, which was effective for audits of financial statements for periods beginning on or after June 1, 2001, added significant new sections regarding the effect of information technology on internal control.

SAS 94 specifies that an entity's use of IT may affect any of the five COSO components of internal control; that IT affects the fundamental way transactions are initiated, recorded, processed, and reported; that IT provides potential benefits of effectiveness and efficiency for an entity's internal control; and that IT poses specific risks to an entity's internal control such as:

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both
- Unauthorized access to data that may destroy data or improper changes to data, including the recording of unauthorized or non-existent transactions or inaccurate recording of transactions
- Unauthorized changes to systems, programs, or data in master files
- Failure to make necessary changes to systems or programs Inappropriate manual intervention
- Potential loss of data

SAS 94 goes on to recommend that the auditor should consider whether specialized skills are needed to determine the effect of IT on the audit, to understand the IT controls, or to design and perform tests of IT controls or substantive tests. A professional possessing IT skill may be either on the auditor's staff or an outside professional. But the auditor should have sufficient IT-related knowledge to communicate the audit objectives to the

professional, to evaluate whether the specified procedures will meet the auditor's objectives, and to evaluate the results of the procedures as they relate to the nature, timing, and extent of other planned audit procedures. Other key new statements in SAS 94 address the effects on the five COSO components of internal control. For example, SAS 94 recognizes that the *control environment* sets the tone of an organization and that management's failure to commit sufficient resources to address security risks presented by IT may adversely affect internal control by allowing improper changes to be made to computer programs or data, or by allowing unauthorized transactions to be processed; the use of IT may be an important element in an entity's *risk assessment* process; the use of IT affects the way that *controls activities* are implemented; the auditor should understand the automated and manual procedures an entity uses to prepare and *communicate* financial statements and related disclosures, and how misstatements may occur; if management assumes that data used for *monitoring* are accurate without having a basis for that assumption, errors may exist in the information, potentially leading management to incorrect conclusions from its monitoring activities.

5.28 SUMMARY OF THE SIX MAJOR INTERNAL CONTROL FRAMEWORKS

Each of the six internal control framework models just presented concludes that the boards of directors, officers, and other managers within every organization are primarily responsible for ensuring that effective control and risk management systems are in place. As an internal control expert, the role of an internal or external auditor is to consult with these key management personnel to help them better achieve their internal control objectives and responsibilities. This role is especially important in the information systems arena due to the rapidly changing environment that does not appear to have an end.

5.29 ADDITIONAL KEYS TO A SUCCESSFUL PROGRAM

The third key to a successful CSA program is the proper training of auditors in the skills necessary to facilitate CSA. Historically, auditors have interacted with client staff and management on a one-on-one basis or in small group meetings. Auditors were not typically required to facilitate discussion by other groups. However, as CSA becomes more and more the norm in leading-edge companies, the demand for IS auditors as well as non-IS auditors who possess CSA facilitation skills will be significantly enhanced. As a result, many firms are finding it necessary to send some of their staff to attend facilitation training to hone their facilitation skills. Because facilitation skills are often used by many course instructors, the training department within an organization should be able to assist in finding facilitation courses. Other possible sources would be conferences and seminars sponsored by local chapters and international headquarters of internal auditing professional associations such as the IIA and the ISACA. The IIA also sponsors the Certificate in Control Self-Assessment (CCSA) designation.

Auditors must also be highly knowledgeable about the internal control framework(s) adopted by an organization's audit department. Therefore, training of both IS and non-IS

auditors on the details of the applicable internal control framework(s) is also critical. Again, conferences and seminars can be an important source of training on internal control frameworks. The fourth key to facilitating successful CSA workshops is that the group being assessed should consist of staff members in the area being assessed but no supervisors or managers. If a management group is being facilitated, higher levels of management should be excluded from the CSA group. A manager insisted on attending one CSA workshop. When she excused herself to answer a pager call and stepped out of the room, there was a marked difference in the willingness of staff members to share their ideas and to participate in the general discussion. When the manager returned, she was oblivious to the staff members' return to their subservient role of looking at her before answering. Since management identifies the control objectives to be discussed in the workshop, they should not be concerned about what their staff might be saying. Instead, they should be optimistic that their people can develop workable solutions to the specified control objectives. Severe resistance to being omitted from a CSA workshop may even be a red flag that there could be some internal control environment weaknesses.

The fifth key to CSA success is having the proper tools. These tools include a private conference room or training room with flipcharts, marking pens, whiteboards or chalkboards, and other typical training materials, in addition to automated tools such as a laptop computer with a visual projection device for recording CSA successes, failures, and action items. For electronically tallying voting results, groupware products such as Option Finder can expedite the voting process, summarize, and analyze the results, and make the process more enjoyable. If the organization is on a low budget, scratch paper and a calculator can be effectively utilized. Be careful not to get carried away with automated tools. They can act as barriers between the groups, as in the case of a training room in which classroom participants each sit in front of their own workstation. Such an arrangement is not conducive to an interactive CSA workshop. A bag of miscellaneous toys or other amusements can prove effective at lightening the atmosphere of a CSA workshop and energizing the group when they get complacent.

Key number six to a successful CSA workshop is to avoid the pitfall of excessive time usage. In many CSA workshops, the need for better communication between management and staff, or between the operation being assessed and the outside departments or areas they deal with, is identified as an obstacle to effective job performance. CSA facilitators should be cognizant of this fact because, although communication among these areas is very important, an entire CSA workshop can be completely consumed by this one issue, often without any deployable internal control enhancements being developed. Ideas for enhancing inter- and intradepartmental communication should be discussed, but the CSA group should not be allowed to dwell on this one issue. During planning for the CSA workshop, the facilitator should accept this issue as a given and plan to spend only about 30 to 60 minutes discussing it.

5.30 DIFFERENT APPROACHES

CSA can be implemented in a variety of ways within an organization. Each approach has positive and negative factors. Therefore, the methodology adopted by an organization should be tailored to meet the specific needs of its management. It might even be necessary to apply one CSA approach for one set of operating units and a different CSA variation to another set of operating units. Four general types of CSA approaches can be utilized: pure CSA, centralized CSA, targeted CSA, and hybrid CSA.

Pure CSA: Pure CSA is a method in which operating units within an organization are responsible for conducting CSA workshops on an ongoing basis as part of their normal operating procedures. The Internal Audit Department or an external consultant usually designs and develops the CSA program to ensure consistent application throughout the organization. Also, internal auditors or consultants usually conduct the initial CSA workshop for each operating unit and provide training to the designated CSA facilitators within the operating unit. After the initial CSA workshop has been completed, management of the operating unit becomes responsible for ensuring that identified action items are appropriately addressed, future CSA workshops are conducted periodically (e.g., annually), and the results of the future CSA workshops are reported to appropriate areas within the organization. Under pure CSA, a central department receives a copy of the report of the results of each CSA workshop. This department then assumes the role of monitoring the progress of the implementation of any solutions and can act as a consultant and mediator on issues that span multiple operating units. This central department can be within the Internal Audit Department, or it can be a separate control-monitoring department. Advantages to pure CSA include complete ownership by operating units, increased awareness of internal controls and who is responsible for ensuring that they are adequately deployed, and more effective solutions because they come directly from the experts within the operating unit. Disadvantages include loss of continuity as turnover occurs within operating units, failure of operating unit management to consider the CSA process as important and thus failure to perform CSA workshops regularly, poor CSA facilitation within operating units, and stifling of new ideas by management of the operating units. The World Bank, headquartered in Washington, D.C., has implemented a pure CSA approach. At the 1996 CSA Conference in Toronto, Blanshard Marke, senior controls specialist at the World Bank, described in detail the approach used in his organization. Marke shared the idea that management wanted to remove the notion that the Internal Audit Department was responsible for internal control. Therefore, the World Bank established a separate Controls Department and charged it with implementing CSA in various work areas.
The main elements of the World Bank methodology are:

- CSA is implemented by management.
- The Controls Department provides intellectual leadership, counsel, and advice.
- The Internal Audit Department and external auditors are actively involved.
- Business units take over the CSA process after the first year. Designated "COSO Champions" are trained to perform future CSA workshops.
- The implementation of action plans is monitored by the Controls Department.

Marke identified the advantages of the World Bank approach as reinforcing the fact that people are critical factors in the success of controls, providing documentary evidence for COSO attestation, providing flexibility to accommodate a diversity of business processes, and providing adaptability to changing world and economic environments.

***Centralized CSA*:** Centralized CSA is a method in which the Internal Audit Department or other designated department within an organization performs the CSA workshops and issues reports on the results to the management of the operating units. The operating units do not assume ongoing CSA workshop facilitation duties. As a result, the department responsible for performing the CSA workshops must devote significant resources to maintaining an effective CSA process. Thus, CSA becomes one of the available audit tools while still enabling traditional audit testing of controls in areas of significant risk to be performed. Centralized CSA is perhaps the most common approach since it enables an Internal Audit Department to gradually develop and implement CSA without the shock of attempting full implementation and the risk of complete failure. Another advantage of the centralized CSA approach is that by performing traditional auditing techniques as well as some CSA workshops, the Internal Audit Department can diversify its audit approaches. Diversification enables internal auditors to tailor the approach most appropriate for each operating unit. Centralized CSA is also the most practical in highly regulated and highly risky industries. Pure CSA may not be an option because a certain amount of compliance testing is required by various laws and regulations. Furthermore, relying on the operating unit to fully report on the effectiveness of controls in high-risk processes may not always be wise. For example, neither management nor staff may be aware of how to effectively implement adequate segregation of duties in a particular process. This situation has been seen in several audits of wire transfer departments in various financial institutions. Potential disadvantages of centralized CSA are confusion by operating units over who is responsible for internal controls, inconsistent evaluation of internal controls throughout the organization, and ineffective solutions in areas where CSA was not applied. Because a centralized CSA approach is easier to implement than pure CSA, the degree of audit resources devoted to centralized CSA implementation varies by organization, but it typically falls somewhere between 10 and 50 percent.

Targeted CSA: Targeted CSA is a method in which the Internal Audit Department performs CSA on a limited basis and does not devote a significant number of resources to facilitate CSA workshops. Targeted CSA is an approach that is best applied by organizations that have researched CSA and have reached a point where they are ready to attempt to facilitate a few CSA workshops. Although the success of targeted CSA obviously cannot be expected to be extensive, targeted CSA can be effective if deployed in high-risk areas, usually in conjunction with traditional audit methods. Targeted CSA can also be useful in organizations where acceptance of CSA by management is spotty. If a few innovative managers are willing to try it, internal auditors should take advantage of the opportunity. If they find value in the process, auditors will have a much easier time selling the process to other managers. Almost all firms that are just beginning to implement CSA are essentially at the targeted CSA stage. The advantages of targeted CSA are low cost in terms of resources required, and minimal risk if the process fails.

The disadvantages are reduced effectiveness at identifying opportunities to improve operations, failure by management to see the benefits of CSA, and lack of enthusiasm within the Internal Audit Department due to limited use of the process.

Hybrid CSA: Hybrid CSA is a method in which CSA is applied centrally in some areas of an organization and its pure form in other areas. For example, some organizations have limited audit resources and multiple remote operating units. In these cases, it may be more practical to apply pure CSA to the remote operating units and centralized CSA to common functional areas in the organization such as accounting, data processing, payroll, human resources, accounts payable, or customer service. A hybrid form of CSA may also be necessary if an organization has limited audit resources and operates in a highly regulated industry. I received an inquiry about CSA from an internal auditor of a non-public, multistate holding company with various subsidiaries, each of which comprises an independent operating unit in a different industry. The Internal Audit Department in this private conglomerate had only a handful of auditors to cover a large territory. For this reason, they felt that pure CSA would be very practical in remote operating units. For centralized operations, they planned to perform centralized CSA.

5.31 BENEFITS OF A SUCCESSFUL PROGRAM

The benefits of a successful CSA program are many. They encompass the entire organization, including individual staff members, management, internal and external auditors, and the owners of the organization. Staff members benefit by having their creative ideas for improving operations and controls implemented, or at least considered. They participate in the process of identifying internal control weaknesses and formulating solutions. Thus, they are more likely to take ownership of the solutions since they contributed to their development. This employee empowerment enhances worker morale while helping to improve operational effectiveness. Without CSA, they might believe that their ideas are not valuable, thereby leading to job dissatisfaction and higher turnover. Management benefits by gaining the opportunity to enhance their ability to meet their business objectives with the direct help of their staff. Management has input into the process by identifying the critical business objectives to be addressed by the CSA workshop participants. This can sometimes directly improve their financial incentives. Also, increased employee morale reduces the incidence of employee disgruntlement and the related difficulties of counselling and other disciplinary actions. Management also learns that they are responsible for internal control, not internal auditors.

Internal auditors benefit by being perceived as helping to add value to the organization. This results from the fact that they are consulting with operating units to address the key business objectives of the operating unit. As facilitators, auditors are also able to focus the direction of CSA workshops on the other objectives of internal controls, including the reliability of financial reporting and compliance with laws and regulations, thereby helping to ensure internal control compliance.

Another major benefit to internal auditors is that performing a CSA workshop as one of the early steps in an audit serves as an icebreaker between the staff participants and the

auditors. The participants have an opportunity to see the facilitating auditor in a role other than the traditional auditor who comes into their realm and points out flaws in their processes. Instead, participants interact openly with the auditors in a fun and constructive manner. Then, in cases in which CSA workshops are followed by the performance of audit testing, the participants are much more comfortable working with the auditors.

External auditors can benefit because can observe internal control compliance, which includes the accuracy and reliability of financial reporting. They also could secure contracts to perform CSA workshops. This is particularly important for external auditing firms because their largest market for future growth lies in increased revenues from consulting services such as CSA. Organization owners benefit because many control enhancements arising from CSA workshops pertain to improving operational efficiency and effectiveness. As a result, firms can maximize their profitability and effectiveness, thereby increasing the value of the organization to its owners, whether it is a publicly traded corporation, a governmental entity, or a privately held business.

The beauty of CSA is that it can be applied in IS areas as well as nontechnical operating areas within virtually any organization. It can even be performed in a mid- or upper-level management group. In such cases, if any potentially significant internal control weaknesses are identified during a CSA workshop, auditors can perform "drill-down" CSA workshops on lower levels of the organization about the potential internal control weaknesses. Drilling down can help determine the extent of the potential weaknesses.

Detractors have argued that CSA is nothing more than a quality control process moulded to fit the needs of auditors. Quality control departments in some firms feel as if they need to compete with auditors who perform CSA. Improved quality and service can indeed result from CSA since quality and service may be one of the key business objectives identified by management. However, CSA goes far beyond just quality control in that it can identify ways to address risks within the generally accepted internal control framework models.

For example, CSA can identify ways to increase the accuracy of financial reporting, compliance with laws and regulations, and safeguarding of assets. CSA has been well received by management within organizations that have properly applied it. However, CSA is not a panacea. It must be diligently applied and constantly re-examined to ensure that it is meeting the current needs of the organization. As organizations adapt to changes in their environments, CSA must also adapt to organizational changes.

5.32 BOEING EMPLOYEES' CREDIT UNION METHODOLOGY

The BECU utilizes a centralized CSA approach. The methodology for applying CSA at the BECU is as follows:

- Meet with the management of the process being evaluated to identify the four most important primary business objectives, answer questions about internal controls and CSA, and schedule internal control training classes and CSA workshops.

- Conduct a two-hour internal control training class with six to eight staff members who are going to be present in the CSA workshop. Supervisors, managers, and higher levels of management are encouraged to attend this class.
- Facilitate a half-day CSA workshop with staff members to identify successes and obstacles to the primary business objectives and to identify action plan items for resolving obstacles.
- Summarize results in a management report. The action plan items for operational and control improvement are treated as if they were typical audit recommendations. In other words, management is expected to respond to the CSA recommendations regarding the actions, if any, they expect to take to address the issues identified.
- Track the action plan items to ensure that the agreed-on actions are implemented.

5.33 SELF-ASSESSMENT QUESTIONS

Q.1 Describe information system operations with examples.
Q.2 Explain the main components of computer operations and media distribution with examples.
Q.3 Write a detailed note on the maintenance procedures of information systems.
Q.4 How would you manage internal database balancing and monitoring systems?
Q.5 Critically evaluate the history of control self-assessment.
Q.6 Write a comprehensive note on internal control frameworks.
Q.7 Describe each of the following:
i. Segregation of duties
ii. CoCo
iii. COBIT
iv. Cadbury
v. SAC and Esac
vi. SASs 55/78/94

5.34 ACTIVITIES

Design a framework of information system operations.

5.35 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised; Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research*, *21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly*, *26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal*, *5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, *14*(1), 43.

UNIT-6

ENCRYPTION AND CRYPTOGRAPHY; COMPUTER FORENSICS

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

Encryption is the ultimate means of information asset protection. If properly implemented, encryption will foil almost any attack short of a nationally sponsored effort. This unit discusses encryption and cryptography and its goals, hashing, computer forensics and investigation. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- Encryption and Cryptography
- Goals of cryptography controls
- Hashing and computer forensics

6.1 ENCRYPTION AND CRYPTOGRAPHY

Encryption is the ultimate means of information asset protection. If properly implemented, encryption will foil almost any attack short of a nationally sponsored effort. Encryption can be used to protect any information asset, whether stored on tape or disk, or while in transit on a communications link. Before the 1990s, national governments, government contractors, and private banking systems were the primary users of encryption technology. With the proliferation of the Internet and electronic commerce, however, the need for secure exchanges of electronic information has now also become of significant importance to commercial entities and the consumer public in general. There appears to be global concurrence that cryptography is the strongest means for securing electronic information against theft or compromise. However, cryptography can be both an ally and an adversary of secure electronic information exchange. On one hand, encryption technology can protect information from unauthorized viewing or attack. On the other hand, dishonest or devious persons can employ cryptanalysis techniques to divulge, alter, steal, divert, or otherwise disrupt electronic information exchanges. The following discussion provides a series of references and quotes that help put into perspective the need for the deployment of strong encryption techniques.

In 1997, Ian Goldberg, a University of California-Berkeley graduate student, linked together 250 idle workstations in a manner that enabled him to test 100 billion possible keys per hour. Using this method, he was able to crack RSA Data Security, Inc.'s 40-bit encryption algorithm in three and a half hours. Computer systems in the United States Department of Defense (DOD) may have experienced as many as 250,000 hacker attacks in 1995, according to a report from the United States General Accounting Office (GAO). Such attacks are often successful, granting unknown and unauthorized persons access to highly sensitive information, and they double in number each year due to easier and more widespread use of the Internet and to the increasing sophistication of computer hackers. According to the GAO, the DOD lacks a uniform policy for assessing risks, protecting systems, responding to incidents, or assessing damages. In addition, the training of users and system and network administrators is haphazard and constrained by limited resources. Technical solutions should help, but their success depends on whether the DOD implements them in tandem with better policy and personnel measures.

Dutch computer hackers stole United States military secrets during the Persian Gulf War and offered them to Iraq. The secrets could have altered the course of the war. But the Iraqis allegedly never used the information, fearing a hoax. The Internet has made it possible to assemble massive computing resources to crack a key. In 1994, a 129-digit RSA key was broken through the combined efforts of 1,600 computers around the world. The attack, which was coordinated through e-mail and involved finding the prime factors of the 129-digit number, consumed 5,000 MIPS (Machine Instructions per Second) months over an eight-month interval of real-time.

Hiding behind anonymous keyboards, a group of hackers struggled for two weeks to breach United States military and civilian computer networks. They succeeded beyond

their wildest dreams... The culprits [were] a special United States national security team that was secretly testing the vulnerability of the nation's computer systems using software found on the Internet... [The] hackers gained access to computer systems across the country..., including the United States Pacific Command in Hawaii. [They also] gained access to a United States electric power grid system that they could have sabotaged to plunge the nation into darkness.

In August 1999, an international team of scientists in the Netherlands was able to determine the prime factors of a 512-bit number that models the key in the well-known RSA-155 cryptographic algorithm used extensively in hardware and software to protect electronic data traffic (e.g., the international version of secure sockets layer [SSL]). RSA-155 was designed by three scientists (Ronald Rivest, Adi Shamir, and Leonard Adelman) at the Massachusetts Institute of Technology in the mid-1970s. It has two parts: a sieving step and a matrix reduction step. For the sieving step, about 300 fast SGI Sun workstations and Pentium personal computers (PCs) ran in parallel mostly on nights and weekends and used about 8,000 MIPS for years. For the matrix reduction step, a Cray C916 supercomputer at the SARA Amsterdam Academic Computer Center was used. The total effort took about seven months. However, the scientists said that using a distributed processing effort over the Internet with thousands of participants, it is possible to reduce the factoring time to one week.

This led world-renowned cryptographer Bruce Schneier to recommend using 2,048-bit keys. But even large keys have their downfall. Typical encryption keys consist of 40 to 2,048 bits of random data, which must be stored on a PC's hard drive where everything is filed in a very logical, ordered way. According to Adi Shamir (RSA codesigner) and Nicko van Someren, chunks of randomness stand out, making it easy for malicious programs to locate them. Encryption is arguably the most important aspect of information security. It is a major component in the overall information security infrastructure of any electronic process. Virtually all electronic exchanges of significant data employ the use of some form of encryption. Encryption is vital to the exchange of information about matters of national security, to electronic monetary transactions within all major banking systems, to electronic commerce among merchants and consumers, to electronic data interchange (EDI) among businesses and their customers, and the security of passwords and other confidential information residing in virtually all computing systems.

Proper cryptographic controls can help ensure the confidentiality, integrity, authenticity, and nonrepudiation of electronic messages transmitted or transported between or among various computing systems. Policies, procedures, physical security over devices, logical security controls, and cryptography all play critical roles in the overall information systems (IS) security environment. Without effective cryptographic controls, the other IS controls are simply supporting a weak infrastructure. Noncryptographic controls are much more susceptible to circumvention because they rely on human education and the ability of humans to carry them out. In modern times, cryptography, while relying on humans for the creation and certain aspects of control, is essentially a set of computerized controls, thereby providing the potential for significantly greater speed and reliability

than human-based controls. Therefore, if properly designed and implemented, cryptographic controls can be broken only by another computer. Fortunately, humans must direct computers to break encryption algorithms and other cryptographic controls. The thought of *intelligent* computers independently determining when, how, and which cryptographic controls to crack and divulge to the world is far less appealing than knowing that when a hacking attempt is identified, somewhere in the world at least one human is perpetrating the action. Probably the time will come when computers must be faced as direct adversaries. Because of the importance of cryptography in helping to secure electronic information in virtually all computer systems, a basic understanding of this concept is essential for IS auditors to effectively perform their jobs. The remainder of this chapter provides enough information to effectively understand and assess the adequacy of cryptographic controls that auditors are likely to encounter.

6.2 TERMINOLOGY

The terms *encryption, cryptography, cryptanalysis,* and *cryptology* are often used interchangeably. However, differences in these terms warrant including their definitions so that they can be used in the proper context in discussing this already complex and sometimes confusing subject.

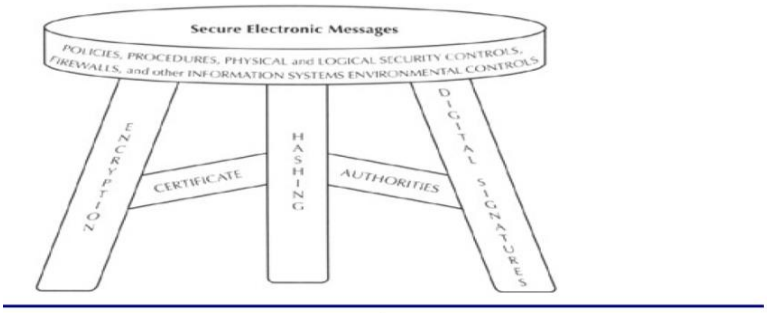
- *Encryption* is the act or process of translating a message into a hidden form using a secret formula, or algorithm.
- *Decryption* is the act or process of translating a hidden message into its original, readable form. Encrypt and decrypt are synonymous with the terms *encipher* and *decipher.*
- An *algorithm* is a step-by-step procedure for solving a problem in a finite number of steps. As applied to encryption, an algorithm is a secret formula used to encrypt and decrypt messages. Each time the formula is employed to encrypt a message, it calculates a unique random secret key, which must be used to decrypt the message.
- *Cryptography* is the art or science of encrypting and decrypting messages using secret keys or codes. Some of the earliest uses of cryptography can be traced back to early civilizations such as the Egyptians around 2000 B.C. The Roman Empire also employed the use of cryptography about 2000 years later. Since then, the need for and use of cryptography has been documented throughout history. With the advent of computers and the need for secure electronic communications, the use of cryptography has spread extensively throughout the world at an ever-increasing rate.
- *Cryptanalysis* is the art or science of deciphering encrypted messages without the benefit of the secret key or code.
- *Cryptology* is the scientific study of both cryptography and cryptanalysis.

6.3 GOAL OF CRYPTOGRAPHIC CONTROLS

The goal of cryptographic controls is to reasonably ensure the confidentiality, integrity, and authenticity of electronic information being transmitted while providing

nonrepudiation by the sender. Encryption, coupled with hashing and digital signatures, has become the most accepted solution to ensure reasonably secure electronic transmissions of information, especially with the need for electronic commerce transactions. Encryption, hashing, and digital signatures can each be thought of as one of three legs supporting a secure electronic message (see Figure 6.1). If any of the legs fails, the message is no longer fully secured.

Figure 6.1: Secure electronic messages



- *Encryption* helps ensure the confidentiality of the information being transmitted.
- *Confidentiality* is achieved when only the intended recipients of transmitted information can read it. Encryption is also used to protect data stored on electronic media such as disk storage devices, magnetic tapes, and diskettes.
- *Hashing* helps ensure message integrity.
- *Integrity* is achieved when the transmitted information has not been altered, other information has not been added to the transmission, and information has not been deleted from the transmission.
- *Digital signatures* help ensure the authenticity of electronic transmissions and help ensure nonrepudiation of the transmissions by their creators.
- *Authenticity* is achieved when the message recipient can be reasonably certain that the message was originated by the entity that appears to have originated it and not by some other unknown entity.
- *Nonrepudiation* is achieved when the sender of a message cannot refute the fact that he or she sent it. The concepts of encryption, hashing, and digital signatures will be discussed in the following sections.

6.4 ENCRYPTION

Within the computing world, encryption algorithms can be classified into two categories: symmetric or asymmetric. *Symmetric algorithms* use the same key for encrypting and decrypting messages. Perhaps the best-known and extensively implemented symmetric algorithm is the Data Encryption Algorithm (DEA), which was adopted as a Federal Information Processing Standard (FIPS) for sensitive but unclassified information by the U.S. government in 1977. This standard is known as the Data Encryption Standard (DES). DES was

developed by IBM under contract with the National Institute of Standards and Technology (NIST), which was formerly known as the National Bureau of Standards. DES utilizes a 56-bit key length. The use of DES by government agencies has led to its general acceptance for commercial encryption. For example, DES is currently deployed by many financial institutions and automated teller machine (ATM) switching services to help ensure secure ATM transactions. In addition, Fedwire, the United States Federal Reserve Bank's wire transfer system, uses DES for transactions among financial institutions.

Advances in technology have eroded the future strength and effectiveness of DES. On June 17, 1997, the DES encryption algorithm was broken by Rocke Verser, a Loveland, Colorado, programmer. He stated, "We have demonstrated that DES can be cracked, and it's not difficult to do it. It means that we need to take a very serious look at how data is encrypted and stored and passed." Verser created a brute-force program that was flexible enough to be downloaded over the Internet and run-on Unix, Windows, Macintosh, and OS/2-based computers. The program was designed to test all the mathematically possible keys for RSA's DES-encoded message. A 56-bit key has over 72 quadrillion possible keys (72,057,594,037,972,936 to be exact). Verser employed the assistance of companies, individuals, and scientists around the world by offering to split the $10,000 prize 60/40 with the operator of the computer that finally identified the winning key. Verser's team, which eventually grew to a network of tens of thousands of volunteer computers, began their cracking effort in February 1997. Utilizing idle computer processing resources from the worldwide network. Verser's team was at times testing nearly 7 billion keys per second and 601 trillion keys per day! The winning computer, a 90-MHz Pentium desktop with 16 megabytes of RAM, was operated by Michael Sanders at Salt Lake City-based iNetZ Corporation. The key was identified after testing about 18 quadrillion keys, or about 25 percent of the possible keys. The winning message read, "Strong cryptography makes the world a safer place."

The cracking of DES was in response to a worldwide "RSA Secret-Key Challenge" sponsored by RSA Data Security, Inc., a wholly owned subsidiary of Security Dynamics, Inc. At its January 1997 Data Security Conference, RSA offered amounts ranging from $1,000 to $10,000 for breaking various RC5 variable-length keys of different maximum sizes and offered $10,000 for breaking the fixed-length 56-bit key DES algorithm. RSA, which was founded in 1982 and is headquartered in Redwood City, California, is named after its founders: Ronald Rivest, Adi Shamir, and Leonard Adelman.

RSA announced "DES Challenge II" on January 13, 1998, at its Data Security Conference in San Francisco. The goal of this challenge was to discover the secret DES key used to encrypt a message in less time than it took Rocke Verser's team to win the original RSA Challenge. The winning team, which consisted of programmers and enthusiasts known as Distributed.Net, solved the challenge in only 39 days. The Distributed.Net team coordinated the efforts of 22,000 participants worldwide, connecting over 50,000 central processing units (CPUs). The winning message read, "Many hands make light work." "The team searched more than 61 quadrillion keys at a peak rate of 26 trillion keys per second. The

winning key was found by a U.S. based machine powered by an Alpha CPU after searching 85 percent of the total possible solutions."

On July 17, 1998, the Electronic Frontier Foundation (EFF) reported that a single computer had been used to defeat the 56-bit DES algorithm. The project, which cost about $220,000, used a computer named "Deep Crack" to break a DES-encrypted message in 56 hours. It used brute force to test about 18 quadrillion possible keys. Deep Crack had a total of 36,864 microprocessors, each of which could test 2.5 million possible keys per second. Since there are at most 72 quadrillion possible keys, Deep Crack could crack any DES-encrypted message in less than 9 days and 1 hour. As a result, every financial institution that has credit, debit, or ATM cards secured with card verification value, card verification code, or data encryption standard offsets must urgently assess its cryptographic security.

Due to the increased processing speeds of computers and their lower cost, DES is reaching the end of its useful life. DES can currently be defeated with the proper knowledge and equipment. The ease with which symmetric algorithms can be defeated is primarily a function of the speed of the computer being used, the key length, and the financial resources available to the hacker. Faster computers can test more possibilities each time. Regarding key length, every additional bit added to the length doubles the number of possible combinations. Since fast computers are usually more expensive than slow ones, the amount of cash available to employ the use of fast computers is a constraint to hackers. One article effectively describes this relationship:

Given current technology, approximately 90 million DES key combinations or 5 million RC4 combinations can be processed per second. The cost of the computer hardware to accomplish this is approximate $50,000–$75,000. In other words, for about $50,000, given current technology, it would take only a second or so to break encryption tied to a key length of 26 bits. It would take approximately one hour to break a key length of 38 bits. A 40-bit key could be broken in about 4 hours, a 48-bit key in about 1 month, and a 56-bit key in 30 years or so. Up the price to about $1 million and DES can be broken in about 10 days. Security tied to a 128-bit encryption algorithm is very secure, given the state of technology today and the expected state of technology for the next 30 years. This quote assumes that only one of a few computers is used. The RSA Secret-Key Challenges demonstrated that multiple internetworked computers working together can reduce these time horizons exponentially.

In 1996, because of these and other technological advances that threaten the security of DES, NIST began the process of selecting a replacement algorithm, to be known as the Advanced Encryption Standard (AES). The goal of NIST is to replace DES with another algorithm that has a 128-bit block size and a key size of 128, 192, or 256 bits. By June of 1998, a total of 15 candidates for the AES were submitted to NIST during round 1 of the selection process. The source code and documentation of all the candidates were openly reviewed by the cryptographic community at large for security, efficiency, and randomness. In March 1999, the candidates were subject to further scrutiny among peers

at the second AES conference held in Rome, Italy. Revisions and enhancements to the candidate algorithms were allowed during round 1. Round 1 culminated in August 1999 with NIST naming the five AES finalists:

1. **MARS**, developed by IBM, is a shared-key symmetric block cypher, supporting 128-bit blocks and variable key sizes. MARS offers better security than triple DES while running significantly faster than single DES. The combination of high security, high speed, and flexibility make MARS an excellent choice for the encryption needs of the information world well into the next century.
2. **RC6**, by Ron Rivest in collaboration with RSA Laboratories, is an evolutionary improvement over RC5 and makes essential use of data-dependent rotations. It offers good security and good performance.
3. **Rijndael**, by Joan Daemen and Vincent Rijmen of Belgium, has variable block and key lengths of 128, 192, or 256 bits. Both block and key lengths can be extended very easily to multiples of 32 bits. Rijndael can be implemented very efficiently on a wide range of processors and hardware.
4. **Serpent,** by Ross Anderson (UK), Eli Biham (Israel), and Lars Knudsen (Norway), is a 128-bit block cypher. It is faster than DES and supports a very efficient bitslice implementation.
5. **Twofish,** by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson, utilizes a 128-bit block and variable key lengths of 128, 192, or 256 bits. It features an efficient key setup on large microprocessors, smart cards, and hardware.

Round 2 ended shortly after the third AES conference, which was held in New York City in April 2000. In October 2000, NIST announced that Rijndael had been selected for the proposed new AES. According to NIST, it showed the best combination of security, performance, efficiency, ease of implementation and flexibility. Rijndael was more versatile and can be implemented efficiently on a wide range of platforms using very simple operations.

The proposed selection of Rijndael as the AES was announced in the *Federal Register* on February 28, 200, and was subjected to a 90-day public comment period. Finally, on December 6, 2001, *Federal Register,* Rijndael was announced by NIST as Federal Information Processing Standard (FIPS) 197, also known as AES. It became effective on May 26, 2002. DES will likely remain the government's standard for less sensitive applications, with AES specified as a standard when the sensitivity of the protected data is higher. If computer processing power continues to increase at the rate of Moore's Law (i.e., doubles every 18 months), AES will likely replace DES in almost all commercial applications. But even AES will not be the panacea of security we might like. Using techniques called "side-channel attacks," even AES-encrypted messages are at risk. These attacks analyze things like the amount of time that cryptographic operations take, power consumption, radiation emissions, and fault analysis to help determine the secret keys. There will never be such a thing as total security.

Asymmetric algorithms require the use of different but mathematically related keys for encrypting and decrypting messages. These keys are commonly referred to as public and

private keys. The public key is provided openly to the public so that entities with which the key creator communicates can send electronic information. The private key is kept secret by the creator of the key. Once a message has been encrypted with one of the keys, only the other key can decrypt it. Also, possession of one key does not enable the holder to determine the other key. Typically, the sender of the message uses the receiver's public key to encrypt a message. Upon receipt, the receiver uses his or her private key to decrypt the message. RSA is a well-known developer of asymmetric algorithms.

Asymmetric algorithms utilize much longer key lengths than symmetric algorithms. To defeat an asymmetric algorithm, one must determine the matching secret key from the public key. In the case of RSA, this is equivalent to factoring a large integer that has two large prime factors. Various mathematical approaches are employed in other cryptosystems. This quote provides a good perspective of the relative security of asymmetric algorithms: For an (asymmetric) RSA cryptosystem, a 256-bit modulus is easily factored by a computer user with average experience and resources. Keys with 384 bits can be broken by university research groups or companies; 512-bit keys are within the reach of major governments. Keys with 768 bits are probably not secure in the long term. Keys with 1,024 bits and more should be secure for several years unless major algorithmic advances are made in factoring; keys of 2,048 bits are considered by many to be secure for decades.

Symmetric or asymmetric encryption algorithms can be defeated in at least two ways. First, the algorithm itself may be weak, or mathematically predictable. For example, in 1995, two first-year graduate students at the University of California-Berkeley, David Wagner and Ian Goldberg (yes, the same Ian Goldberg referred to at the beginning of the chapter) discovered a method to crack the public key encryption scheme deployed within the popular Netscape Navigator World Wide Web browser software. For each encrypted transaction, the software required a new key. To create the key, it needed a starting number, which it generated using the time and date of the transaction and certain information about the user's computer system. All this information is obtainable by a codebreaker, who would then face a greatly reduced task to crack the code. In fact, according to reports, "Goldberg and Wagner could break Netscape code in less than a minute using a simple workstation."

Similarly, Paul Kocher identified the fact that the keys to some encryption systems could be predicted by noting the elapsed time the algorithm required to decrypt a message. Brute-force attacks can also be used to defeat encryption algorithms. *Brute force attacks* employ the use of a computer or computers to systematically test all possible keys until the correct one is identified. The longer the key, the more difficult it becomes to defeat the encryption algorithm in terms of time and money. However, longer keys have operational drawbacks. The longer the key, the more time-consuming and costly it becomes for the intended recipient to decrypt the information. Because many asymmetric cryptosystems have keys that are much longer than keys in most symmetric cryptosystems, they can be many orders of magnitude slower than their symmetric counterparts. One group of authors recently reported that some of the old private key (symmetric) cryptosystems are about 100 times faster than some public key (asymmetric) cryptosystems.

As a result, asymmetric cryptosystems are less practical for encrypting high-volume, real-time, or large information transmissions. For example, most automated teller machine (ATM) networks use symmetric encryption systems such as DES. Some ATMs encrypt just the personal identification number (PIN) as it is being transmitted between the ATM and the host computer at the cardholder's financial institution. Other ATMs encrypt the entire transaction message and the PIN. Computers processing speeds have advanced enough that many new ATMs support triple-DES encryption without significantly affecting transaction speeds. Asymmetric encryption appears to be the generally accepted method of ensuring the confidentiality of most electronic commerce transactions.

6.5 HASHING

The primary purpose of hashing is to help ensure that electronic information is transmitted to a receiver has not been altered, other information has not been added to the transmission, and information has not been deleted from the transmission. This kind of message integrity can be achieved through the deployment of *one-way hash functions.* A one-way hash function is a mathematical formula that uses an electronic message as its input and creates a block of data called a *message digest.* When both an electronic message and a cryptographic key are processed through a one-way hash function, the resulting block of data is called a *message authentication code* (MAC). Two common one-way hashing functions are Message Digest 5 (MD-5) and Secure Hash Algorithm 1 (SHA-1). MD-5 is not considered to be as secure as SHA-1. SHA-1 is currently a United States government Federal Information Processing Standard (FIPS) as well as a standard of the American National Standards Institute (ANSI). One-way hash functions should be designed so that they can be used only to calculate message digests or MACs in a single direction. In other words, someone should not be able to determine the original information from the corresponding message digest or MAC. Another desirable characteristic of one-way hash functions is that they should not generate the same message digest or MAC for different sets of data. Such assurance is achieved by designing hash functions that create lengthy message digests or MACs. The longer the message digest or MAC, the less risk there is of a "hash clash" from two different originating sets of data.

6.6 DIGITAL SIGNATURES AND DIGITAL CERTIFICATES

Digital signatures and digital certificates are used to assure the message recipient that the message is authentic and that it cannot be repudiated by the sender. To digitally sign a message, the sender subjects a message to a one-way hashing function. The resulting message digest is encrypted, using the sender's private key, thereby resulting in a *digital signature.* The digital signature is appended to a message that has been encrypted with the receiver's public key. Before receiving a message from the sender, the receiver must independently obtain a *digital certificate* for the sender. A digital certificate is issued by a trusted *certificate authority* (CA). The digital certificate identifies the sender and contains the sender's public key as well as the digital signature of the trusted CA.

6.7 KEY MANAGEMENT

Symmetric encryption key management is practical for a relatively limited number of communicating pairs wishing to exchange information. For example, most ATM networks that employ symmetric encryption can reasonably manage keys because the number of ATMs with which the host computer must communicate is relatively small (i.e., a few thousand). The encryption keys are usually administered and controlled by a central entity such as a network switching service vendor. Unfortunately, with electronic commerce, key management becomes a much greater challenge. Consider that every individual in the world who utilizes the Internet could be a potential customer of every business in the world, with each business needing to communicate securely with every individual. Also, every business in the world could be a customer of almost every other business in the world. As a result, the number of potentials communicating pairs is staggering.

6.8 COMPUTER FORENSICS

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. Computer forensics -- which is sometimes referred to as *computer forensic science* -- essentially is data recovery with legal compliance guidelines to make the information admissible in legal proceedings. The terms *digital forensics* and *cyber forensics* are often used as synonyms for computer forensics. Digital forensics starts with the collection of information in a way that maintains its integrity. Investigators then analyze the data or system to determine if it was changed, how it was changed and who made the changes. The use of computer forensics isn't always tied to a crime. The forensic process is also used as part of data recovery processes to gather data from a crashed server, failed drive, reformatted operating system (OS) or other situation where a system has unexpectedly stopped working.

In the civil and criminal justice systems, computer forensics helps ensure the integrity of digital evidence presented in court cases. As computers and other data-collecting devices are used more frequently in every aspect of life, digital evidence -- and the forensic process used to collect, preserve, and investigate it -- has become more important in solving crimes and other legal issues. The average person never sees much of the information modern devices collect. For instance, the computers in cars continually collect information on when driver brakes, shifts, and changes speed without the driver being aware. However, this information can prove critical in solving a legal matter or a crime, and computer forensics often plays a role in identifying and preserving that information. Digital evidence isn't just useful in solving digital-world crimes, such as data theft, network breaches and illicit online transactions. It's also used to solve physical-world crimes, such as burglary, assault, hit-and-run accidents, and murder. Businesses often use a multilayered data management, data governance and network security strategy to keep proprietary information secure.

Humanity has become dependent on computers to store and process personal, professional, and business-related information. Even criminals cannot resist the power of

the computer for maintaining records of their illegal activities. Prostitution rings maintain databases of their "Johns"; drug traffickers maintain lists of their primary customers, distributors, and suppliers; and murderers, rapists, stalkers, abusers, and other violent criminals may keep detailed accounts of their obsessive behaviour and other activities. Businesses may produce volumes of data in their systems that describe in detail illegal activities such as discrimination, sexual harassment, environmental pollution or damage, antitrust activities, bribery, extortion, and a host of other legal and regulatory violations. Governmental agencies and military organizations also maintain a wealth of classified and top-secret information about their activities as well as those of other countries. There is more information stored on all the hard drives, disk packs, floppy diskettes, compact disks, and other electronic media in the world that exists on printed matter.

Experts in the field of computer forensics have come to the forefront of many legal battles to assist plaintiffs, defendants, and courts in assimilating these previously hidden facts. *Computer forensics* is the science about the relationship of computer facts and evidence to legal issues. Computer forensic experts can obtain and access computer information and explain it in court using legally accepted methodologies and procedures. These specialists also offer training courses to law enforcement agencies on the proper legal acquisition, handling, and storage of computer evidence. One of the most sophisticated computer forensics companies in the world is New Technologies, Inc. (NTI), which is headquartered in Gresham, Oregon. The organization was founded in 1996 by several internationally recognized technology experts, including Michael R. Anderson, an artificial intelligence and computer forensics expert who spent 27 years performing high-tech criminal investigations and training for U.S. federal law enforcement agencies. Other members of NTI include experts in the areas of forensic computer science, forensic utility and security software development, technology trends, network issues, cryptography, risk analysis, and risk assessment. The firm's services include forensic computer science training and consulting computer security assessments, and expert testimony in computer evidence issues. Fortunately for society, NTI works on the right side of the law, aiding law enforcement while avoiding requests for assistance from drug dealers and other criminals.

6.9 INVESTIGATIONS

Suppose a system administrator (SA) was performing a routine scan of network devices and found that a user had installed an unauthorized software program that is capable of extracting user IDs and passwords from the network and of using brute force to systematically determine most of the passwords. Suppose further that the user signed on to the network using a compromised SA user ID and password and then used the special SA privileges to extract all sorts of confidential information from the organization's network. Would the SA know what to do? Every organization should have an action plan for such discoveries. The action plan should adequately address how to handle computer evidence in such a way that it does not become tainted and include specific procedures on how to create a complete and accurate chain of evidence. The rest of this unit focuses on these questions to help organizations become better prepared to investigate e-crime scenes before they happen.

6.10 Reality check

The just-described scenario is not fiction. A freeware program called LOPHTCRACK (with the number 0, not the letter O), which has been around for several years, can extract the file containing the user IDs and passwords of Windows NT file servers and use brute force to determine many of them, especially the weak ones. The target files on NT operating systems are known as SAM files. Two former employees were recently charged with using LOPHTCRACK to illegally copy the SAM file from Epicor Software Corporation where they were employed and subsequently copying the company's international list of customers. Both individuals later copied the SAM file of a subsequent employer, VP Projects, Inc. Programs like LOPHTCRACK have existed for many years and use the same approach to determine the passwords within other common network operating systems such as Unix.

Some criminals have child pornography on their computers, while others use Internet chat rooms to meet children. Patrick Naughton, a former executive of Seattle-based Infoseek, was arrested by the FBI on September 16, 1999, for violating a 1994 federal law in which it is illegal to travel from one state to another with the intent to have sex with a minor. In this case, Naughton, then 34, travelled from Seattle to Santa Monica with the intent to have a sexual encounter with a minor who turned out to be an undercover FBI agent.

Most of Naughton's e-conversations during his seven months of luring were recorded on his personal laptop computer. Another example of a trusted employee stealing sensitive information took place in 1997 at General Motors (GM). A high-ranking officer who was negotiating an even better position with Volkswagen (VW) in Germany copied an estimated 40,000 pages of CAD (computer-assisted- design) drawings and component specifications. Although GM discovered the theft shortly after the executive started with VW, and GM received an enormous settlement after successful legal action against VW, the event was widely publicized, much to the embarrassment of GM.

These and many other types of e-crimes have become all-too-frequent news headlines. The bottom line is that despite the implementation of various types of logical and physical security controls, it is not a matter of if but when an organization will be hit with an e-crime. As with any disaster, all organizations should be prepared to initiate an investigation that will lead to a conviction or favourable settlement if the damages are significant. Although the legal system is gradually imposing harsher penalties for e-crimes, thus far punishments have been relatively mild and are not a significant deterrent. Complicating matters further is the difficulty in securing convictions. If evidence is mishandled or tainted in even the slightest way, the risk of the defendant being found not guilty increases substantially. So, what should be done after a potential e-crime has been identified? This is where computer forensics comes to the forefront.

6.11 EVIDENCE HANDLING

Fortunately for those seeking legal evidence, information on computers is extremely difficult to eradicate. Joan Feldman, the owner of Computer Forensics, Inc., the Seattle-

based firm that helped investigate the Naughton case, uses the analogy that computers are like tape recorders that are always running. David Julian, data recovery manager of Northwest Computer Support, another Seattle-based company, says that he has recovered data from computers that have been driven over by a car, thrown into a river, and shot with a gun. Even throwing a computer into the ocean would not succeed in destroying the data. Alan Brill, global practice director for computer forensic and high-technology investigation services for Kroll and Associates in New York, reveals that "where a previously used part of a hard drive (called a cluster) is assigned to a new file, whatever space in the cluster not used for new data retains old data. This slack space is invisible to the operating system. And there are files (including swap files, temporary files and buffer files) where information may be stored even if the user never asked the machine to store it." Before beginning the technical analysis of computer data, many steps should be taken to help ensure a successful investigation and prosecution, if needed. The primary concept to keep in mind throughout the investigation is that the chain of evidence must be preserved, otherwise, the success of any prosecution will be jeopardized. Computer forensics experts from Ernst & Young, Admiral plc (UK), and Datum EBS all concur that maintaining the chain of evidence is the "golden rule" for any computer forensics investigation. Care must be taken to ensure that a standardized, well-thought-out approach is applied.

Internal information technology (IT) security professionals play a critical role in identifying crimes and in securing the evidence. However, allowing an untrained IT security professional to perform the technical forensics analysis could taint irreplaceable evidence, which subsequently could not be introduced in court. Walt Manning, director of the Techno-Crime Institute warns, "Being computer literate is not the same as being computer-forensics literate." Even if the internal IT security professional has the skills, the fact that computer forensics analysis could take days, weeks, or even months to complete makes it impractical and unrealistic for that individual to perform the forensics analysis—unless, of course, management chooses to hire a temporary replacement.

Furthermore, the computer forensics analyst will likely be required to testify if the case goes to trial. Again, inexperience in the courtroom can prove disastrous. Then there is the independence issue. An internal investigator testifying in court on behalf of the organization will automatically be presumed to be biased in favour of the organization, thus making the evidence less credible. For these reasons, organizations should seriously consider utilizing an independent forensics expert in cases likely to go to trial.

6.12 INVESTIGATION STEPS RECOMMENDED BY EXPERTS

Computer forensics should not be viewed in a vacuum. It should be part of an organization's overall computer incident response program. Even "regular" hacks may require at least some computer forensics analysis to be performed after the fact. One systems manager described the mistakes he made in a recent intrusion incident in his organization. Based on his battle scars, he compiled a 10-step "recipe for successful

incident handling." Although not specific to computer forensics, this recipe provides useful guidance for those developing or assessing overall computer incident response programs:

- Write a clear, concise statement of scope, intention, and constraints.
- Add computing and network resource descriptions.
- Perform an impact assessment.
- Delegate roles and responsibilities.
- List staff and vendor contact information.
- Spell out incident response actions, notifications, and priorities.
- Identify essential response resources
- Determine incident investigation and documentation requirements.
- Define supporting data needs.
- Continually exercise and maintain the plan.

Mark Bigler, a senior information systems auditor at Pacificorp in Salt Lake City, Utah, provided similar advice. His six-step list includes:

- Develop effective information protection policies and forensics procedures.
- Notify your organization's legal group and possibly law enforcement.
- Maintain a chain of custody for all evidence.
- Prepare detailed reports and work papers.
- Seize the suspect computer.
- Make a mirror image copy of the hard drive.

Bill Betts, a private computer security consultant in Pleasanton, California, detailed 11 steps that should be performed in consecutive order when beginning a computer forensics investigation:

- Gain appropriate authorization to evaluate computing resources.
- Shut down the computer (best to just pull the plug)
- Document the hardware configuration of the system (photographs/video).
- Transport the computer to a secure location.
- Boot the computer from a DOS boot diskette or remove the hard drive and install it in an isolated test computer. This step is very critical and should only be performed by experts.
- Make a bit-stream backup image of the target drive.
- Authenticate data on all storage devices via a hash total.
- Document the system date and time.
- Make a list of key search words.
- Examine free space.
- Examine file slack space.

Mark Morris, an investigator for the Computer Forensics Investigation Service at Admiral plc in the United Kingdom and former detective in the Computer Crime Unit at New Scotland Yard, agrees that performing a bit-stream backup is important. Morris stresses that maintaining an audit trail and comprehensive notes for all activities are

integral steps. "No action taken by the investigator should alter the original data. This is why a bit image copy must be taken of the original hard drive, he says."

6.13 PUTTING IT ALL TOGETHER

Consider taking the following 13 steps in the event of an e-crime. Be prepared in advance for any e-crime. Appoint a base emergency response team (ERT). The ERT should be composed of designated management, IT security professionals (e.g., network system administrators), security staff (in the event of physical intervention), fraud investigation staff, internal audit staff, and human resources staff (if an employee is a perpetrator). The ERT should include senior management in all communications.

1. Identify one or two computer forensics consultants, preferably local, who are available if their highly technical (and time-consuming) skills are necessary. They should prove their expertise in both technical computer forensics analysis and courtroom testimony. Research their current and previous clients. Ensure that there is at least some knowledge transfer to your internal IS security and auditing staff, so they gain valuable experience during the process.
2. Protect the network. This is network administrators' first duty upon discovery of a potential e-crime. Often, they must take immediate and sometimes extreme measures without the luxury of group consultation (e.g., shutting down the entire network if a malicious attack is detected in progress or immediately resetting the passwords of all users if it is discovered the network password files have been copied). By the same token, system administrators must be careful not to jump the gun and alert offenders, thereby providing an opportunity for them to partially or fully destroy or remove critical evidence. As one systems manager put it, "On-the-fly response can lead to careless mistakes, which could be quite painful." In the end, system administrators must make judgment calls.
3. As soon as possible after initial identification (within hours), convene the ERT. The ERT should perform a risk assessment to determine the potential damage that could or did result from the crime, which systems and data storage devices may contain evidence, and the actions that need to be performed by each team member.
4. Open a case file and begin making a physical record of every step taken during the investigation, including the date and time each task was performed, any tools used, the person performing each task, the location, and controls over each piece of evidence, and any other pertinent information. Each ERT member should record his or her activities, and this information should be compiled by a single, designated ERT member to ensure a consistent and complete format.
5. If an employee is suspected of the crime: The Human Resources Department should notify the employee that an investigation is commencing and should place the person on paid administrative leave until it is determined whether he or she appears to have committed a crime. Extreme care should be taken not to invade the employee's privacy.
6. Disconnect the suspect computer from the network as soon as possible. Collect any electronic storage media in the immediate vicinity (e.g., diskettes, CDROMs and CD-RWs, zip-drive cartridges) as well as any potential paper evidence and take it to a designated evidence room, which is locked and accessible only by authorized individuals. Again, take extreme care not to invade the employee's privacy. Going through purses and

other personal belongings could lead to a lawsuit and much larger damages than the e-crime being investigated.

7. Copy remote electronic storage media that may contain evidence (e.g., disk storage devices connected to network file servers located either on-site or in a remote data centre, CD-ROMs stored in a network "jukebox" device) using a suitable forensics tool. This step is where the computer forensics expert should be consulted.
8. Using an appropriate software tool, perform a bit-stream backup of each suspect piece of electronic storage media. Again, the computer forensics consultant should be consulted and probably be the one to perform this step.
9. Evaluate the results of the investigation with the appropriate level of management. Management should decide whether to prosecute the individual. If so, legal counsel should be notified. Appropriate law enforcement officials should also be notified, especially in cases of child pornography or other potentially violent crimes.
10. Close the case file and archive all documents and evidence for a period dictated by the organization's legal counsel.
11. Conduct a case postmortem to evaluate how the overall process was handled and whether any improvements need to be made.

6.14 CONCLUSION

Computer forensics tools are, by themselves, scientific. The proper use of the various computer forensics tools and analysis of the results are both an art and a science. The steps that we as laypersons can perform amount to common sense. Nonetheless, such common-sense steps can mean the difference between a successful prosecution and a perpetrator getting away with an illegal act. It is hoped that readers will use the information in this chapter as a guide to help their organizations develop procedures that will increase the likelihood of convictions of perpetrators of electronic and other crimes.

6.15 SELF-ASSESSMENT QUESTIONS

Q.1 Describe the terms encryption and cryptography with relevant examples.
Q.2 Explain the main goal of cryptographic controls with examples.
Q.3 Discuss computer forensics with suitable examples.
Q.4 Explain each of the following:

- Encryption
- Hashing
- Cryptographic controls

6.16 ACTIVITIES

Design a conceptual model of computer forensics.

6.17 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised; Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research*, *21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly*, *26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal*, *5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, *14*(1), 43.

UNIT-7

OTHER CONTEMPORARY INFORMATION SYSTEMS AUDITING CHALLENGES

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

This unit describes challenges facing information systems auditing, computer-assisted audit techniques, computer virus and software piracy. It also explains electronic commerce, the security description of the internet, the history of the network, and data manipulation. It also describes hacking and graffiti, web spoofing and other misrepresentations. Furthermore, topics on information privacy, commercial availability of personal information, identity theft and fraud, and privacy laws and regulations. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- Information system audit program
- Advantages of audit programs
- Information systems security policies
- Information system security standards
- Information system security guidelines

7.1 INFORMATION SYSTEMS AUDITING CHALLENGES

The body of knowledge that encompasses information systems (IS) auditing is enormous. First, IS auditors must understand how computers work, what risks they present, and how they can best be controlled. The number and types of computers, operating systems, database management systems, and applications, each with its unique idiosyncrasies, are staggering and continually increasing. Information systems auditors must keep current on these new technologies. Also included in the IS auditing body of knowledge are laws and regulations about the countries and industries in which organizations do business. Information systems auditors must also be fluent in traditional auditing methodologies, which have evolved from the auditing branch of the accounting profession.

Knowledge of accounting principles is also extremely beneficial when examining expenditures for computer equipment and services and how they are recorded on financial statements. A detailed understanding of business operations and high-level management issues such as strategic planning and forecasting is essential for IS auditors to communicate IS control and security issues with executives and board members. Depending on each auditor's area of speciality, additional bodies of knowledge may be encompassed. Finally, auditors must be able to apply this knowledge and information by effectively communicating in written and verbal form. Delving into detail on the entire body of knowledge related to IS auditing is beyond the scope of this book. However, several IS auditing topics were not discussed in other chapters but are important enough to discuss briefly here. These topics include computer-assisted audit techniques, computer viruses, software piracy, electronic commerce, Internet security, and information privacy.

7.2 COMPUTER-ASSISTED AUDIT TECHNIQUES

Internal and external auditors of many organizations and firms have developed and implemented computer-assisted audit techniques (CAATs) that have greatly increased the efficiency and effectiveness of their audits. Using CAATs, the productivity and value of their audits and consulting services to their clients have also increased. A CAAT can be defined as any computer program or application that has been used to enhance the efficiency and effectiveness of an audit process through the automation of previously manual procedures, expansion of the scope of audit coverage, or the creation of new audit procedures. The most powerful CAATs are the ones that independently search databases for information that could indicate the existence of significant or material control weaknesses or operational inefficiencies.

Examples of tools that provide the ability for auditors to perform these types of CAATs include report-writing applications that accompany many vendor information systems; off-the-shelf databases, spreadsheets, and data analysis applications; and data warehouses. The keys to the successful deployment of these CAATs are the integrity and reliability of the data on which the CAATs are dependent, the independence of the method in which the data was obtained, and the timeliness with which the data is

available. Report-writing applications or modules that accompany vendor information systems have the advantage of extracting the desired data directly from production databases. Production data is not subject to the risk of data loss or corruption that could occur when production data is downloaded or extracted to another computer system for subsequent querying by a third-party application. By having the ability to create reports directly from the production database, auditors do not have to rely on data owners or other areas to run download or extract jobs and are thus able to maximize their independence. Also, the production data is available for report writers immediately upon completion of spooling, and the report writer programs can be run at any time after spooling.

Download and extract programs must frequently wait until all production jobs are completed before they are processed. Vendor report-writing applications have their drawbacks, however. For example, obtaining access to the ability to perform vendor report writing on the production database may prove to be difficult. In some systems, report writers can bog down the production system if they require heavy processing, as in the case of numerous calculations or large history searches, or if many report writers are running concurrently. As a result, data owners may be reluctant to grant report-writing ability to anyone outside their areas. Also, some vendor report-writing applications may require specialized training to use them efficiently and effectively.

To use an off-the-shelf database (e.g., Access), spreadsheet (e.g., Excel), or data analysis applications (e.g., ACL, IDEA, Monarch), the data must first be downloaded from the production database. This requires the data owner to authorize the development of a report writer or program to extract the desired pool of data. If the desired pool of data is relatively small, the data owner can create a report writer to extract the data. The report output can then be electronically downloaded to the auditor's workstation or network were a database, spreadsheet, or data analysis application can be used to perform multiple queries. If the desired pool of data is relatively large, it may be more efficient to work with the programming and/or systems development departments to design an extract program that generates a database on which multiple queries can be performed. Either method reduces the independence of the auditor, but data integrity can be reasonably assured through proper systems development and change control procedures. Where possible, procedures in the audit department should require that the extracted data be balanced with the production database. Otherwise, audit results may not be as complete and accurate as expected. In some cases, data analysis applications can be configured to interrogate the production database, thereby eliminating the need to balance it. However, data owner approval must be acquired, and care must be taken to ensure that queries do not impact production application performance. Once the data has been downloaded, the extracted database has been created, or production database access has been established, auditors can perform multiple queries using their database, spreadsheet, or data analysis applications, without affecting the performance of production central processing units (CPUs). This significantly enhances the efficiency of the computer operations area and the auditors. Keep in mind that third-party databases,

spreadsheets, or extract applications are only practical when auditors are going to be performing multiple queries. If only one query is required one time, then it would probably be more efficient to request a single report from the data owner.

Data warehouses (e.g., Sagent) are large databases that provide users, including auditors, the ability to access information from two or more different systems. They eliminate the need to have separate report writers or extract programs for each production system and enable an analysis of entire customer relationships in one location using client software that is part of the suite of data warehouse application software. Information systems auditors can develop countless ways to interrogate a data warehouse for potential internal control weaknesses. Risks associated with data warehouses include incomplete or inaccurate data, unauthorized or excessive data access, high cost, and inability to gain authorization to include all data in the data warehouse. As with report writers and extract programs, procedures should be in place for the data warehouse owner to balance the data within the data warehouse to its source systems to ensure that all applicable production data has been completely and accurately downloaded. Data warehouse system security administrators should also restrict access to data based on management authorization. Data warehouse technology can be very expensive, so IS management should perform an extensive needs analysis before initiating a data warehouse project. Senior management support is crucial to ensuring that access to all necessary data is granted so that a complete data warehouse can be created.

As new technologies are created, auditors should continue to challenge themselves to develop new and innovative audit approaches and techniques that will further enhance their efficiency and effectiveness. Literally, millions of CAATs are deployed in the audit workplaces of the world.

7.3 COMPUTER VIRUSES

With the proliferation of the Internet and other public and private networking technologies, the risk of an organization's personal computers becoming infected with a virus is significant. It is not a matter of whether the computers will become infected, but when and to what degree. Every day malicious programmers are creating new viruses. Some viruses are no more than nuisances, while others have the capability of wiping out data and causing computer operating systems to fail. The most damaging viruses and worms in terms of economic impact in recent years according to *Computer Economics* (*www.computereconomics.com*) were "Code Red" (2001), $2.62 billion; "SirCam" (2001), $1.15 billion; "Nimda" (2001), $635 million; "I Love You" (2000), $8.75 billion; "Melissa" (1999), $1.10 billion; and "Worm.Expore.Zip" (1999), $1.02 billion. Other less damaging but well-known viruses and worms include "Goner" (2001), "Anna Kournikova" (2001), "Chernobyl" (1999), and "Bubbleboy" (1999). The risks of viruses include these costs:

- Recovering lost data

- Eradicating viruses that have infected workstations, network file servers, mainframes, diskettes, CDs, and other storage media.
- Purchasing, installing and maintaining virus detection and prevention software
- Educating users on the risks of viruses, how to test for viruses, and what to do and whom to contact when a virus is detected.
- Developing and maintaining policies on virus prevention
- Reduced data processing system efficiency, or complete loss of use of a system
- Adverse publicity
- Incorrect operational, financial, and other reports
- Unauthorized access to existing as well as other systems

According to the Computer Security Institute (CSI), a virus is a computer program that could reproduce by modifying other programs to include a copy of itself. Such programs may execute immediately or wait for a preprogrammed set of circumstances. The CSI goes on to define other related threats, including bacteria, logic bombs, Trojan horses, worms, password catchers, repeat dialers, trapdoors, and war dialers.

- *Bacteria* are programs designed to reproduce exponentially until the host central processing unit (CPU) runs out of processing capacity, memory, or storage space, thereby denying service to any other users or processes. Bacteria programs do not damage other programs.

- *Logic bombs* are programs that act upon the occurrence of a certain event, such as the passing of a date or the failure of its creator to reset a special counter. When the event occurs, the "bomb" is triggered and the program performs some malicious commands, such as reformatting the hard drive of a server or shutting down a host computer.

- *Trojan horses* are programs that look and perform certain functions innocently but contain malicious code such as viruses, bacteria, and logic bombs. The innocent part of the Trojan horse program may execute routinely for the user but may be performing malicious tasks concurrently or later.

- *Worms* are programs that search for and execute themselves in available host CPU processing memory and then continuously copy themselves to other computers, usually resulting in a denial of service to other users.

- *Password catchers, repeat dialers, trapdoors,* and *war dialers* are technically not virus-like programs that can infect computer systems. However, they can be used to exploit or create security weaknesses and are therefore worthy of one's awareness and further research. Viruses operate in a variety of ways, depending on how the creator programmed them. Roxanne Mashburn, director of the Information Technologies Group for the Eccles Institute of Human Genetics at the University of Utah, provided these descriptions of the various types of viruses:

- *Memory resident.* This type of virus stays in memory after being loaded with its host program.

- *Nonmemory resident.* This type of virus is erased from memory after the host program closes.

- *Stealth.* This type of virus can hide from antivirus scanners.

- *Encrypting.* This type of virus encrypts itself to avoid detection.

- *Polymorphic.* This type of virus mutates by altering its signature. It is the most difficult type of virus to detect.

- *Triggered event.* This type of virus is triggered by a certain event, date, time, sequence of keystrokes, or another set of circumstances.

Most virus-scanning software programs on the market today enable users to peruse the list of viruses in their inventories. These virus lists usually provide brief descriptions of how each virus works, the history of when each was first encountered, and how each can be eradicated. Some older examples include:

- *Gulf War Virus.* This virus was imported by an officer who brought some computer games to the U.S. Gulf War headquarters in Saudi Arabia. It may have wiped out as many as half of all the chemical weapons logs maintained by the U.S. military. Incidentally, physical diskettes containing another quarter of the chemical weapon's logs were lost from a safe at Aberdeen Proving Ground in Maryland and during shipment to the U.S. Central Command headquarters in Florida.

- *PKZIP300.ZIP*. This virus will wipe out a hard disk and disrupt modems that operate at 14.4 kilobytes per second and faster. PKZIP300.ZIP is reportedly very difficult to eradicate. The name of this virus is intentionally similar to the genuine PKZIP and PKUNZIP file compression software written by PCWare.
- *Jerusalem.* This was the first memory resident virus. While loaded, it infects or deletes

*.COM and *.EXE executable files, except for the COMMAND.COM file. It was first identified at Hebrew University in Jerusalem in 1987 and was to trigger on Friday, May 13, 1988, the 40th anniversary of the last day of existence of an independent Palestinian state. Later strains become active primarily on Friday the 13th but can also be active on other days, slowing systems down after each infection.

- *Michelangelo.* First appearing in 1991, this virus reformats hard drives every March 6, Michelangelo's birthday.

- *Stoned.* This virus originated in early 1988 and became prolific in 1991. Early strains did nothing more than create a message on boot-up that the PC was "stoned" and to "legalize marijuana." Later strains reformatted hard drives and may have been the culprit in the Gulf War Virus previously discussed.

7.4 SOFTWARE PIRACY

Software piracy is the act of copying a copyrighted software program for personal use or for resale to another party, thereby denying the rightful owner royalties and any other legal benefits to which they would otherwise be entitled. In its 1991 Worldwide Report, the Business Software Alliance (BSA) reported that the annual cost of software theft worldwide ranged from $10 billion to $12 billion. The Institute of Internal Auditors (IIA) reported that an independent study commissioned by BSA and the Software and Information Industry Association (SIIA) found that, in 1996, the cost of software piracy worldwide was estimated at $11.2 billion. The study also found that about half of all new software applications used in 1996 were pirated. More recently, BSA says the total dollar losses from software piracy have trended down from $ 12.2 billion in 1999 to $ 11.8 billion in 2000, to $11 billion in 2001. But BSA estimated that 40 percent of all new software installed in businesses in 2001 was obtained from the black market. These reductions are due to increased successes in prosecutions and settlement, sting operations, and changes in domestic laws such as the U.S. Digital Millennium Copyright Act (DMCA), which was signed into law on October 28. 1998, and successes in getting foreign governments to crack down on piracy. Because of these heavy losses, software industry trade groups have been formed in numerous countries, including Australia, Argentina, Belgium, Brazil, Canada, Chile, Columbia, the Czech Republic, Denmark, Ecuador, Egypt, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Israel, Italy, Japan, Korea, Luxembourg, Malaysia, Mexico, the Netherlands, New Zealand, Norway, the Philippines, Portugal, Peru, Puerto Rico, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, the United Arab Emirates, the United Kingdom, the United States, and Venezuela. The trade groups in these countries are trying to control the theft of software revenues. To help mount a united international effort to protect software copyrights, the BSA was established in 1988. Headquartered in Washington, D.C., the BSA works with government officials and national industry groups to achieve its international mission, which is to advance free and open world trade for legitimate business software by advocating strong intellectual property protection for software, increasing public awareness of the legal protection of software, and acting against unauthorized software copying in all forms. The risks to organizations that promote or tolerate software copyright infringement include financial penalties and fines, loss of reputation due to negative publicity, and other legal remedies. In addition, software companies lose much-needed revenues, governments lose tax revenues, and communities suffer from increased drug and related criminal activities fueled in part by illegal software sales. Officers and directors of organizations, as well as the individuals who performed software copyright violations, can all be held criminally accountable. In the United States, individuals convicted of criminal copyright violations can be fined up to $250,000 and face up to five years in jail. Civil lawsuits can result in

the payment of actual damages (including the infringer's profits) and statutory damages up to $150,000 per infringement. In addition, pirated software can expose an organization to viruses, improperly performing software, inadequate documentation, lack of technical support, and lack of software upgrades. Recent busts have resulted in the confiscation and prosecution of perpetrators who caused millions of dollars in lost revenues. For example, $5 million worth of pirated software was confiscated in Vancouver, British Columbia, in 2002; $100 million of illegal software in Los Angeles in 2001; $60 million in illegal software in Dallas in 2001; $2.5 million was paid in restitution by 159 firms worldwide in 2001; and $56 million in counterfeit software in California in 1999.

In China, where 94 per cent of all software was pirated in 2000, the government has been assisting Microsoft in piracy prevention efforts. In June 1997, BSA collaborated with the Filipino National Bureau of Investigation and raided three Filipino computer companies and prosecuted two people for selling pirated software. The value of the software was approximately $2 million. The. The Philippines is considered a "hotbed" of piracy, with only 8 percent of software legally purchased. To avoid these risks, BSA recommends that all organizations implement these recommendations for responsible software use:

- Senior management should circulate to all new and current employees a notice stating that it is illegal and against company policy to make or use unauthorized software copies. Such notice should be communicated to users via a banner page that appears during sign-on. Furthermore, if an organization has a new employee training program, software copyright violations should be incorporated into the curriculum. Users should be informed that the organization is allowed to make only one backup copy of the software and that the number of concurrent users allowed by network versions of software is specified in the organization's software license.

- Conduct periodic audits of all PCs and file servers so that a record of software programs installed on each machine is created. Any illegal software copies should be deleted.

- Information system auditors should confirm that system security administrators are performing these audits at least annually. In the United States, SIIA provides automated tools to help inventory software. Be cognizant of the fact that automated tools may not identify all software products on a particular device. The reason is that sophisticated users may disguise executable files to make detection difficult. Performing regular audits will alert users to the fact that the company does not tolerate illegal software. As a result, these audits will act as a deterrent and reduce the incidence of illegal software.

- Maintain a current software inventory system to record the purchase of software. Access to installation diskettes should be restricted to authorized personnel. Furthermore, centralized purchase authorization and installation can control the degree of software piracy immensely.

- Make a requisition form available to all employees so that they may submit requests for new software to their managers.

Other new control technologies are being developed to help thwart some piracy of articles and pictures on the Internet. For example, *Playboy* magazine has recently adopted Digimarc™ digital watermarks to help prevent copyright infringements of photographic images located on its website. These watermarks will be randomly embedded into some copyrighted images. To locate watermarked images downloaded by unauthorized users, *Playboy* technicians use a special software application called MarcSpider, which crawls the World Wide Web, looking at hundreds of millions of objects, in search of any that have a Digimarc watermark. The Internet addresses of identified images are recorded for follow-up investigations by *Playboy* technicians. As new and better controls are developed, and as international cooperation continues to progress so that copyright violators are sternly prosecuted, the incidence and risk of copyright violations can be reduced to reasonable levels.

7.5 ELECTRONIC COMMERCE

Electronic commerce is the process whereby goods and services are purchased through some electronic medium. Electronic commerce is becoming the desired transaction method for many businesses. It is relatively inexpensive to administer as compared to cash, check, and verbal transactions because it requires very little human labour. Many people enjoy the convenience of being able to purchase goods and services via their PCs at home or work. The primary drawback to this transaction method has been the risk of consumers having their credit card numbers, checking account numbers, and other personal information stolen or intercepted during an electronic commerce transaction and used for unauthorized purchases, especially for transactions conducted through the Internet. As a result, many potential customers are uncomfortable sending their credit card numbers and other information across the Internet or any other open electronic network. While the growth in the number and amounts of electronic commerce transactions has been rapid in our technology-hungry society, the general acceptance of this transaction method has been much slower than expected. Encryption technologies have significantly increased the security of electronic transactions and are a critical aspect of electronic commerce. Several electronic commerce security technologies are described next.

VISA International and MasterCard International, which jointly have nearly 1 billion credit and debit cards in circulation worldwide, have been collaborating to develop a single technical standard for safeguarding payment card purchases made over open networks since February 1, 1996. The standard is called SET (secure electronic transaction) and is an open industry standard intended to provide financial institutions, merchants, and vendors with a reasonably secure solution to enable trusted electronic commerce to flourish. Secure Electronic Transaction relies on specially designed public key cryptography and digital certificate controls and was jointly developed in partnership with seven technology companies: GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, and VeriSign. On May 13, 1997, VISA and MasterCard announced that they

had contracted with CertCo and SPYRUS to provide the root certificate authority (CA) system for SET. CertCo is a leader in enabling trustworthy electronic commerce while SPYRUS is a leading provider of secure hardware cryptographic solutions. The segregation of duties enabled by a joint root CA control process provides added security, flexibility, and economy. According to the CertCo chairman:

The security of the entire SET system depends on the protection of the SET root private key. To guard that key in a single site would require lavishly expensive physical controls and heavy armouring. By splitting and distributing the root's private key fragments among independent parties, the CertCo/SPYRUS system substantially increases SET security. By making the system stronger, SET security was improved, and operating costs were reduced. VISA's website also quoted the SPYRUS CEO as stating "The deployment of the SET Root CA provides a top-level point of trust for secure credit card payments and provides the missing element necessary to jump-start electronic commerce." The number three and four credit/debit card issuers in the world, American Express and JCB Company Limited of Japan, also have both endorsed the SET standard and the selection of CertCo and SPYRUS as root CA providers. Despite the progress of SET, its commercial implementation has been slow. But there is still an urgent need for SET, as evidenced by the arrest of a 36-year-old hacker who stole over 100,000 credit card numbers online. For more information on the history of the development of SET, visit the website of VISA International at *www.visa.com* and the website of MasterCard International at *www.mastercard.com*. Secure sockets layer (SSL) technology is by far the most common control used to secure electronic transactions over the Internet (see the Chapter 8 section on remote access controls for a brief description of SSL). Although adequate in many cases, SSL does not afford the same strength of security as SET. In the interim, other technologies have been developed that significantly reduce the risk of personal information being divulged while still providing consumers with the ability to conduct electronic commerce. For example, electronic wallets and purses enable consumers to securely purchase products from retailers. One such new technology is called CyberCash Wallet.™ In 1997 two credit unions began offering CyberCash Wallet service to their members in conjunction with the systems developer, Digital Insight of Camarillo, California.

Initially, credit union members load their electronic "wallets" by initiating an automated clearing house (ACH) transaction, which sends funds from their financial institution to CyberCash. CyberCash holds the funds until purchases are authorized, and then CyberCash sends the funds to the merchant's bank accounts. This service limits purchases only to those merchants who accept CyberCash, but the developers hope to enlist many merchants, thereby making CyberCash a commonly accepted electronic commerce medium. Smart cards, e-cash, and prepaid debit cards are other types of secure electronic commerce services that are emerging. Europay, VISA, MasterCard, and other major credit and debit card issuers are planning to migrate from magnetic strip-based cards to "smart cards" that have microprocessors with mini-operating systems embedded in the plastic. These microprocessors enable a much greater degree of security than is possible with magnetic strip cards. E-cash enables consumers to exchange funds with other

individuals as well as retailers. This is different from electronic wallet services, which only allow the exchange of funds between individuals and retailers. Prepaid debit cards are also limited to acceptance by retailers. These cards are issued in limited-value increments and can be discarded once the issued amounts have been used. As with any computerized process, complete electronic commerce security is impossible. There will always be a way for criminals to perform unauthorized transactions. So long as consumers are protected and electronic commerce losses can be effectively controlled, however, the economic benefits of electronic commerce to businesses and other organizations throughout the world will far outweigh the costs. Electronic commerce will continue to grow as a standard method of purchasing goods and services for most people.

7.6 INTERNET SECURITY DESCRIPTION OF THE INTERNET

The Internet is a global wide-area network (WAN) consisting of millions of host computers that enable millions of local- and wide-area networks, mainframes, workstations, and personal computers located within governments, businesses, research agencies, educational institutions, and individual homes to share information utilizing various Internet services. The Internet provides a wide variety of benefits to individual users as well as organizations. These benefits include the rapid sharing, dissemination, and exchange of information and news as well as high-impact, low-cost marketing of products and services. Computers communicating on the Internet can have any type of operating system, so long as it supports the transmission control protocol/Internet protocol (TCP/IP), which enables computers with different kinds of operating systems to communicate among themselves. (TCP/IP is explained further in the History section.) Some common Internet services include:

Electronic mail (e-mail) is a low-cost mode of communication that enables users to send and receive messages. Various types of data files can be attached to e-mail messages so users can access them. E-mail is perhaps the most popular Internet service. The main benefit of e-mail is that it enables people to communicate personal as well as business issues with anyone on the Internet, anywhere in the world, at little or no cost, any time. E-mail is easier than writing a letter by hand, addressing the envelope, buying a stamp, and mailing it. Delivery of e-mail is also much faster than conventional mail. On the negative side, e-mail is less personal and, as is the case with any Internet communications, the authenticity of messages can be brought into question if not adequately secured.

- *Telnet* is an Internet service that enables one to connect to another computer on the Internet and then use it as if one was directly connected to that computer. Remote access to computers via Telnet can be restricted via system access controls, but it is still a fairly risky service to make available to most users within an organization.

- *Gopher* is a hierarchical text database developed at the University of Minnesota and named after the university's mascot. Gopher provides interconnected links between files residing on different computers on the Internet such that they appear as directories of files on the operator's computer. It is an efficient organizer of information on related topics.

- *Usenet* is an electronic bulletin board type of news service. News groups have various articles and messages posted for public reference. As a result, Usenet can be an excellent information resource.

- *File transfer protocol (FTP)* is a file manager application for the Internet that provides the ability to upload and download data files of various formats (e.g., ASCII, EBCDIC, binary) to and from other computers. File transfer protocol has drag-and-drop functionality.

- *World Wide Web (WWW)* is another highly popular service that enables users to access and exchange various types of information located on computers anywhere in the world.

The World Wide Web was created in 1989 by researchers at CERN (the European Laboratory for Particle Physics) in Geneva, Switzerland, to facilitate the exchange of information among widely dispersed sites. Today, the World Wide Web uses hypertext transfer protocol (HTTP) to enable users to access text, graphics, multimedia such as sound and video, and information databases. Within World Wide Web documents, hypertext enables instant linking to other locations within the same document and computer, and within other documents and computers anywhere on the Internet. Hypertext markup language (HTML) is used to format documents so that they can be properly displayed through the World Wide Web. Browser software applications make it simple for users to access the wealth of information sites available on the Internet. These sites are called websites. Each website has a unique "address" called a uniform or universal resource locator (URL). The format of a URL is typical as follows: http://www.entity-name.ext. The name of the entity is usually the name of the organization, while the letters "ext" refers to the type of organization. The World Wide Web originally had six types of extensions:

1. .com—commercial sites
2. .org—sites of nonprofit and other organizations
3. .gov—government sites
4. .edu—educational sites
5. .mil—military sites
6. .net—Internet service provider sites

In October 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was formed by a broad coalition of the Internet's business, technical, academic, and user communities. The ICANN is a technical coordination body for the Internet. It assumed official responsibility for a set of technical functions previously performed under a U.S.

government contract by Network Solutions, Inc., and other groups. Specifically, ICANN coordinates the assignment of three identifiers that must be globally unique for the Internet to function:

- Internet domain names
- IP address numbers
- Protocol parameter and port numbers

In addition, ICANN coordinates the stable operation of the Internet's root server system. As a non-profit, private-sector corporation, ICANN is dedicated to preserving the operational stability of the Internet; promoting competition; achieving broad representation of global Internet communities; and developing policy through private-sector, bottom-up, consensus-based means. In November 2000, ICANN approved seven new extensions:

1. .name
2. .biz
3. .info
4. .museum
5. .pro
6. .coop
7. .aero

Websites can contain a wealth of information about organizations. Most organizations have created Internet websites to provide information to interested parties, solicit information by taking advantage of the interactive nature of the Internet, and perform a variety of transactions. Websites are also a low-cost, high-impact marketing medium through which organizations can promote their products and services as well as describe their mission, officers, locations, communication channels, and virtually any other public disclosure information, 24 hours a day, seven days a week. Websites provide a level competitive playing field for all organizations, regardless of size. Even the smallest of organizations can have very impressive websites that outshine those of large corporations. Consumers and potential customers find it highly desirable and efficient to visit websites to perform transactions and obtain information when it is convenient for them. Previously, consumers had to telephone an organization during business hours, explain what transactions or information they wanted, and then wait for the transaction to be completed or the information to be mailed or faxed. Through websites, consumers can quickly perform transactions or obtain much of this same information. Organizations can also request information from visitors to their websites. For example, new business opportunities can be solicited, and prospective employees can be recruited. Many commercial and non-commercial websites also provide articles, references, and other highly useful pieces of information.

7.7 HISTORY OF NETWORK

In the mid-1960s, the U.S. Department of Defense Advanced Research Projects Agency (DARPA) created an experimental network that allowed remote research and development sites to exchange information without regard to the type of computer being used. The network became known as ARPANET. Reliability was the key so that the network would remain functional even if part of the network was damaged, as in the case of military strikes and various disasters. The ARPANET was also designed to allow new computers to be added to the network and old ones to be removed without impacting the network. One of the most important developments from ARPANET research was the creation of TCP/IP, which enables different kinds of computers to communicate among themselves and is now the computer communications protocol of today's Internet. During the 1970s, the U.S. government began encouraging educational institutions and libraries to take advantage of ARPANET. In 1983, ARPANET became the backbone computer network to which all other TCP/IP computer networks were physically connected, thereby spawning the Internet. The National Science Foundation (NSF) funded and managed the Internet backbone until 1995, at which time corporations and private foundations began managing the Internet. The Internet Engineering Task Force (*www.ietf.org*), which is a group of scientists and other technical experts, provides support on technical issues related to the Internet. The Internet Society (*www.isoc.org*), a not-for-profit organization, guides the general direction of the Internet by establishing standards and allocating certain resources.

7.8 RISKS

Although the Internet is a huge global WAN, many of the risks associated with it are not much different from those risks faced by any computer system. The Internet has spawned an enormous number of variations of traditional IS security risks due to its open nature and the number of different hosts that data may pass through before reaching its destination. The Internet is also relatively risky since the development of controls to protect against Internet risks is belated. This is because the Internet was originally designed to encourage widespread information sharing among researchers and educators rather than to restrict information sharing. Further complicating the situation is the fact that current legal penalties for committing crimes on the Internet are relatively mild compared to other white-collar crimes. Some of the major risks associated with the Internet are discussed next.

7.9 DATA INTERCEPTION OR MANIPULATION

When information is transmitted through the Internet, the data is transformed into data packets, which are sequentially organized and tagged with identifying information. Upon reaching their destination, the data packets are pieced back together in their original order. The risk during this process is that the message can be intercepted and analysed using data packet "sniffing" devices and programs. The data can also be altered, lost, diverted, or replaced with bogus data. These techniques are used in cases of electronic

espionage in which highly sensitive and confidential information is being transmitted among key executives and high-ranking officials. These risks are also contributing to the slower-than-desired growth of electronic commerce. Many organizations have internal internets known as intranets. Data interception or manipulation can be as risky while data is being transmitted within an organization via its intranet as it is while being transmitted outside an organization. Controls to help reduce the risk of data interception or manipulation include dedicated communication channels, and secure sockets layer (SSL) technology. SSL is a protocol used in modern web browsers to establish relatively secure communications between two computers on the Internet. It encrypts all information in both the HTTP request and the HTTP response, including the URL.

7.10 UNAUTHORIZED ACCESS, HACKING, AND GRAFFITI

These risks pertain to the viewing, alteration, replacement, deletion, or other damage to sensitive information while it is residing on an organization's file servers and other computers. Hackers are notorious for taking over complete systems for their benefit. Malicious internal users and external parties, including corporate and political spies, can also use hacking techniques to gain unauthorized access to sensitive information. Sometimes hackers limit their activities to website damage or graffiti, as was the case when the U.S. Department of Justice's web page was changed to the "Department of Injustice." In other cases, hackers can expose innocent consumers to financial risks. For example, in April 1996, more than 10,000 credit card account numbers, names, and expiration dates were somehow obtained from First Bank in Minnesota and copied to an Internet service provider file server, where they were available on the World Wide Web. The bank contended that the numbers were randomly generated. However, all the numbers were affiliated with Northwest Airlines, which is headquartered in Minneapolis. The bank immediately cancelled all the card numbers after the problem was publicized on the local news. The method by which the numbers were obtained has not been determined. After these early defacements and hacks, similar breaches have become commonplace.

7.11 OVERVIEW OF HACKING

Internet websites are simply programs and data files that reside on domain file servers. Internet domain file servers are file servers which communicate directly on the Internet, as opposed to private file servers, which are not able to communicate outside the organization. Every organization with a presence on the Internet either has connected one or more of its domain servers or has paid a service organization to connect and maintain a domain server on its behalf. Each domain server on the Internet is technically identified by a sequence of four numbers, called octets, separated by periods. In general, these octets are numbered from 0 to 255 (e.g., 123.255.0.211). These Internet protocols "addresses" are issued by domain name registration services. Organizations can register multiple sites, so long as they pay the nominal annual fees. Internet protocol addresses are of interest to Internet technical support personnel as well as hackers and their

gregarious associates, who may have less than noble intentions. Obtaining an Internet protocol address is usually the first step in the hacking process.

A domain server address can be obtained in several ways. Some organizations may willingly divulge the Internet address of their domain server, although most prefer to just give the World Wide Web alpha-numeric address (i.e., their URL). One can also sign on to the website of an Internet domain name registration service and perform an inquiry. For example, sign on to the website of any Internet registration service and perform a "who is" search on any name. The search results will list all the domain names registered to organizations with a name matching the word or words you entered. For each domain name, the search result will include the mailing or street address of the organization, the domain name (i.e., alpha-numeric website name), the administrative contact's name and phone number or e-mail address, the domain server names and Internet protocol addresses, and other information.

A third way to obtain Internet protocol addresses is by using special programs. PING is one such program that is widely available on the Internet. If the World Wide Web address of a particular organization is known, PING can be used to retrieve the numeric Internet protocol address. Armed with other special programs, hackers can begin to probe the Internet protocol addresses of the identified domain servers for weaknesses and vulnerabilities. Examples of free Internet and network vulnerability analysis tools include CIS (Cerberus Internet Scanner), Nessus, Nmap, Nmap, SAINT (Security Administrators' Integrated Network Tool, version 3.2.1 or earlier), Whisker, and WinfingerPrint. As with any freeware, there are risks that the software may be buggy or may not have all the reporting bells and whistles provided in other software. More sophisticated commercial vulnerability analysis tools, which can cost several thousand dollars, include CyberCop Scanner, Internet Scanner, Retina, and later versions of SAINT.

Hundreds of other free and costly hacking software tools are available on the Internet. Some sites categorize exploits by an operating system and version and provide descriptions of what each exploit can do. Three such sites are *www.attrition.org*, *www.hackersclub.com*, and *www.insecure.org*. I recommend visiting these sites from home or from a secure lab computer that is not attached to the organization's network. Be sure to have current virus software and at least a personal firewall (e.g., BlackICE, Tiny, ZoneAlarm, etc.) to protect yourself should you receive an infected file, or an unscrupulous hacker tries to attack. If you try to visit these sites from work, the organization's firewall should block you. If you get through, you put your organization's network at risk. Once hackers gain control over an initial defence computer like a firewall, they then have a foothold or beachhead from which to launch further attacks on each subsequent set of computers networked to the compromised one. Every networked computer within an organization then is at risk, including mainframes and other hosts. There are no truly safe computers. The "holy grail" of hackers is achieving system security administrator access capability. If they succeed, they can effectively take over a system by changing the password of the system security administrator user ID they signed on with and then removing all other users' IDs. The only way to recover from this

situation is to disconnect the telecommunications link being used, perform an initial program load (IPL), and reinstall the computer configuration parameters, which were, it is hoped, backed up the previous day or week.

Many "Big Four" public accounting firms and other companies are marketing "network penetration testing" services. Network penetration tests are exercises that are preauthorized by organization management. During the test, a "tiger team" of experts attempt to penetrate the firewall and other controls of the organization to gain as much unauthorized access as possible, thereby simulating an actual attack on an organization's computer systems. The timing and results of their exploits are carefully recorded and detailed in a management report. Although this service can be expensive, the results may be highly valuable in identifying weaknesses before they are discovered by spies and hackers. Most organizations do not possess the technical and tactical expertise to take on a full-scale hacker attack. If an organization encounters a situation in which highly skilled hackers are attacking, "mercenary" services can be hired to help defend, identify, and prosecute the malicious party or parties. However, even mercenary experts may not always achieve success. In some situations, mercenaries have been able only to achieve a stalemate, whereby the hackers could disappear without prosecution, leaving the spectre of a possible return later.

7.12 DENIAL-OF-SERVICE ATTACKS

Denial-of-service attacks typically occur when a domain server or servers must respond to huge volumes of messages or data so that they cannot process any other information. Such attacks are typically initiated by outside hackers. For example, a worm is one form of denial service attack. One of the most famous worm attacks occurred on November 2, 1988. The worm, which was written by Robert T. Morris, Jr., replicated itself onto thousands of Internet computers across the country, causing them to slow to a crawl. Ironically, Robert was the son of the chief scientist at NSA's National Computer Security Center. Young Morris was sentenced to three years probation, 400 hours of community service, and a $10,000 fine.

The computer emergency responses team (CERT) was formed shortly after this event. Denial of service can also occur internally and even by accident. A friend who works in a large corporation told me of an incident where an employee of the Human Resources Department sent a routine e-mail to over 10,000 network users during peak business hours and instructed the e-mail application to notify her when the messages were viewed. The resulting e-mail traffic congestion slowed the system to a crawl for all users. Controls to reduce the incidence of denial-of-service attacks include strict logical security controls, restrictions on the size and priority of messages that servers will respond to, and limitations on the use and availability of Internet features such as e-mail.

7.13 WEB SPOOFING AND OTHER MISREPRESENTATIONS

Web spoofing occurs when one website falsely appears to be that of another website. In a web spoofing attack, the web spoofer gains unauthorized access to the victim's website and changes the HTML references from the proper web address (i.e., URL) to that of the spoofing server. All information exchanges between the user and the proper website then pass through the spoofing server. When properly deployed, the user will not even realize that the original site is being spoofed. The primary goal of a web spoofer is to acquire account numbers, passwords, and other sensitive information that unsuspecting users think they are entering into a secure website. The spoofers can then sell the information or use it for their gain.

A 1997 article described an example of an ingenious combination of a website scam that also employed the use of a Trojan horse. Victims were lured to sites such as *www.sexygirls.com* and *www.beavisbutthead.com*. These sites instructed users to download and execute a special viewer program called david.exe. This program disconnected the user's computer from its existing service provider automatically dialled a service provider phone number in Moldova, and then remained connected until the computer was turned off, thereby racking up enormous phone bills for the unsuspecting user. Unfortunately, there are no truly effective ways for Internet users to prevent web spoofing. Internet users must rely on website designers and owners to implement proper security measures so that their sites cannot be altered to direct traffic to a spoofing server. However, users can observe spoofing. For example, if the URL displayed by the web browser does not match the URL of the desired website, or if the location line no longer is visible, spoofing may be taking place. Examples of other types of user misrepresentation that may be encountered on the Internet include web stalkers and paedophiles who spoof themselves as friendly young people to try to lure their prey into face-to-face meetings and those who violate copyrights of software, articles, graphics, and other visual images.

7.14 INFORMATION PRIVACY

This section examines the various information privacy risks, recent privacy laws and regulations, and a case related to website privacy. Major privacy risks include cookies, web bugs, spam, commercial availability of personal information, and identity theft and fraud.

***Cookies—A Violation of Privacy*?:** One way that personal privacy can be violated is by using "cookie" files, or cookies. Cookies are text files residing on the hard drive that is created by major web browser applications, such as Netscape and Microsoft Explorer. Some websites are programmed to write information to cookie files as well as retrieve information from cookie files when users access the site. The types of information recorded in cookies are typically personal. For example, a website may request that a user enter her name, e-mail address, zip code, area code, the type of computer being used, the organization she works for, or other identifying information. Other information copied to cookie files could include the most recent websites a user has visited. This information could be loaded into a cookie file

without the user being aware of it. Cookie-seeking websites could then copy the cookie file into their internal database. The site could also record the types of information the user examined during the visit. Over time, an extensive database of the user's website activity and tendencies could be created and used for marketing promotions and even malicious attacks. A *Consumer Reports* article revealed that Dilbert, Sonic the Hedgehog, Doonesbury, and other popular Internet sites "shill" for DoubleClick Network, an advertising agency, which is "collecting dossiers on the millions of people who visit dozens of popular websites daily—and who may not be aware that someone's gathering private information."

According to the article, "DoubleClick says it uses the information to target its clients' Web ads more effectively to receptive viewers, directing ads to particular occupations or employees in a specific company." One way to control the dissemination of personal information via cookie files is to search the hard drive for cookie files and delete them. In Netscape 3.0 or higher, users use the sequence Options-Network Preferences-Protocols-Show and Alert Before Accepting a Cookie to get an alert that a cookie is being set. Users may also be able to download and install software like Cookie Monster, PGPcookie.cutter, and Cookie Cutter to help control cookie files. Fortunately, in June 1997, Microsoft joined Netscape, Firefly Network, Inc., and Verisign, Inc., in their alliance to more tightly control the personal information that cookies provide. The new "open profiling standard" enables computer users of Netscape Navigator and Microsoft Internet Explorer to determine what information they leave behind on websites.

Web Bugs: "Web bugs" are very much like cookies in that they track Internet use and are virtually undetectable. They are clear Graphics Interchange Format (.gif) images measuring only a single pixel and are not detectable by most cookie filters. Web bugs hidden in e-mail and newsgroup postings can indicate who received them, who read them, and whether the e-mail was forwarded. Cutting and pasting also transfer the bugs. Bugs can even talk to existing cookies on a user's computer if they and the cookies come from the same website. The best option for preventing Web bugs is to install a firewall and configure it to block malicious code from accessing an organization's computers.

SPAM: *Spam* is unwanted or unsolicited e-mail. Spam costs millions of dollars in time, effort, disk storage space, telecommunications bandwidth usage, and user frustration. In a 1999 Gartner Group survey of 13,000 e-mail users, 90 percent received spam at least once a week and almost 50 percent got spammed at least six times a week. In an extreme case in 1998, a Philadelphia spammer named Sanford Wallace sent out as many as 25 million unsolicited ads! In 1999, Connect Northwest, an Internet service provider in the state of Washington, sued CTX Mortgage, a subsidiary of Centex Corporation headquartered in Dallas, for $6 million for overwhelming its network by sending 5,800 unsolicited home mortgage advertisements on April 8 and 9, 1999. This violates a Washington state law that makes it illegal to send an unsolicited commercial e-mail with misleading subject lines, phoney return addresses, and false headers hiding the messages' origin. Many states, including Washington, have antispam laws. In 1998, Washington state sued Jason Heckel and his Salem, Oregon, firm, Natural Instincts, for using a misleading subject line: "Did I get the right email address?" The law was challenged, but in 2001, the Washington State Supreme

Court upheld the law. Spam is best controlled by having users avoid unreputable sites and opt out of information-sharing sites. Numerous antispam software applications are available, including (*www.eprompter.com*), which is free; and Mailbox Filter (*www.mailboxfilter.com*), which is free for a 30-day trial, then $70.

7.15 COMMERCIAL AVAILABILITY OF PERSONAL INFORMATION

A significant problem before the implementation of various privacy laws and regulations (see the section below) was that commercial entities were selling, exchanging, or otherwise making personal information available to third parties without the authorization or knowledge of consumers. For example, in 2000 Amazon.com was discovered to have been selling customer information, much to the chagrin of its customers. Amazon subsequently became the target of lawsuits claiming it violated its privacy statement posted on its website. Amazon ultimately bowed to consumer and government pressure and changed its privacy statement and certain of its information privacy practices. In another case targeted at a specific individual, a former Snohomish County, Washington, a sheriff won a $2.6 million invasion of privacy lawsuit against the Washington State Pharmacy Board after he was accused of obtaining prescription drugs illegally. In addition, his wife and children were awarded $200,000 for the pain and suffering caused by the ordeal. The court found that the Pharmacy Board had used private information in its possession to invade the privacy of the sheriff. Fortunately for consumers, lawmakers in the United States and Europe have enacted strict information privacy laws and regulations. While many organizations continue to ignore them, the largest and most reputable firms have no choice but to comply or risk damaging their reputations and subsequently losing business.

7.16 IDENTITY THEFT AND FRAUD

Undoubtedly the most significant privacy risk is that of identity theft and fraud. It is a scourge on society that lowlife criminals' prey on the identities of law-abiding citizens to facilitate the trafficking and use of illicit drugs, cashing of stolen checks, use of stolen credit cards, money laundering, and other black-market operations. Some of the more notable identity theft and fraud articles include:

- Experian, one of the largest credit reporting bureaus in the United States, reported that between April 2001 and February 2002, unauthorized inquiries were made into about 13,000 credit reports. With information such as Social Security numbers, addresses, account numbers, creditor names, and payment history on credit reports, the thieves have enough information to commit credit fraud. With as many as 700,000 cases annually and 86,000 complaints reported to the Federal Trade Commission in 2001, identity theft tops the list of consumer fraud concerns.

- Hijacking personal data for fraud or theft made up 42 percent of the 204,000 fraud complaints (about 86,000) filed with the Federal Trade Commission in 2001. Identity theft complaints grew immensely from 23 percent in 2000 when it first topped the list.

- Scam artists crack Internet databases, intercept mail, or bluff their way past bank tellers and credit bureaus to gather Social Security numbers, bank account numbers, and other confidential personal information.

- A major crackdown on web-based fraud has broken up pyramid schemes, phone "Beanie Bay" auctions, and other Internet scams that have cheated 56,000 people out of more than $117 million. A total of 88 people were charged and 62 arrested in Operation Cyber Loss involving 61 separate federal, state, and local investigations, the FBI and Justice Department said. The federal and state charges include wire fraud, mail fraud, bank fraud, money laundering, and intellectual property rights violations.

- Two Lucent Technologies, Inc., scientists and a third man were arrested and charged with stealing the "crown jewel" of the telecommunications equipment giant's systems with the intent of transferring the information to a Chinese state-owned company. Two Chinese nationals, Lin Hai and Xu Kai, and a U.S. citizen, Chang Yong-Qing, were accused of corporate espionage by conspiring to steal source code and software associated with Lucent's PathStar Access Server, which provides call-waiting, speed dialling, and other telephone-related Internet communications.

- A busboy allegedly masterminded the largest theft of identity in Internet history and is suspected of stealing millions of dollars from some of the richest people in America.

- Western Union suffered a serious compromise in September 2000 when its website was hacked and almost 16,000 credit and debit card numbers were stolen from an unprotected database while systems underwent routine maintenance. Western Union advised all affected customers to change their card numbers and asked their banks to monitor accounts for suspicious activity. The lapse was attributed to human error. Rival Wells Fargo immediately launched a marketing campaign to tout its superior security record and plant doubt in consumers' minds about less secure firms.

  Since the above type of stolen information could also be made readily available to vast audiences via the Internet, including unscrupulous people and organizations, the information can be used in combination with public information about consumers to steal their identities. When this happens, it can take violated consumers years to fully restore their identities. As with the previous types of information privacy risks discussed, stiffer laws and regulations have been enacted to help protect consumers.

7.17 PRIVACY LAWS AND REGULATIONS

Some of the most notable recent privacy laws that have significant are security and auditing ramifications are presented next. A list of selected privacy resources available on the Internet is also provided.

1. Gramm-Leach-Bliley Financial Services Modernization Act of 1999.

Perhaps the most far-reaching and significant law about information privacy and protection was the Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLB). Senator Phil Gramm (R-Texas) was the lead sponsor of this act, which was signed into law by President Clinton on November 12, 1999. Among other things, this act enables organizations to offer a wide variety of financial products and services to consumers, such as deposit accounts, loans, insurance, and investments. Consumer advocates became concerned that too much information about individuals could be collected by a single organization and possibly sold to others. To help prevent such information exploitation, Senator Gramm spearheaded a consumer privacy amendment, which was added before the act before was signed. Under the final version of GLB, privacy requirements were effective November 13, 2000, with full compliance required on July 1, 2001. In its more notable privacy provisions, the law:

- Requires one-time disclosure of an organization's financial privacy practices to new consumers and annual disclosures of financial privacy practices to all consumers.

- Extends privacy requirements to third-party vendors with whom organizations provide information. Since most third-party arrangements are bound by existing contracts, organizations providing financial services are allowed a two-year grandfathering period for their contracts with third-party vendors to fully safeguard member information in compliance with GLB, although early adoption is highly encouraged.

- Provides consumers with the right to "opt-out" if certain activities would otherwise provide non-public personal information to third parties.

- Requires disclosure of the types of non-public information organizations might provide to outside third parties.

- Requires disclosure of the types of non-public information provided to outside organizations allowed under the Fair Credit Reporting Act of 1970 (e.g., credit bureaus can sell information to mail and telemarketers offering preapproved credit).
- Requires organizations to disclose their information privacy and protection practices.

- Provides civil and criminal penalties for pretext calls, which typically are made by collection agencies, private investigators, and even criminals who pretend to be consumers to get additional non-public information about the consumers.

GLB provides the Federal Trade Commission (FTC) the authority to regulate, monitor, and enforce the information privacy and protection practices of all U.S. organizations providing financial services to consumers, except those falling under the specific jurisdiction of other federal agencies, such as the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), National Credit Union Administration (NCUA), Securities and Exchange Commission (SEC), and all state insurance commissions, which separately regulate insurance activities. These other regulatory entities must still adopt the privacy and security requirements of GLB at a minimum but may do so within the format of their existing regulatory requirements and may add additional privacy requirements. For example, the NCUA included the GLB privacy requirements within its previously existing Rule 716, while the GLB information security requirements were added to its previously existing Rule 748, which covers many other types of credit union security practices. Some of the GLB requirements overlap with existing laws and regulations. Persons committing fraud by using private information gathered illegally would already have been subject to existing fraud laws. With GLB, additional privacy violation charges could be applied on top of the fraud charges. In a more specific example, the Internal Revenue Code already prohibits certified public accountants (CPAs) from disclosing specific tax return information to anyone without the consumer's permission. But since CPAs have many other types of personal information about their clients, the FTC still regulates CPAs regarding information privacy and protection practices. Similarly, a trusted company chartered under the jurisdiction of the OCC is already required to have strict standards of confidentiality under fiduciary law. In this case, any gaps in information sharing would be covered by the OCC's additional regulations implemented under the GLB requirements.

2. Safe Harbor Act of 2000

Europe is ahead of the United States in the information privacy and protection arena. In 1998, the European Union (EU) passed the Data Protection Directive (EUDPD). The EUDPD mandates fair information protection practices for online as well as offline data transfers from the EU before data can be transferred. Although some EU members require additional protections, the DPD provides the minimum information privacy and protection requirements. To address the EUDPD requirements, the U.S. government enacted the Safe Harbor Act of 2000 (SHA), which governs data transferred to the U.S. from the EU. As with GLB, compliance was required by July 1, 2001. The more notable SHA requirements include:

- Must clearly and conspicuously notify users about the purposes for which data will be collected, the mechanisms for limiting use and disclosure, the types of third parties to which data is disclosed, and where to direct inquiries and complaints.

- Must offer users the ability to opt out of disclosures to third parties and secondary uses.

- Must offer users the ability to opt-in for sensitive information such as medical conditions, ethnicity, political views, religion, trade union membership, sexual preference, and so on.
- Must implement reasonable precautions to protect personal information from unauthorized access, disclosure, alteration, destruction, or other loss.

- Regarding electronic systems and databases, "reasonable precautions" implies adequate security measures such as those discussed in this book.

- Must retain information only for the period necessary to fulfil purposes.

- If a third party is acting as an agent, disclosure is not required if the third party meets the safe harbour requirements or is already subject to the EUDPD. This verbiage should be included in any contracts between the organization and third parties.

- Penalties for failure to comply with the Safe Harbor Act include economic sanctions, civil damages, and other remedies. With such motivation, many large organizations doing business in Europe are beginning to meet the SHA requirements. For example, in May 2001, Microsoft announced it would sign the safe harbour agreement.

3. Children's online privacy protection act of 1998

The main goal of the Children's Online Privacy Protection Act of 1998 (COPPA) is to protect the privacy of children using the Internet. The act requires commercial websites to obtain verifiable parental consent before collecting, using or disclosing personal information from children under 13. To inform parents of their information practices, these sites are required to provide notice on the site and to parents about their policies concerning the collection, use, and disclosure of children's personal information. President Clinton signed COPPA into law on October 21, 1998. The law became effective on April 21, 2000, with full compliance required of applicable websites by October 21, 2000. According to the FTC chairman, COPPA puts parents in control over the information collected from their children online and is flexible enough to accommodate the many business practices and technological changes occurring on the Internet. The law was enacted after a three-year effort by the FTC to identify and educate the industry and the public about the issues raised by the online collection of personal information from children and adult consumers. The FTC recommended that Congress enact legislation concerning children following a March 1998 survey of 212 commercial children's websites. The survey found that while 89 percent of the sites collected personal information from children, only 24 percent posted privacy policies and only 1 percent required parental consent to the collection or disclosure of children's information. COPPA has received widespread support from industry, consumer, and law enforcement groups.

4. Health insurance portability and accountability act of 1996

Consumer health records are routinely transmitted over insecure networks and the Internet. Often more than the necessary amount of information is transmitted, and in

some cases, incorrect information is transmitted. Among healthcare organizations, this is sometimes due to inconsistent data classification schemes. These practices frequently violate the medical privacy of consumers. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to help protect and restrict consumer health information. The act provides heavy penalties and potential jail time for offenders, including corporate officers. President Clinton signed HIPAA into law in August 1996. It includes a wide variety of requirements designed to make health insurance more affordable and accessible. With support from health plans, hospitals, and other healthcare organizations, Congress included provisions in HIPAA to require the U.S. Department of Health and Human Services (DHHS) to adopt national standards for certain electronic healthcare transactions and security. By ensuring consistency throughout the industry, these national standards will make it easier for health plans, doctors, hospitals, and other healthcare providers to process claims and other transactions electronically and to better protect personal health information from inappropriate uses and disclosures. In addition, uniform national standards are projected to save healthcare organizations billions of dollars each year by lowering the costs of developing and maintaining software and reducing the time and expense needed to process healthcare transactions.

A three-year deadline was set by HIPAA for Congress to enact comprehensive privacy legislation to protect medical records and other personal health information. When Congress did not enact such legislation by August 1999, HIPAA required DHHS to issue health privacy regulations. At that time, DHHS issued final electronic transaction standards to streamline the processing of healthcare claims, reduce the volume of paperwork, and provide better service for providers, insurers, and patients. The new standards establish standard data content and formats for submitting electronic claims and other administrative healthcare transactions. Most covered entities must comply with these standards by October 16, 2002.

In December 2000, DHHS issued specific rules to protect the confidentiality of medical records and other personal health information. The rules limit the use and release of individually identifiable health information; give patients the right to access their medical records; restrict most disclosure of health information to the minimum needed for the intended purpose; and establish safeguards and restrictions on access to records for certain public responsibilities, such as public health, research, and law enforcement. Improper uses or disclosures under the rule are subject to criminal and civil penalties. These rules become effective on April 14, 2003. Despite these efforts, healthcare organizations have been struggling with HIPAA compliance due to a lack of enough specific requirements from DHHS. The December 2000 rules specified what kinds of records need to be protected, but DHHS still has not specified how such information is to be safeguarded. All that is known is that the requirements will be comprehensive and non-technology specific. Most healthcare organizations are attempting to be proactive by implementing common general information systems controls over their consumer data, although they will not be able to fine-tune their information privacy and protection practices until the final HIPAA requirements have been established.
Some selected privacy resources available on the Internet include:

- Department of Commerce (*www.ita.doc.gov/td/ecom/menu.html*). Safe harbour provisions
- Department of Health and Human Services (*www.hhs.gov*). HIPAA
- Electronic Frontier Foundation (*www.eff.org*). Online Privacy
- Electronic Privacy Information Center (*www.epic.org*). Online Privacy
- Federal Trade Commission (*www.ftc.gov*). GLB and COPPA
- Online Privacy Alliance (*www.privacyalliance.org*). Online Privacy
- Privacy Foundation (*www.privacyfoundation.org*). Online Privacy

5. Monitoring of employee internet activity

To combat lost employee productivity due to non-work-related use of the Internet via company-owned computers and information systems, many firms have begun to restrict and monitor the Internet activities of their employees and to implement disciplinary actions for those employees whose activities are deemed unacceptable. Applications exist that enable system security administrators to prevent users from accessing specifically named URLs. Such applications can also create logs of URLs that have been accessed. This information can then be downloaded and queried for management reporting and productivity analysis purposes. For example, the most frequently visited URLs can be identified and the percentage of time users spend accessing non-work-related URLs can be approximated.

While monitoring controls intend to help ensure that employees are productive at work, failure to adequately disclose monitoring practices can result in lawsuits by employees for violation of their privacy. The Electronic Communications Privacy Act requires employers to inform employees that their use of the Internet or other electronic communications via company information systems may be monitored.

To mitigate the risk of lawsuits by employees claiming violation of privacy, organizations should have a written policy, clearly notifying users that their activities via any company information system, including desktop and laptop computers and telephone devices, may be monitored at any time and that they may be subject to disciplinary action if company information systems are used for purposes other than those necessary to perform their work-related duties. Having users sign an acknowledgement that they have read and understand the policy helps protect the organization. The legal position of an organization can be further strengthened by programming the text of the policy into a banner page that must be read and acknowledged by users each time they sign on to company information systems.

Upon proper disclosure to employees, monitoring controls can be deployed to help reduce the incidence of lost productivity due to non-work-related activities by employees on the Internet. For example, software such as Cyber Patrol, Websense, or Net Nanny can

block access to pornographic and other non-business-related Internet sites. Organizations can also deploy proxy file servers and specialized software to record the URLs being accessed by employees, the dates and times of access, and the user IDs of the employees accessing them. This URL traffic information can be stored for periodic examination by information security personnel. Analysis of URL traffic can reveal the percentage of work-related and non-work-related sites employees are visiting. Based on the times and dates the sites were visited, estimates of the cost of lost employee productivity could be determined and reported to management.

6. Internet risks

The number and types of risks that are possible are limited only by the imaginations of Internet users with malicious intentions. General controls to help prevent Internet risks include environmental controls (e.g., policies, standards, user education), physical security (e.g., securing computer hardware), and logical security controls (e.g., user IDs, passwords, access controls). Cryptography-based controls, such as the SET and SSL cryptographic protocols, are critical if electronic commerce is to flourish.

7. Firewalls

Firewalls can be one of the most effective controls against Internet attacks. They are essential to any organization that is connected to the Internet. A *firewall* is a specialized information system designed to examine incoming and outgoing electronic transmission packets. Based on a set of rules that have been preprogrammed into the firewall configuration by the system security administrator, the firewall determines which electronic transmission packets are allowed to travel through the firewall and under what restrictions. Although unique in their purpose, firewalls can be viewed as just another type of information system. As with any information system, a risk assessment should be performed, and design requirements specified such that the business objectives of the organization can be achieved through the Internet while still enabling the IS security policies and standards of the organization to be deployed upon implementation of the firewall. As a rule of thumb, firewalls should be designed to reject all incoming messages, unless specifically allowed. The extent to which outgoing messages are allowed is a function of organizational culture and desired level of security. Low-risk firewalls may consist of software only (e.g., ZoneAlarm®, BlackICE®, Norton®, Tiny®) or a single electronic network traffic router, which screens electronic transmission packets as they pass from the Internet directly to the destination server.

More complex firewalls consisting of additional hardware components and security applications are necessary for higher-risk systems. For example, a proxy server is a separate CPU that resides between the Internet and the destination server. Using a network address translation (NAT) function, the proxy server can be configured to mask the true address of the destination server so that it appears to be that of the proxy server. In addition to protecting the destination server from outside probing, proxy servers can enable more sophisticated screening, monitoring, and logging of incoming packet traffic before it reaches the destination server. Some products provide system security administrators with warnings (e.g., via reports, and e-mail messages) or alarms (e.g., via

pagers) as well as encryption of outgoing messages. Since proxy servers are application-specific, multiple proxy servers may need to be deployed in a firewall configuration to achieve the desired level of security for each of the Internet applications (e.g., World Wide Web, Telnet, Gopher, Usenet, File Transfer Protocol). In simple terms, each Internet electronic transmission packet consists of a header, interface standards, and data content. The header contains characters that identify the packet as an Internet packet (i.e., " TCP"), the packet number, and the total number of packets. Packet numbering enables the message to be reassembled in its original order. Therefore, a packet with a header of " TCP;38;75;" means that the packet is an Internet packet and that it is the 38th out of a total of 75 in the transmission. The interface standards contain the Internet source address (e.g., "123.241.1.9"), the destination address (e.g., "91.239.88.7), the source port (e.g., "1776"), and the destination port (e.g., "80"). Thus, the above packet header followed by the interface standards "123.241.1.9;91.1.239.88.7;1776;80" identifies where the message came from (unless, of course, the sender is spoofing), where the message is destined, the port number used by the sender, and the source port to which the sender wishes to send the message. The data content is the message or information being transmitted. It can appear in a plain or encrypted format, depending on the security applied to the message. Each network service is mapped to any one of thousands of different port numbers. There are 65,536 (i.e., 216) total ports numbered 0 to 65,535. Ports 0 to 1,023 are well-known ports managed by the Internet Assigned Numbers Authority (IANA). Ports 1,024 to 49,151 are classified as registered, while ports 49,152 to 65,535 are classified as dynamic and/or private. Standard port numbers for a variety of selected internet services are listed next as example references:

Ports 20,21—FTP (file transfer protocol)

Port 23—TELNET (remote sign-on)

Port 25—SMTP (e-mail)

Port 33—DSP (display support protocol)

Port 43—WHOIS

Port 69—TFTP (trivial file transfer protocol—has no security)

Port 70—GOPHER

Port 79—FINGER

Port 80—HTTP (hypertext transfer, World Wide Web)

Port 119—NNTP (network news/bulletin boards)

Port 137—Netbios (name service)

Port 443—SSL (secure sockets layer commonly used for e-commerce)

Port 512—EXEC (remote process execution)

Port 513—(remote login)

Port 515—PRINTER (spooler)

Port 540—UUCP (Unix to Unix communication protocol)

Port 2049—NFS (network file system)

By using a variety of port scanning and network administration tools, hackers will attempt to identify which Internet applications an organization is using. Port numbers can be mapped (i.e., rerouted) to other unused port numbers to make it more difficult for hackers to determine an organization's Internet applications. Although firewalls are a necessary component of any organization's Internet and intranet security environment, firewalls can be easily circumvented by someone within the organization. For example, a network workstation or laptop computer may be outfitted with an analogue modem. The user could plug the modem into an analogue phone jack in the office, connect to an outside Internet service provider, and begin performing activities normally prohibited by the company's firewall. Worse yet, the user could unknowingly download a virus file and infect the entire company network. Furthermore, the workstation or laptop could be hacked and used as a launching pad for additional hacking attempts against the network.

7.18 SELF-ASSESSMENT QUESTIONS

Q.1 Write a comprehensive note on the main challenges during information systems auditing.

Q.2 Describe computer-assisted audit techniques with examples.

Q.3 Write a detailed note on a computer virus.

Q.4 Explain each of the following:

- Software privacy
- Electronic commerce
- History of network
- Information privacy
- Privacy laws and regulations

7.19 ACTIVITIES

7.20

Draft a model of electronic commerce.

7.20 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised; Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research*, *21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly*, *26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal*, *5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, *14*(1), 43.

UNIT-8

Humanistic Aspects of Information Systems Auditing; Information Systems Project Management Audits

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

An effective internal audit function serves multiple roles within an organization. The primary function of an internal audit is to assist the management of an organization in achieving strategic business objectives within a framework of sound internal control practices. All internal auditors, including information systems (IS) auditors, play key roles in this ongoing process. This unit discussed various humanistic aspects of IS auditing, humanistic skills for successful auditing, IS project management, IS project risks, motivational factors of auditors, standardized IS project management methodology and trademark search etc. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- Humanistic characteristics of IS auditing
- Humanistic skills required for IS auditing
- IS project management
- IS project risks

8.1 HUMANISTIC ASPECTS OF INFORMATION SYSTEMS AUDITING

An effective internal audit function serves multiple roles within an organization. The primary function of an internal audit is to assist the management of an organization in achieving strategic business objectives within a framework of sound internal control practices. All internal auditors, including information systems (IS) auditors, play key roles in this ongoing process. Depending on the process or system being evaluated, internal auditors must be able to perform the role of a consultant, mediator, negotiator, investigator, facilitator, and educator. The ability of internal auditors to effectively fill these roles benefits management and therefore provides a valuable resource to many organizations. On an individual basis, auditors who are flexible enough to effectively perform multiple roles should be highly valued by their companies.

Auditing originated as one of the fields within the accounting profession. The accounting profession can be divided into two general categories: public accounting and private accounting. Public accountants perform a variety of services for their clients, including financial statement audits, income tax planning and preparation, financial planning, and consulting in a variety of areas, including IS controls. Private accounting encompasses accountants who work for commercial, government, not-for-profit, and other types of entities. Many of the activities of private accountants essentially mirror those of public accountants, but these activities are performed on behalf of private organizations. As the activities in which businesses, governments, and other entities engage have become more complex, auditors have had to evolve beyond only evaluating controls directly about financial statements. Because organizations are involved in so many different types of businesses and related activities, unique sets of internal controls had to be developed within these activities. Auditors had to become highly knowledgeable about specific types of internal controls, which, if not properly deployed, could eventually impact the financial condition of an organization in a material way. As a result, auditing specialists began to appear. Examples of areas in which auditors specialized include trust, financial services, and internal and external fraud prevention. With the advent of computers, a new breed of control specialist was born—(the electronic data processing (EDP) auditor.

Electronic data processing auditing was once viewed as a separate profession from another auditing in general. Many EDP auditors came from technical backgrounds rooted in computer science. However, as technology continues to evolve and expand into the end-user environment, the barrier that once existed between traditional auditing and EDP auditing has shrunk enormously. Traditional auditors have had to become computer literate or risk losing their livelihood. Traditional auditors, both internal and external, have had to reach outside their typical auditing paradigms and increase their understanding of and proficiency with computers. Conversely, EDP auditors have had to enhance their business skills to better communicate risks associated with computing systems to a more knowledgeable and computer-savvy management group. What we are witnessing is the evolution of a new breed of auditor: the IS auditor.

8.2 TRAINING

Training related to IS audit, controls, and security of new and existing technologies can be obtained from a variety of sources. For example, professional associations such as the Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), and AICPA sponsor one or more technology-related conferences and seminars each year. A host of other organizations sponsor conferences covering a wide variety of audit, control, and security-related subjects. Conferences and seminars offer several benefits. First, they provide high-to midlevel training sessions on a variety of technical subjects. These training sessions are typically grouped into several categories, or "tracks." The length of the sessions usually ranges from two to eight hours. The overall length of conferences usually ranges from three to five days, while seminars are typically one to three days.

Second, conferences and seminars offer the ability to network with peers, scholars, and experts in the field of IS controls and security. Conferences are one of the most effective means through which to meet numerous IS experts from a variety of industries and countries. Conference sessions with such large and diverse groups of IS auditors frequently generate enthusiasm among attendees to apply audit techniques to the applicable technologies in organizations. Conferences and seminars are also excellent forums for sharing experiences so that each may benefit from the other's collective knowledge. The third benefit of conferences and seminars is that they are a source of continuing professional education (CPE) credits for attendees who possess one or more certifications that require them to earn a minimum number of CPE credits annually. Most professional associations provide the added benefit of offering brief training sessions during monthly or quarterly meetings and technical sessions sponsored by the local chapters of the associations. Independent training organizations such as the MIS Training Institute also offer highly detailed courses lasting one week or more that discuss the operations and controls about specific computing system platforms. Because these courses are relatively small by design, they provide the opportunity for hands-on exercises and direct interfacing with the instructors and other students. Facilitation skills were traditionally not a part of the IS auditor’s portfolio. However, with the advent of control self-assessment (CSA), facilitation skills are becoming a must.

Another audit management flaw in some organizations is their reluctance to budget sufficiently for training auditors. Expense control is understandable, but some organizations allow very little for any outside training, instead opting to rely on on-the-job training. In one organization, the auditors were lucky to receive mileage for driving to an off-site audit location, let alone be allowed to attend a conference or seminar or have the organization pay for membership in a professional association and the costs to attend association functions. This sort of audit management is highly unfortunate because the auditors become "inbred." They tend to assess situations almost exclusively from the perspective of their organization. They are much less likely to directly exchange ideas and benchmark with auditors and other professionals in other organizations within and outside their industry. As a result, their creativity and enthusiasm can be stifled. A small

but continuously and highly trained IS audit staff will significantly outperform a large but restricted staff. The small and highly trained staff would prove to be much more effective and valuable to their organizations than many IS auditors with little or no ongoing training.

8.3 ACTIVE PARTICIPATION IN PROFESSIONAL ASSOCIATIONS

Becoming actively involved with local chapters of professional auditing associations can be one of the most important career-enhancing activities an auditor can undertake. Besides providing a forum for learning about technical subjects, active participation can contribute greatly to professional growth by allowing one to network with local auditing peers. Holding leadership positions can also provide a high profile for an organization's audit group and the organization in general. Furthermore, holding officer positions can provide valuable leadership and teamwork skills in a democratic, not-for-profit environment.

8.4 NETWORKING

Networking at conferences and professional association leadership functions was discussed in the previous section. However, networking can also be accomplished at the local level as well. Through an effective local network, one can develop contacts in a variety of different industries. These individuals can be valuable resources when one is searching for information on different auditing techniques, technical information on new and existing technologies, or simply to exchange ideas. Contacts from organizations within the same industry can provide benchmarking standards for an organization. Also, contacts from different industries can add diversity to one's perspective. The nice part about personal "local area networks" is that one can physically meet these people for lunch or at some other informal venue to discuss topics of interest. Networking opportunities of a different nature occur when one is an active chapter board member. For example, the ISACA International office helps facilitate the development of chapter leaders throughout the world by hosting annual leadership conferences. Both the international and regional leadership conferences generate teamwork, camaraderie, and fun among the attendees through group social functions and outings.

8.5 PROFESSIONAL CERTIFICATIONS RELATED TO INFORMATION SYSTEMS AUDIT, CONTROL, AND SECURITY

Professional certifications related to the field of IS audit, control, and security attest to the holder's knowledge and experience. In general, these professional designations are designed to achieve these objectives:

- To evaluate individual competence in the field
- To provide a mechanism for maintaining such competence

- To provide management objective criteria for personnel selection and promotion

Earning and maintaining professional designations provide many benefits to certificate holders. These benefits include:

- Demonstrate expertise and competence in the field
- Attain career recognition
- Enhance career through promotions
- Establish professional credibility and qualification across industry lines
- Encourage professional growth

To earn a professional certification, candidates are typically required to pass an examination, or series of examinations, which tests their mastery over a particular body of knowledge. By passing the examination, candidates attest that they have attained the required knowledge level. Although professional certifications are not a substitute for practical experience, most audit-related certifications require candidates to provide proof of at least a few years of practical auditing experience. By requiring proof of a few years of practical auditing experience, the overall competence of the certificate holder is supplemented.

After earning a professional designation, certificate holders are expected to maintain a current proficiency by earning a certain number of continuing professional educational (CPE) credits each year. A CPE credit is typically equivalent to 50 minutes of contact time. Continuing professional education credits can be earned by attending seminars, conferences, college courses, and some correspondence courses and tests; meetings of audit-related professional associations: writing books, articles, and research papers; performing oral presentations; and participating as an officer or committee member in an audit-related professional association. The number of CPE credits allowed for these types of activities varies among each certification sponsor.

8.6 CERTIFIED INFORMATION SYSTEMS AUDITOR

The CISA designation is sponsored by ISACA. There are currently over 26,000 ISACA members in over 100 countries. The CISA designation was first established by ISACA in 1978. There are currently more than 14,000 CISAs worldwide. To earn the CISA designation requires candidates to pass a four-hour-long examination consisting of 200 multiple-choice questions covering seven areas:

1. The IS Audit Process
2. Management, Planning and Organization of IS
3. Technical Infrastructure and Operational Practices
4. Protection of Information Assets
5. Disaster Recovery and Business Continuity
6. Business Application System Development, Acquisition, Implementation, and Maintenance
7. Business Process Evaluation and Risk Management

8.7 CERTIFIED INTERNAL AUDITOR

The Certified Internal Auditor (CIA) designation is sponsored by the Institute of Internal Auditors (IIA). There are currently over 75,000 IIA members in over 120 countries. The CIA designation was first established by the IIA in 1974. There are currently over 35,000 CIAs worldwide. Earning the CIA designation requires candidates to pass a four-part examination administered over two days. Each part is 210 minutes long, for a total examination length of 14 hours. Each part consists of 80 multiple-choice questions, broken down into four parts:

Part 1—Internal Audit Process
Subjects: Auditing, Professionalism, Fraud

Part 2—Internal Audit Skills
Subjects: Problem Solving and Evaluating Audit Evidence, Data Gathering, Documentation, and Reporting Sampling and Mathematics

Part 3—Management Control and Information Technology
Subjects: Management Control, Operations Management, Information Technology

Part 4—Audit Environment
Subjects: Financial Accounting, Finance, Managerial Accounting, Regulatory Environment. In addition to passing the examination, candidates must hold a bachelor's degree or equivalent from an accredited college-level institution. In some cases, other professional designations may be accepted as equivalent to a bachelor's degree. A character reference must also be submitted from a responsible person, such as a supervisor, manager, educator, or CIA. Finally, candidates must possess two years of internal audit or equivalent experience. A master's degree can be substituted for one year's work experience. To maintain the CIA designation, certificate holders must earn a minimum of 80 CPE credits over a fixed two-year period. Certificate holders must adhere to a code of professional ethics.

8.8 CERTIFIED PUBLIC ACCOUNTANT

The Certified Public Accountant (CPA) designation is sponsored by AICPA, which has over 330,000 members across the United States. The Uniform CPA Examination was first administered in 1917. There are currently over 400,000 CPAs in the United States. Although membership in most sponsoring organizations is not mandatory to maintain certification, it is interesting that the number of CPAs far exceeds the number of AICPA members. This is since a CPA license is mandatory for those practising public accounting. Earning a CPA designation requires candidates to pass a four-part examination administered over a two-day period. Each part is from 180 to 270 minutes long, for a total examination length of 15.5 hours. Each part consists of multiple choice and/or essay questions, broken into four parts:

Part 1—Business Law & Professional Responsibilities; Information Technology (70–80 per cent multiple choice/objectives, 20–30 per cent essay)

Part 2—Auditing (70–80 percent multiple choice/objectives, 20–30 percent essay)

Part 3—Accounting & Reporting—Taxation, Managerial, Governmental and Not-for-Profit Organizations (100 per cent multiple choice/objective)

Part 4—Financial Accounting & Reporting (70–80 per cent multiple choice/ objectives, 20–30 per cent essay).

8.9 CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

The Certified Information Systems Security Professional (CISSP) designation is sponsored by the International Information Systems Security Certification Consortium, Inc. (ISC2). The CISSP designation was first established by the ISC2 in 1992. There are currently about 8,500 CISSPs worldwide. To earn the CISSP designation requires candidates to pass a six-hour-long examination, consisting of 250 multiple-choice questions covering 10 domains:

1. Security Management Practices
2. Security Architecture and Models
3. Access Control Systems and Methodology
4. Application Development Security
5. Operations Security
6. Physical Security
7. Cryptography
8. Telecommunications, Network, and Internet Security
9. Business Continuity Planning
10. Law, Investigations, and Ethics

8.10 CERTIFICATIONS IN CANADA, THE UNITED KINGDOM, AND AUSTRALIA

The Canadian Institute of Chartered Accountants (CICA) and the Institute of Chartered Accountants in England and Wales (ICAEW) both sponsor a designation known as the *Chartered Accountant* (CA). Each is independently administered and subject to unique and independent certification requirements. There are over 76,000 members of the CICA and 120,000 members of the ICAEW.

In Australia, there are two somewhat competing professional accounting bodies: the Institute of Chartered Accountants in Australia (ICAA) and the Certified Practising Accountants of Australia (CPAA), formerly known as the Australian Society of Certified

Practising Accountants (ASCPA). The ICAA has over 37,000 members, while the CPAA has over 105,000 members. Each is an independent association that sponsors separate professional certifications: Chartered Accountant (CA) and Certified Practising Accountant (CPA), respectively. For purposes of establishing standards and guidelines, the two organizations have created the Australian Accounting Research Foundation (AARF), with representatives from each organization comprising the Joint Standing Committee, which oversees the foundation's board of management. The National Institute of Accountants (NIA) is yet a third organization with over 14,000 members. The NIA does not sponsor a separate certification but offers several levels of memberships based on experience and education.

8.11 OTHER CERTIFICATIONS

A list of another audit, control, and security-related professional designations follows. The eligibility and maintenance requirements of each of these certifications are like the professional designations.

- *Certificate in Data Processing (CDP),* sponsored by the Association of Information Technology Professionals (AITP). Before 1996, the AITP was known as the Data Processing Management Association (DPMA).
- *Certified Management Accountant (CMA),* sponsored by the Institute of Management Accountants (IMA).
- *Certified Fraud Examiner (CFE),* sponsored by the Association of Certified Fraud Examiners (ACFE).
- *Certified Financial Services Auditor (CFSA),* sponsored by the National Association of Financial Services Auditors (NAFSA). In mid-2002, NAFSA merged with the Institute of Internal Auditors (IIA). The CFSA certification will continue to be offered through the IIA.
- *Certified Government Auditing Professional (CGAP),* sponsored by the Institute of Internal Auditors (IIA).
- *Certification in Control Self-Assessment (CCSA),* sponsored by the Institute of Internal Auditors (IIA).
- *Global Information Assurance Certification (GIAC),* sponsored by the SANS Institute. GIAC is a program where candidates can earn up to 10 different GIAC certifications in differing areas of specialization.

- *Systems Security Certified Practitioner (SSCP),* sponsored by the International Information Systems Security Certification Consortium (ISC2).
- *Certified Protection Professional (CPP),* sponsored by the American Society for Industrial Security (ASIS).

8.12 READING

Because of the rapidity with which information technology changes, one must budget as much time as reasonably possible to read various publications about IS audit, control, and security, as well as new technologies. The reading regimen should be something done daily. Often, new control weaknesses may be identified in information systems currently being used in an organization or that one is preparing to examine. Since new technologies are constantly being implemented within organizations, one of the most timely and effective means for one to stay current is through reading. Among the types of publications that provide current information about new technologies and IS audit, control, and security techniques are books, trade journals, magazines, national and local newspapers, various business news services, newsletters from professional auditing associations and their local chapters, and industry-specific bulletins, newsletters, flyers, and regulatory updates. Many of these publications are available on the Internet. Some publications are available only on the Internet. One thing to keep in mind is to not overwhelm yourself by thinking you must read every word of every technology-related publication.

8.13 PRACTICAL EXPERIENCE

There is no substitute for practical experience in auditing information systems, new technologies, and related processes. At some point, your training, professional affiliations, networking, certifications, reading, and other education must be applied to real-world situations to recoup your and your organization's investments of time and financial resources. Application of these skills is where your organization will reap the benefits of a significantly more secure IS control environment. Theory alone is no substitute for the reality of practical experience. The human factor is the great unknown in the deployment and control of all information technologies. Humans are what create an unpredictable IS an environment. Our role as auditors and IS security professionals is to continuously evaluate IS controls to minimize the risk presented by the human factor. As you gain more and more practical experience, you will become progressively more comfortable and adept at auditing the logical security, physical security, and operational aspects of a variety of applications, database management systems, operating systems, and related processes. You will also become a valuable consulting resource for your organization when IS control and security issues arise, as in the case of the development

and implementation of new technologies, or the resolution of recently identified IS control weaknesses or operational deficiencies.

8.14 HUMANISTIC SKILLS FOR SUCCESSFUL AUDITING

One of the most often overlooked but essential skills for IS auditors and any other type of auditors to possess are those about communication and interpersonal relations. Skills such as a high-level business understanding, verbal and written communication skills, analytical skills, and negotiation skills are equally as important as the technical skills necessary to effectively evaluate IS control environments.

Under modern internal control frameworks, auditee management is encouraged to look to auditors for suggestions as to how to improve operations and achieve strategic objectives. Auditors must be able to act as a liaison between management and staff and between the management of different departments that rely on each other but may be experiencing common difficulties. They must be able to present findings and effectively interact with staff at all levels of the organization, from executive management down to the individual workers, and at every level in between. This interaction may be in the form of verbal conversations, written or electronic correspondence, and/or a combination of the two, as in the case of a presentation to management or the performance of a CSA workshop. All auditors must have a high-level business understanding to assess the potential significance of operational and control issues and to communicate the effects of these issues to management. Auditors must also be likeable, approachable, and able to befriend people. These skills are especially important when dealing with line workers. Line workers are frequently an excellent source of detailed information of which management may not be aware, especially when evaluating efficiency/effectiveness issues.

8.15 MOTIVATION OF AUDITORS

The motivation of auditors is as complex a subject as for any group of individuals. Everyone has different wants, needs, and desires, and is therefore motivated by different factors. To delve deeply into human psychology and management theory as to all the possible motivating factors that exist are creativity in one's job and goal-oriented financial incentives.

8.16 INFORMATION SYSTEMS PROJECT MANAGEMENT AUDITS

New electronic products and services are being introduced into the marketplace at an increasing pace. Computers have evolved to the point where new applications can be created and implemented quickly, often before they have been thoroughly evaluated for control weaknesses. Because of the sheer number of new products and services companies are deploying, and because of limitations on the size of many auditing staffs, it is becoming increasingly difficult to find enough time and resources to perform

effective audits of new systems and processes using traditional auditing methodologies. To adapt to this changing systems development environment, information systems (IS) auditors must adjust their approach. As with any audit, a risk assessment should be one of the first steps to be completed when examining a new process. The risk assessment will help determine whether the process warrants expending a significant amount of audit resources on the project. The scope of the audit depends on the risk. But even for high-risk systems, the scope should be limited to testing the critical internal controls upon which the security of the process depends. Throughout the development of any new process, IS auditors can provide expertise not only on internal control issues, but also on issues that ensure that systems and related policies and procedures can be performed efficiently and effectively and conform to applicable laws, regulations, and other standards to which management wishes to adhere. Depending on the scope of the audit, auditors can also confirm that the development, implementation, and hardware costs of the new process are properly recorded and reported in the financial statements. Auditors should also assess the adequacy of the overall project management.

Project management oversight can stymie a project just as quickly as an internal control weakness or operational difficulty. Many information systems development project management (ISPM) controls were formally developed during the early days of computers and are still applicable in today's IS environments. However, the number of cases in which these controls need to be applied has exploded, especially over the last 10 years. Virtually all organizations have become highly dependent on computer information systems to achieve their strategic business objectives. To maintain and enhance their competitive positions, these organizations must continue to maintain and upgrade their existing computer systems. They must also continue to develop and implement new systems. Over the last five years, many organizations have deployed new e-commerce products and services to remain competitive, often at significant costs. The Gartner Group predicts that global information technology (IT) spending will reach $3.3 trillion in 2002.

Furthermore, the total dollar amounts and transaction volumes processed by these systems are increasing at an exponential rate. All large projects are faced with a myriad of potential risks. The project management body of knowledge is vast, and volumes have been written about project management. It is no wonder that project management is considered a separate profession. Information systems project risks affect all areas of an organization, either directly or indirectly, and thus pertain to all components and objectives of the COSO (Committee of Sponsoring Organizations of the Treadway Commission) internal control model.

8.17 INFORMATION SYSTEMS PROJECT RISKS

- IS project failure (complete or partial)
- The vendor goes out of business

- Poorly worded contracts or agreements
- External contractor risks
- Financial statement risks
- Each of these risks is discussed in a separate section, with an emphasis on the IS project
- failure risk. Within each section, internal controls designed to mitigate the risks are presented.

8.18 PROJECT FAILURE

The primary risk of any IS development project is that of project failure. Failure can be total or, more commonly, partial. Partial failure includes completing the project late, over budget, with fewer features, or some combination of these.

8.19 STANDARDIZED INFORMATION SYSTEMS PROJECT MANAGEMENT METHODOLOGY

Every organization should develop and implement a standardized ISPM methodology. An ISPM methodology is a major control that helps ensure that IS development projects are completed in a consistent, timely, efficient, and effective manner. It also helps prevent scope creep, or the tendency to keep adding additional features to a system during the design phase beyond that which was originally planned. Without a standard approach, IS projects are left under the direction of individual project managers. This may be acceptable and successful if the same person manages all IS projects and is sufficiently skilled in ISPM.

Project management methodology

I. Initiation
II. Analysis
III. Design
IV. Development
V. Test
VI. Implementation
VII. Postimplementation support

8.20 PROJECT OVERSIGHT GROUPS

Project oversight groups such as steering committees and applicable project subcommittees are often overlooked. Project oversight groups perform valuable monitoring functions to help determine when projects are falling behind or are going over

budget. They are responsible for implementing measures to rectify project problems promptly. Such measures include the retention and replacement of key project personnel.

8.21 TRAINING OF PROJECT TEAM MEMBERS

Without adequate project management training, internal team members will not be as productive as desired which can be a detriment to their projects. One potential source of project management training is the Project Management Institute (PMI), an international organization devoted exclusively to the field of project management. The PMI provides training, education, networking, and other resources related to the project management field, and sponsors two related professional certifications. The IS project budget should also provide adequate funding for technical training, especially for technical staff who may be implementing a new operating system or database management system or updated versions of existing systems.

8.22 CHANGE CONTROLS

Upon completion of testing, system access controls should exist to ensure that the transfer of approved software programs into the production environment is performed by an area independent of the software development group. This segregation of duties helps ensure that programmers do not introduce unauthorized programs and changes into the production environment. Change controls are not unique to new IS development projects. Routine procedures should already exist to ensure that all new and updated software programs are subjected to quality reviews and that programmers do not move new and updated programs into the production environment.

8.23 TRADEMARK SEARCHES

Project managers should ensure that any necessary trademark searches and applications are performed early in a project. Failure to secure a trademark could cause project delays and force marketing areas to spend excessive funds to re-create advertisements and other promotional materials.

8.24 VENDOR GOES OUT OF BUSINESS

As evidenced by the recent dot-com bust, there are no guarantees that prospective vendors will remain in business. If a vendor goes out of business or significantly reduces staff, the success of an IS development project will be in jeopardy. Therefore, due diligence is an important control that organization management should perform before expending significant IS resources and before signing any contracts or agreements. After obtaining competitive bids, due diligence efforts should include:

- Reviewing audited financial statements of vendors for the last two or more years
- Contacting current and former clients to assess customer satisfaction.

- Reviewing vendor privacy policies displayed on their websites.

- For organizations which are external service providers or IS security vendors, review the last two or more SAS 70s or other applicable IS security certification results (e.g., TruSecure, CPA SysTrust, CPA WebTrust, BBBOnline, TRUSTe).

- Outsourced technology services create significant enough risks to financial institutions.

8.25 POORLY WORDED CONTRACTS OR AGREEMENTS

Contracts and agreements play a critical role in the development and ongoing success of information systems. Optimally, contracts and agreements should be finalized before significant IS project resources have been expended. A formal contract management process within the organization will help ensure that standard provisions are included in all IS contracts and that they have been reviewed by legal counsel. Like project management, contract management is a separate field with its own vast body of knowledge, as evidenced by the many attorneys who specialize in the field. However, it is important to highlight a few critical provisions which should be contained within all software license, maintenance, and support agreements. They include:

- The exact amounts of the software license, maintenance, and support fees and payment terms.

- Service levels to be provided by the vendor (e.g., 24/7 availability for critical problems: 10/5 for noncritical ones). These provisions are often referred to as service-level agreements. They may be a separate agreement or contained within the maintenance and support agreement.

- Confidentiality/nondisclosure statement providing recourse against the vendor company in the event of theft or divulging of proprietary information or other information privacy breaches. This statement is usually included within the master agreement or contract.

- A section requiring the current version of the application source code to be held in escrow at an independent third party. This section should specify the conditions under which the source code will be released to the client (e.g., vendor ceases operations, vendor breaches contract).

8.26 EXTERNAL CONTRACTOR RISKS

External consultants, contractors, and vendor representatives working on-site expose organizations to increased risks of unauthorized system access, unauthorized expense payments, theft of intellectual property, and information privacy violations. These

contractors are often placed in high-profile ISPM positions and other positions of high trust. Some staff-level employees may perceive them as having management authority and may unwittingly perform duties that are not authorized by organization management. They also often have physical access to sensitive areas of the contracting organization. In larger organizations, the problem is magnified. Typically, many IS projects are in process at any time. Often a steady stream of external consultants, contractors, and vendors revolves through the IS department, performing various IS project duties. In this type of environment, strangers are often taken for granted as just another external contractor.

Five controls can help mitigate external contractor risks:

- Expenditures should follow the contracting organization's standard accounts payable process, which includes requiring signed authorization by organization management for expenses and researching vendors for legitimacy and potential conflicts of interest. Since contractors are not employees, they should not be allowed to act as agents of the organization or otherwise contractually obligate the organization.

- The contractor's direct report should provide a current list of individual contractors who are deployed at organization locations to the Human Resources Department. The list should include for each person: the full name; the name of their direct report within the organization; contact information (phone number, e-mail address); the project or projects being worked on; and the start and end dates at each organization location. This list should be made available to all staff via e-mail and/or intranet in the event a particular contractor's presence or purpose is questioned.

- Each contractor, consultant, or vendor representative who is deployed at any of the contracting organization's locations should sign a confidentiality/nondisclosure agreement, even if the vendor company has already signed one. The reason is that on-site personnel may meet private information unrelated to the project. Thus, they must be held individually accountable for their actions. This agreement should state, among many potential legal limitations, that during their contractual duties they will not divulge any information they develop, observe, or otherwise become aware of to any outside parties without written permission from the contracting organization's management. The agreements should be included as part of the project documentation or maintained within the Human Resources Department.

- Every outside person who is going to be on-site for an extended period (e.g., more than one week) should be provided with a one- to a two-hour training session on evacuation routes and procedures during fires and disasters, location of first aid and other safety equipment, and whom to contact in the event unauthorized activities by the client organization's employees or other contractors are observed. Such training serves to help protect the safety of contractor personnel.

- As always, the Human Resources Department should be aware of the types of activities and durations of stays of external personnel to reduce the risk of them claiming they are acting as employees of the organization.

8.27 FINANCIAL STATEMENT RISKS

Information systems projects present several financial statement risks due to the relatively large dollar budgets associated with them. Project cost overruns rank at the top of the list. Two additional risks warrant discussion. The risk of unauthorized expenses from external contractors has been mentioned. The same risk exists for internal IS employees. For example, a former Starbucks IS employee was charged with embezzling $3.7 million by forging her supervisor's signature on a fictitious consulting services agreement. This enabled her to begin drawing funds to pay over 100 invoices she created in the name of the fictitious business for services that were never rendered.

A lesser known generally accepted accounting principle is AICPA Statement of Position (SOP) 98-1 entitled "Accounting for Costs of Computer Software Developed or Obtained for Internal Use." SOP 98-1, which was issued on March 4, 1998, specifies various costs that should be capitalized and amortized over the estimated useful life of an internal-use system. Typically, the most difficult of these costs to measure is the hours spent by internal staff on software development. The reasons are that many developers abhor keeping track of the hours they spend on projects, and the system used to track the hours is inadequate.

These controls can help mitigate the above-mentioned financial statement risks:

- General ledger entries for IS project expenses should be recorded with enough detail so that reports comparing all applicable IS project expenses to all budgeted expenses can be prepared in a timely and accurate manner for review by the IS steering committee and other project oversight groups. Project expenses should include payments to IS project vendors for items such as contractor hours for labour and internal staff training, software license fees, software maintenance and support fees, and on-site contractor travel costs (airfare, hotel, meals, rental cars, taxi, "other"). This type of monitoring activity should occur on a monthly or more frequent basis.

- Expenditures should follow the contracting organization's standard accounts payable process, which includes requiring signed authorization by organization management for expenses and researching vendors for legitimacy and potential conflicts of interest.

- An accurate process should exist for recording all hours spent by internal staff on software development as well as recording all other software development costs.

8.28 SELF-ASSESSMENT QUESTIONS

Q.1 What are the main characteristics of an IS auditor? Explain

Q.2 What skills are required for an IS auditor? Discuss.

Q.3 Write a comprehensive note on IS project management.

Q.4 Explain each of the following:

i. Professional certification related to IS

ii. IS project management audits

iii. Trademark

8.29 ACTIVITIES

Sketch IS project management and explain each component.

8.30 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised; Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research*, *21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly*, *26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal*, *5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, *14*(1), 43.

UNIT-9

New Technologies and Constant Risks

Compiled by: **Dr. Amjid Khan**

Reviewed by: **Dr. Pervaiz Ahmad**
Dr. Muhammad Arif
Muhammad Jawwad

CONTENTS

INTRODUCTION

This unit discussed emerging technologies related to IS and IS auditing. It also described the challenges and risks associated with IS and IS auditing. At the end of the unit, self-assessment questions followed by practical activities are given to the students.

OBJECTIVES

After reading this unit, you will be able to understand:

- New emerging technologies related to IS auditing
- Risks associated with IS auditing

9.1 NEW TECHNOLOGIES

In 1998, the broadband Internet-in-the-Sky network of over 840 satellites envisioned by the Teledesic LLC of Bellevue, Washington, seemed a certainty. But by mid-2002, according to their website (*www.teledesic.com*), the concept called for a total of only 30 satellites, with an initial launch of 12. Service is slated to begin in 2005. The reduced number of satellites is undoubtedly due in part to the economic downturn, the dot-com bust, and the subsequent lack of additional venture capital. It remains to be seen whether primary investors such as Bill Gates, Craig McCaw, and the Boeing Corporation will be successful with their $9 billion-plus investment and whether it will ever reach its originally planned constellation of interlinked medium-Earth orbit, low-cost satellites that can provide true global access to a broad range of telecommunications services such as computer networking, broadband Internet access, interactive multimedia, and high-quality voice. If successful, this technology will present some interesting risks, including eavesdropping or intentional disruption of the data transmitted throughout the network. It also seems possible that hackers could wrest control of the satellites and alter or terminate their orbits.

A simpler technology holds more immediate promise. ***Microsoft*** is researching password technology whereby users click on several points within a screen of images. The points correspond to pixels, which are then converted into a random number that is stored in the computer. Users only must remember where on the images they clicked and in what sequence. They will essentially be creating a 20- or more-character password without having to remember it. This technology sounds promising, but auditors must be alert to obvious potential risks, such as whether the file containing the 20-character passwords is encrypted and whether the passwords are encrypted while in transit across networks or the Internet.

Biometric technologies are gaining in reliability and costs have come down. Therefore, applications of biometric technologies to access controls that help prevent fraud and help ensure security are becoming more commonplace. One credit union is using hand-image verification in conjunction with a personal identification number to provide unescorted access to safe deposit boxes. Similar technologies are becoming available for automatic teller machines, airport security devices, driver's licenses, and state-issued identification cards.

The National Aeronautics and Space Administration has been using an Internet outsourcing service from eTrue, Inc., which authenticates users for both Web and local network log-on through multiple biometrics, such as face and fingerprint verification. Iris recognition systems such as those developed by Iridian Technologies (*www.iridiantech.com*) have been used in prisons and airports.

Facial recognition is also becoming a reality now that the public is more open to deploying such technology for passive surveillance and possibly a national identification card system. The International Biometric Group, a biometric consulting group, estimates that sales will grow from $58 million in 1999 to $594 million in 2003, with 65 percent of the market being in the United States. Since this prediction was written the events of September 11, 2001, I suspect that demand for biometric security devices will increase even more rapidly.

While biometric controls will likely replace or at least supplement passwords and additional controls, they, too, can be circumvented. A Japanese researcher recently found that he could create fake fingers from gelatin and fool fingerprint readers an average of 80 percent of the time. Perhaps a more critical concern would be the theft of the electronic "prints" of innocent people and the subsequent usage of the information to steal identities. Therefore, IS auditors will need to be alert to the limitations of the biometrics that they encounter in their organizations.

Nanoscience, which is the study of materials smaller than 100 nanometers (1/10th the width of a human hair), has come to the forefront of technology circles within the last year. One application of the technology is to create computer circuits based on single molecules. In August 2001, IBM reported that its researchers had built a logic circuit that can perform processing functions using tiny cylindrical structures, called carbon nanotubes, as semiconductors. The nanotubes are about 100,000 times thinner than a human hair, about 10 atoms across, and about 500 times narrower than current silicon processors. This nanotechnology could render the existing silicon-based semiconductors obsolete. At the current rate of progress, silicon-based chips are projected to have a 10- to 15-year life cycle because it will no longer be possible to make them smaller, thereby limiting improvements in chip size and speed.

Nanotechnology has such great potential; it could rival and eventually exceed the human brain in processing and learning power. Nanoscience could also lead to other unexpected properties, such as lightweight breathable fabrics that stop bullets. Even more mind-boggling, in September 2001 physicists in Denmark made two samples of trillions of atoms that interact at a distance. This breakthrough could lead to real-life quantum communications systems and computers, even teleportation.

But nanotechnology is not without its risks. Stephen Hawking, the world-renowned physicist, projects that computers could develop intelligence and potentially take over the world, given enough time. This is because, in contrast to our intellects, computer performance has been doubling every 18 months. Hawking suggests that one solution to combat this threat would be to use genetic engineering to increase the complexity of human DNA and improve human beings.

About IS auditing, the general risks and controls will be the same so long as nano-based computers function on the binary system. However, the almost incomprehensible speed and beyond-microscopic size of the individual processors will undoubtedly present risks that we cannot even imagine. It will be up to future IS auditors to help create controls that can help mitigate these new risks.

9.2 CONSTANT RISKS

We must implement controls to help our organizations and our government prevent such atrocities from ever happening again. But we must not forget about the traditional weaknesses and challenges that we face daily. In its popularly quoted but non-scientific 2002 Computer Crime and Security Survey of practitioners in a variety of U.S.

corporations, government agencies, financial institutions, and universities, the Computer Security Institute (CSI) found that 223 of the 503 respondents were willing and able to quantify their computer crime losses at $456 million. The actual loss figure within the United States is most certainly many orders of magnitude larger since many organizations are reluctant to share loss information. The most common loss categories cited by CSI were theft of proprietary information ($171 million), financial fraud ($116 million), insider abuse of Internet access ($50 million), and viruses ($50 million). While the CSI survey references insider abuse of Internet access, insider abuse is a farther-reaching problem. There have been many incidents of insiders causing astronomical harm, some even jeopardizing the security of the United States. The following cases are just a sampling of many cases of insider abuse.

- Robert Hanssen, an FBI agent with high-security clearance, was one of the most damaging spies in U.S. history. Hanssen was convicted of espionage by spying for Russia for 22 years. Hanssen said that security was so lax at FBI headquarters that he never worried about being searched. He combed the FBI's computer system to obtain and disseminate over 6,000 classified documents and even to check whether he was under suspicion. He was quoted as saying "Any clerk in the bureau could come up with stuff on that system. It was pathetic." The FBI reportedly cancelled a classified computer system fearing Hanssen, a skilled computer programmer, might have planted malicious code or a back door into the system.

- John Rusnak, a once-promising currency trader for the U.S. branch of Allied Irish Banks, tried to conceal an estimated $691 million in trading losses in 2001 while simultaneously receiving bonuses of $100,000 to $200,000 on top of his $85,000 salary. This case closely mirrors that of Nick Leason, who lost over $ 1.4 billion and caused the collapse of England's Barings Bank in 1995.

- Frank Gruttadauria, a former Lehman Brothers Holdings, Inc., stockbroker manager, admitted in 2002 to bilking investors out of $277 million over the past 15 years. He simply shifted money from one account to another, systematically looting each one.

- Timothy Lloyd, a former New Jersey computer programmer for Omega Engineering Corporation, was convicted in May 2000 of causing about $12 million in damages. Before being fired in 1996, Lloyd planted a logic bomb that erased all Omega's contracts and the proprietary software used by the company's manufacturing tools. One Omega manager said that it would "never recover." Lloyd's actions also caused the layoff of 80 employees.

- Bill Conley, former president of U.S. Computer Corporation of Redmond, Washington, pled guilty to federal wire-fraud charges and agreed to pay Hewlett-Packard (HP) $1.5 million after admitting he had paid an HP employee to reveal competitors' bids on used computer servers, thereby enabling him to buy the equipment by submitting slightly higher bids.

- Five former security employees for Nordstrom were charged with stealing $140,000 by falsifying receipts and returns for cash at out-of-state stores.

- Two former Lucent Technologies scientists, Hai Lin and Kai Xu, and an accomplice, Yong-Qing Cheng, were charged with stealing trade secrets from Lucent and selling them for $1.2 million to a Chinese company. The three formed a joint venture with a Chinese government-owned company called Datang Telecom Technology Co., Ltd., of Bejing.
- Aaron Blosser, an obsessed contract computer consultant for Qwest, was charged in 1998 with hacking into the U.S. West (now Qwest) computer system and diverting 10.63 years of processing power from 2,585 computers toward his effort to solve a 350-year old math problem of finding a new prime number.
- Martin Frankel bilked insurance companies in five states out of over $200 million. He pled guilty to 20 counts of wire fraud and various other crimes under the Racketeering Influenced Corrupt Organizations (RICO) Act.

Organizations must also work in harmony with applicable governmental agencies so that offenders can be charged, and any necessary changes can be made to applicable laws and regulations. In extreme cases, such cooperation could even help military leaders determine where to deploy support.

Another constant hurdle is that internal and external IS developers continue to program applications with weak security. There will continue to be new systems that allow minimum password lengths to be under eight characters, that fail to have password expiration, that do not have logging capabilities, that do not provide sufficient encryption of passwords and other critical information, that allow concurrent sign-on by no system administrators, and that do not provide automatic session time-outs. Security continues to be an afterthought for these developers. We as IS control and security professionals must be constantly on the lookout for these types of systems. Too often, management in information systems and end-user areas falsely presume that the developers always design adequate IS security features into their applications.

Since the culture and operational practices of each organization and within each country are different, it is up to the internal and external auditors of all organizations to ensure that management is aware of the IS risks mentioned in this book, any risks that are unique to their organizations and countries, and the new risks posed by emerging technologies and terrorism. Once risks are identified, internal controls can be tailored to mitigate them and to result in healthy and thriving IS environments within their organizations, as well as a safer world for all of us.

9.3 SELF-ASSESSMENT QUESTIONS

Q.1 Write a detailed note on the IS auditing technologies.
Q.2 What risks are associated with IS auditing? Describe.

9.4. ACTIVITIES

Enlist new emerging technologies related to IS auditing.

9.5 REFERENCES

Forster, P. K. (1994). Accounting Profession in Australia, Revised; Professional Accounting in Foreign Country Series.

Gendron, Y., & Barrett, M. (2004). Professionalization in action: Accountants' attempt at building a network of support for the WebTrust Seal of Assurance. *Contemporary Accounting Research*, *21*(3), 563-602.

Markham, S., Cangelosi, J., & Carson, M. (2005). Marketing by CPAs: Issues with the American Institute of Certified Public Accountants. *Services Marketing Quarterly*, *26*(3), 71-82.

Pathak, J. (2005). *Information technology auditing*. Springer-Verlag Berlin Heidelberg.

Rahman, A. A. L. A., Islam, S., & Ameer, A. N. (2015, May). Measuring sustainability for an effective Information System audit from a public organization perspective. In *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* (pp. 42-51). IEEE.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Sayana, S. A. (2003). Approach to auditing network security. *Information Systems Control Journal*, *5*, 21-23.

Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, *14*(1), 43.