Auditing and Security
AS/400, NT, Unix, Networks, and Disaster Recovery Plans

YUSUFALI F. MUSAJI
Auditing and Security
Auditing and Security
AS/400, NT, UNIX, Networks, and Disaster Recovery Plans

Yusufali F. Musaji

John Wiley & Sons, Inc.
New York • Chichester • Weinheim • Brisbane • Singapore • Toronto
DEDICATION

This book is dedicated to my grandmother, Mrs. Kulumbai Nurbhai, who taught me to sacrifice so I could grow.

To my mother, Mrs. Fatima Musaji, who sacrificed her material well-being so I could pay my school fees.

To my son, Ali Musaji, who taught me perseverance, patience, and the marvels of life.

To my wife, Naomi Musaji, for her love, tolerance, and faith.
Because information technology is a combination of science and arts, auditing information systems requires knowledge of many disciplines. Management science, computer science, information security, accounting, finance, business, and human resources are just a few of the physical, intellectual, and emotional energies one would need to effectively undertake the job.

Before one begins to study the aspects of auditing information technology, one needs an understanding of the most advanced platforms with an idea of their scope. The management of information technology, including the motivation and mobilization of the necessary human resources, is the cornerstone for any information technology audit. Once we begin to grasp the hardware and operating system connections and the management of information systems, we can concentrate on the networks that enable the interconnection of all these platforms and the applications for the logistics and deployment of information technology. Finally, a review of the disaster recovery plan is needed since without it there is the imminent danger that the utility of information technology may never reach its full potential.

Chapter 1 introduces the auditor to the overall structure of the management of Information Security (IS) and to the considerations that apply to the dynamic company’s need for IS manager/leaders. These IS manager/leaders are change agents committed to the transformation to a dynamic culture and who inspire that commitment in others. IS manager/leaders need to understand the big picture, see their roles within it, continuously improve their skills, and coach and mentor others’ learning. They need to know how and when to lead, manage, and do. Consequently, they become role models for a dynamic company’s core values.

Chapter 2 discusses the Physical Safeguarding or Physical Security of information technology resources and reiterates the age old adage: Security Is a Management Issue . . . Not a Technological One!

In the heyday of the mainframe, physical and logical security were synonymous in that they were both viewed as significant. This was because the mainframe was huge and there was no question of where the information was processed. As computers evolved (paradoxically computers became more powerful as they became smaller in size), and with the emergence of networking capabilities, logical security became more significant and physical security became more obscure. In part, because logical security required technical expertise and computer resources could be accessed remotely, computer owners concentrated on logical security to protect their resources. However, in trying to protect computer
resources from hackers and computer thieves, corporations neglected the physical security aspects and as a result suffered financial loss from lack of physical security controls, thus becoming easy game for crooks. In spite of this, physical security continued to be regarded as being limited to the perimeter controls and bodyguards at the front doors.

Theft or damage to information processing resources, unauthorized disclosure or erasure of proprietary information, and interruption of support for proprietary business processes are all risks that managers who own or are responsible for information resources must evaluate. Since physical access to information processing resources exposes a company to all of these risks, management must institute physical access controls that are commensurate with the risk and potential loss to the company.

The objective of the physical security audit is to determine if management processes have been implemented, are effective, and are in compliance with established instructions and standards as formulated in the company security policy. Do they ensure that the company’s information resources are protected from unauthorized access or loss?

Chapters 3, 4, 5, and 6 discuss auditing the most advanced platforms: AS/400, Microsoft NT, and Unix.

Why are system concepts and architecture important to understand? Business leaders do not start by choosing a computer platform. They start by choosing an application that fits their business needs. Because of this, the computer system is very often considered first.

Why should the computer architecture matter? The accelerating rate of change of both hardware and software technologies necessitates that the system selected has been designed with the future in mind. Do the platforms accommodate inevitable, rapid, and dramatic technology changes with minimum relative effort? Are the systems future-oriented? Paradoxically, the characteristic of the most advanced design and technology is subtle. It accommodates the rapidly changing hardware and software components—permitting one to fully exploit the latest technologies.

Is the operating system conceived as a single entity? Are the facilities such as relational database, communications and networking capabilities, online help, and so on fully integrated into the operating system and the machine?

Successful audits of computer platforms are intended to provide an analysis of the computing and network hardware components with potential risks and recommendations. If the computing platform is not secure, neither is the company’s data.

Chapter 7 continues the discussion of auditing networks. Corporations deploy networks to lower the total cost of network ownership, maximize their return on investment, provide seamless, enterprise-wide services, enable applications, enhance their performance, control network resources, speed up project implementation, and minimize risk and complexity.

Driven by the rush to e-commerce, security has rapidly become a mission-critical component of the corporate IT infrastructure. By protecting these mission-critical networks from corruption and intrusion, network security has enabled new business applications by reducing risk and providing a foundation for expanding business with intranet, extranet, and electronic commerce applications.

Therefore, network security should be a continuous cycle, consisting of establishing a security policy that defines the security goals of the enterprise, implementing security in a comprehensive and layered approach, and auditing the network on a recurring basis to ensure that good network security is easier and more cost-effective. Also, network security should ensure that no irregularities have developed as the network evolves, and the results of the audits should be used to modify the security policy and the technology implementation as needed.
Chapter 8 discusses auditing the disaster recovery plan. Large pools of shared databases, time-sharing, vast teleprocessing networks, telecommunications connections to non-company facilities, multiple distributed printers and systems, and thousands of users characterize the state-of-the-art computer centers in corporations. Disruption of service or the intentional or inadvertent destruction of data could potentially bring business processes to a halt.

Across this entire computer infrastructure, the Information Security (IS) processes must be implemented to ensure the confidentiality, integrity, and availability of the company's information assets. The responsibility for the implementation of an effective IS program is assigned according to the company's goals and objectives. Generally, this responsibility is delegated to the information system because of its traditional role as Provider of Service. However, IS is often not the Provider of Service for smaller systems that exist at a location. Regardless of the organizational roles and responsibilities, the corporate information officer (CIO) is responsible for the overall implementation.

With the emergence of disaster recovery planning, physical security is regarded as the cornerstone to developing a viable disaster recovery plan. The pundits have suddenly proclaimed "Eureka," and the dawn of physical security as the foundation on which the disaster recovery plan can be built has begun to take hold. Protecting assets from disasters is now one edge of a double-edged sword with the other edge preventing losses from theft and human errors, which in fact pays partly if not wholly for the costs of disaster recovery planning. The auditor must ensure that the computing environments supporting vital business processes are recoverable in the event of a disaster.

Auditing and Security has been developed for IT managers, IT operations management, and practitioners and students of IT audit. The intent of this book is to highlight the primary areas of computer controls and to present them to the reader in a practical and pragmatic manner. Each chapter contains usable audit programs and control methods that can be readily applied to information technology audits. As an added value, two presentations are available on the World Wide Web. The first presentation is a proposal for investing in a disaster recovery plan and the second is a firewall selection guide. Please visit www.wiley.com/musaji. The user password is: auditing. These documents are in Powerpoint format.