soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Information Security
In
Business Applications

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدي

Prof. Ahmad Abdel-Salam Abu-Musa
PhD Aberdeen University, UK
Professor of Accounting Information Systems,
Vice Dean for Education and Students Affaires;
Faculty of Commerce, Tanta University, Egypt.

30006101601571 30006101601571 30006101601571

2022

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

سليمان طارق شبل ابراهيم السعدنى

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Preface

The main focus of this textbook is to introduce the basic information related to the information security. It introduces the nature and main characteristics of information security policies, security threats, and security controls, as well as information security governance in business organizations.

The current textbook is written in response to numerous calls from BIS students to write a simple textbook to enhance the body of knowledge concerned with information security which covers the scientific material of this course. There is a shortage of textbooks which introduces the information security in business applications, and this book represents a substantial step in that direction. This textbook addresses the concept of information security and its main components in an attempt to clarify confusion in that area. Through theoretical conceptualization of information and systems security, an integrated theoretical framework of information security which includes security objectives, threats and controls has been developed. The current textbook focuses on evaluating the security of information rather than the security of specific information technology products and accounting software: therefore it contributes to filling a vacuum left by the dearth of empirical study in this research area.

2021/2022 2021/2022 2021/2022

From a practical standpoint, students, managers and practitioners alike stand to gain from this book. It enables managers and practitioners to better secure their information and to champion information technology development for success of the business. The authors mainly depend of the following references for the material provided in this textbook:

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Abu-Musa, Ahmad A. (2010), "Information Security Governance in Saudi Organizations: An Empirical Study", ***Information Management & Computer Security***, Bradford, Vol. 18, No. 4, pp. 226-276.

Abu-Musa, Ahmad A. (2010), “Investigating Adequacy of Security Controls is Saudi Banking Sector: An Empirical Study”, ***Journal of Accounting, Business & Management (JABM),*** Vol. 17, No. 1, PP. 1- 40.

Abu-Musa, Ahmad A. (2008), “Information Technology and its Implications for Internal Auditing: Empirical study on Saudi Organizations”, ***Managerial Auditing Journal,*** Vol. 23, No. 5, pp. 438- 466.

Abu-Musa, Ahmad A. (2007), “Exploring Information Technology Governance (ITG) in Developing Countries: AN Empirical Study” ***The International Journal of Digital Accounting Research,*** Vol. 7, Iss.13-14, pp. 71-120.

Abu-Musa, Ahmad A. (2006), **“**Perceived Security Threats of Computerized Information Systems in the Egyptian Banking Industry”, ***Journal of Information Systems***, Vol. 20, Iss.1, PP. 189 -205.

Abu-Musa, Ahmad A. (2006), "Exploring Perceived Threats of CAIS in Developing Countries: The Case of Saudi Arabia", ***The Journal of Managerial Auditing, UK,*** Vol. 21, Iss.6, pp. 487- 407.

Abu-Musa, Ahmad A. (2004), “Investigating the Security Policies of Computerized Accounting Information Systems in the Banking Industry of an Emerging Economy: The Case of Egypt”, ***The Review of Business Information Systems***, summer, Vol. 8. Number 3; PP. 83-102.

سليمان طارق شلبي ابراهيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Abu-Musa, Ahmad A. (2003), "The Perceived Threats to the Security of Computerized Accounting Information Systems", ***The Journal of American Academy of Business, Cambridge, USA,*** Vol. 3, No.1, September, pp. 9- 20.

Abu-Musa, Ahmad A. (2002), "Security of Computerized Accounting Information Systems: An Integrated Evaluation Approach", ***Journal of American Academy of Business, Cambridge, USA***, Vol. 2. No.1 September 2002, pp. 141-149.

However, the complete reference list used for preparing the material of this textbook is presented at the end of the last chapter of this textbook.

The Author

Alexandria, January 10, 2020

سليمان طارق شبل ابراهيم السعدنى

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

سليمان طارق شبل ابراهيم السعدنى

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

TABLE OF CONTENTS

Chapter One: Information Security: Concept, Importance and Objectives

Chapter Two: Information Security Threats

سليمان طارق شبل ابراهيم السعيدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

سليمان طارق شبل ابراهيم السعيدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

سليمان طارق شبل ابراهيم السعيدى

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Chapter Five:
Information Security Governance

سليمان طارق شبل ابراهيم السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Chapter One
Information Security:
Concept, Importance and Objectives

1-1. Introduction

In this chapter, the concept and the meaning of information security will be presented. The importance of the issue of information security as a significant element for an organization's success and survival will be discussed. The security objectives of information and its main components will be highlighted; information principles security will be briefly mentioned; and finally, an integrated approach to information security will be presented.

1-2. The Importance of Information Security Topic

In recent years, the popular accounting press has begun publishing regular columns reviewing computer hardware and software for all types of accounting applications. It is apparent that the nature of recording, reviewing and safeguarding accounting information is changing rapidly and this makes the job of accountants, auditors, or accounting professors more challenging. Further, more and more articles are appearing in these publications discussing security methods for the new technologies. As accounting systems become more sophisticated and more readily available to all types and sizes of businesses, the need to understand and employ adequate systems security becomes an issue no business owner can ignore (Henry, 1997).

2021/2022 2021/2022 2021/2022
سليمان طارق شلبى ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

From Harris and Sidwell's (1994) point of view, security of computerized systems is a broad concept, encompassing not only the consideration for privacy and keeping information secret (confidentiality), but also the issues of system integrity and availability.

Therefore, the need to preserve the accuracy of information and the integrity of data transactions and to ensure the continued availability or continuity of services of the system should be also considered in preserving security. Conversely, threats to system security can threaten the integrity and accuracy as well as the availability of that system and its data (p. 548).

Eloff et al. (1993) argued that information security appears on the list of critical success factors of most major organizations. It has become apparent, from discussions at international conferences on information security, that the main areas of interest today are network security, disaster recovery planning, and risk analysis. These areas have been identified by the industry itself on the bias of its needs (p. 597).

Loch et al. (1992) confirmed that the security of information systems remains high on the list of key issues facing information systems executives. Traditional security concerns range from forced entry to computer and storage rooms, to destruction by fire, earthquake, flood, and hurricane. Recent attention focuses on protecting information systems and data from accidental or intentional unauthorized access, disclosure, modification, or destruction (p. 173).

Information has become one of the most valuable assets of the corporation which must be protected with care and concern, because business continuity and success are heavily dependent upon the integrity and continued availability of critical

سليمان طارق شبل ابراهيم السعيد
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

information. The reliance on information and rapidly changing technology forces organizations to implement comprehensive information security programs and procedures to protect their information assets. The success of implementing a security program relies largely on security awareness and compliance by employees (Lee, 1995).

From the point of view of Goodhue et al. (1991) the awareness of potential security problems is one of the major considerations for many organizations. It is expected that individuals who are more aware of the potential for abuse against their information would be more sensitized to the dangers of inadequate security and would be more likely feel that security was unsatisfactory. It is also expected that greater awareness of potential abuse would lead to more concern about security and to perceptions that the environment was less satisfactory.

The failure to secure the organization's information or to make it available when it is required to those who need it can, and does, lead to great financial losses. For example:

- More than one in every two respondents to Ernst and Young’s information security survey said that their organizations had experienced financial loss due to the lack of information security. Seventeen respondents reported losses in excess of $1 million (Info. World Canada, 1995).
- Mau and Catlin (1993) state that American businesses lose over $ 550 million annually due to computer based crime.
- Feeney (1993) suggests that although it is difficult to quantify the exact extent of damage from computer fraud in the American businesses, estimates range up to several billion dollars per year.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Meall (1992) has argued that accurate estimates of the overall costs of computer misuse in the UK are difficult to come by, but that various figures put the annual cost at somewhere between £ 400 million and £ 2 billion.
- The National Computing Centre (NCC), with support from ICL, conducted a survey based on more than 900 responses from information technology managers. According to the survey results, more than a half of UK organizations had suffered a significant security breach during the previous 5 years. The survey provides a thorough assessment of the likely effects of these breaches on organizations of various sizes and within various industry sectors. The survey further highlights the following:
  1. The cost to UK industry is estimated at just over £1.1 billion annually.
  2. Physical breaches cost £ 580 million annually.
  3. More than 50 percent of those respondents suffering a physical breach had no contingency plan in place.
  4. Some 75 percent of the respondents had not yet changed their disciplinary measures in the light of the computer misuse act.
  5. More than 80 percent of the respondents failed to even measure the costs associated with the computer breach (EDPACS, 1992).
- Rockwell (1990) reports that businesses are having difficulty in protecting information and preventing computer-related crimes. In the US, annual losses from computer-related fraud total $300 million, with an estimated potential annual loss of $40 billion. Much crime

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

goes undetected and victimized companies often absorb losses rather than admit to poor security.

- Irregularities and fraud are of much concern to managers, accountants and auditors. Computer fraud alone is estimated to amount over $6 billion a year in the US (Doost, 1990).
- Recent Home Office estimates put the cost of computer-related crime at between £400 million and £ 1.5 billion a year (Corbitt, 1996).
- One of the main findings of the information security survey conducted in 2000 by KPMG's Information Risk Management practice is that security breaches are raising.

The number of security breaches reported has risen in all areas since 1998. Of particular note is the increase from 20 percent to 74 percent of reported virus incidents. In addition, theft of equipment has risen from 23 percent to 46 percent, and email intrusion from 2 percent to 29 percent. More organizations now have formal reporting of security breaches (KPMG, 2000).

2021/2022 2021/2022 2021/2022

The financial losses from abuse of information security are very significant when it is considered that many security breaches and computer frauds are not publicly reported. Meall (1993) comments that many firms are reluctant to involve the police, even when computer-related fraud is discovered and the perpetrator identified. Firms believe that a prosecution, and the publicity it would attract, would indicate a weakness in their business system to shareholders, potential customers and competitors. Thus, unreported security losses and computer fraud represent an important aspect of the problem. The information security losses would be even more serious if unpublished financial losses were included.

سليمان طارق شبل ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Over recent years, changes in technology and the continuous decline in prices have made computer use easier and more widespread. Accordingly, many organizations were motivated to computerize their accounting systems or at least to move towards doing so.

Henry (1997) confirmed that the steady decline in the price of the information technology and the increasing availability of “off the shelf” accounting software have led more and more businesses of any size to automate all or part of their accounting functions. Further, in an effort to be extremely “user friendly”, accounting software requires little knowledge of accounting to be put to effective use. It is doubtful that such users would have direct knowledge of security issues in accounting systems. They must be made aware of potential security problems and solutions by the accounting, auditing or tax professionals they may occasionally consult.

User-friendly systems also create significant risks related to the security and integrity of computer and communication systems, data, and management information. West and Zoladz (1993) state that, although computers provide many benefits, inherent computer security issues are not often addressed by management. Many organizations do not realize the importance of computer security until some unauthorized modification to a payroll file, or some other event, occurs. Because information might be an organization's most valuable asset, leaving it without protection is tantamount to underinsuring fixed assets or inventory.

2021/2022 2021/2022 2021/2022

Organizations can no longer afford to ignore the importance of information security in the light of computer fraud, hackers and computer viruses. Davis (1996) states that drastic

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

changes in computer technology are occurring with greater frequency than ever before and many of these changes are being adapted into organizations' accounting information systems. With these ethnological advancements, however, come new security concerns for information systems auditor which should be considered. Since information security is a major concern for information systems auditors, Davis attempted to explore some of security issues in practice by replicating the work done by Loch et al. (1992). The results of Davis' survey revealed a high perception of information security threats. Moreover, most respondents recognized that different computing environments (microcomputer; minicomputer, mainframe and network computer) have relatively different levels of security risks.

A great number of security vulnerabilities arise in the process of using today's business computing and communication systems. Some of them are the result of natural disasters and others arise from human error, mischief, carelessness or intentional acts. Schweitzer (1987) considered the intentional act as the most serious problem, especially internal acts, since most such cases (95 percent) involve the organization's own employees.

McIntyre (1991) stated that security threats to an organization's information are now too well documented to be ignored. Yet many organizations still fail to take computer security seriously enough. The "it can't happen here" attitude is still alive in many organizations.

Davis (1996) stated that it is an accepted fact that new technology increases the security risks in accounting information systems. Even with all the advances in security measures, there remains the risk associated with the humans who use and

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

implement these measures. The respondents of his survey had ranked a human factor as one of the top threats to information security.

It is argued that computer security encompasses several disparate problems, potentially demanding different measures to solve them. These problems range from simple misuse, through software piracy, to the most dramatic and serious risk, that of theft or destruction of confidential and vital company information. Whether accidental, intentional, or plain malicious, abuse of computer resources can cause disruption at best, and serious financial loss, even bankruptcy, at worst (Weingartner and Burton, 1991, p. 33).

From reviewing the previous literature, it seems that developed countries pay more attention to the information security issues comparing with the developing countries, although the former still suffer from computer crimes and security abuse.

Although implementing adequate security controls over information has become an essential requirement, which is imposed by law and regulations in many developed countries, it seems that most developing countries are still suffering from insufficient understanding and inadequate awareness of security issues. Moreover, it seems that there is a lack of established laws and regulations concerned with computers crimes and security abuse, as well as inappropriate legal actions against the security perpetrators.

An organization using information should employ adequate safeguards and sufficient security controls to protect their assets, regardless of existence of any rules or regulations. In the absence of legal obligations, regulation comments, issued

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعيدي

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

security standards and significant positive management motivations towards information security issues, it is expected that only a minority of Egyptian organizations (including financial institutions) will voluntarily adopt and implement formal information security programmers.

In the USA, the Privacy Act of 1974 and the 1974 Office of Management and Budget Circular A-71 impose computer security requirements on federal government agencies (Parker, 1981, p. 97). The American Department of Defense has issued the "Orange Book" series. This contains 17 documents that provide a comprehensive set of guidelines both for people introducing computer security measures and for companies developing secure computer systems and products.

In addition, The Advisory Committee for the Co-ordination of Information Systems (ACCIS) (1992) has issued "Information System Security Guidelines for the United Nation Organizations". This book aims to provide assistance to managers in the United Nations organization who are looking for adequate and cost effective security for their information systems.

2021/2022 2021/2022 2021/2022

In the UK, "The Code of Practice for Information Security Management" was published in late 1993. Later, this code of practice was transformed into a standard (The British Standard BS 7799). The main objective of both initiatives is to provide a common basis for companies to develop, implement and measure effective security management. In addition, there is the Data Protection Act, issued in 1987 and revised in 1998. Weingartner and Burton (1990) argued that the UK's Data Protection Act forced every computer user in the UK to think twice about the information they stored. The Data Protection Act aimed to

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

prevent the misuse of information and make company directors accountable for its security.

In Germany, The German Accounting Information Security Agency (Zentralstelle fur sicherheit in der informationstechnik) published in July 1989 its "Criteria for the Evaluation of Trustworthiness of information Technology Systems" (for more details, see Roux, 1991, P. 61).

In most developing countries (such as Egypt) as far as is known to the researcher, there are no similar professional security standards, settled legal acts and regulations related to information security and computer crime. Most organizations in developing countries still consider the cost of implementing information security programs as an unnecessary overhead cost that should be reduced to the minimum. Moreover, in many organizations, information security might not be considered in managers' performance evaluation.

Although computers can be found in most organizations in developing countries, manual accounting information systems are still being taught in most university classes. Moreover, where there is exposure to information, it is at the introductory level only. In most cases it is presented in one chapter within an auditing course. The chapter will be theoretically taught, with no applications or handout computer work to simulate practice. Most students and graduates might not be sufficiently aware, even of simple accounting applications and software. The majority of available textbooks might not be well enough prepared to produce well-educated graduates, who are able to deal with practical problems. Students are learning to memories, rather than to analyze and use logical reasoning to solve practical problems.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

According to the above discussion, it seems that although the conversion from manual accounting information systems (MAIS) to information achieves many advantages to an organization regarding the speed and accuracy of data processing as well as the variety of accounting reports obtained, on the other hand, this radical change and fast development in technology might create some problems related to preserving the security of information.

Therefore, converting to information creates new challenges regarding protecting these systems and the information that they contain against various security threats and vulnerabilities.

The security status of information needs to be evaluated continually, to determine the security gaps and weaknesses and to prescribe and adopt the appropriate security controls. Thus, enhancing the security awareness among an organization's staff and employees has become an important issue.

It is observed that the objectives and components of information might differ from one person to another. Some terms such as “security”, “information security”, “information systems security” and even “computer security” are used interchangeably in the literature to mean the same thing. Moreover, most of the literature treats security problems as technical problems; no considerable effort was directed to the organizational and human aspect of these problems.

It seems also that there is no clear cut off line between security threats and security controls; in many cases, the lack of security controls were treated as security threats. Furthermore, the information security issues have been treated in a piecemeal rather than in a rounded- “integrated”- fashion. Moreover, the

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

very few studies concerned with evaluating the security of information were actually trials to evaluate IT products and computer software, rather than the information themselves.

Kay (1994) assents that security is an important issue because the majority of today's operating systems were developed without any consideration for security. Most of the operating systems either offer no security capabilities whatsoever, or security and controls features were tacked as an afterthought. Software systems designed from the ground up with security as an important consideration are only now beginning to appear (p. 165).

The availability, integrity and confidentiality of data and information resources are vital for an organization's survival and success, and they need to be protected by all employees. Information security presents the issues of confidentiality, integrity and availability. Therefore, management must educate employees to think about information security in business terms, which means making its computer users focus on activities that add value to the organization.

There is a real need for management to develop and implement effective security procedures to protect business information and company resources, and make sure the employees comply with regulations. Lee (1996) recommended that management should make efforts to implement security measures that are as employee-friendly as possible, so that employees treat security controls as part of their job and adhere to them with minimal intrusion (p. 20). Henry (1997) argued that discussions of security issues in accounting press do not manifest themselves in actual practice.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1-3. The Concept of Information Security

Parker (1981) mentioned that "Security is an ill-defined term in the technical literature. It has been used to denote protection and well being of political entities, as in the term "national security". It may also refer to industrial protection by the security or protection departments. Police forces having limited responsibilities are also sometimes called security forces. The standard lexical definition equates security with freedom from danger, fear, anxiety, uncertainty, economic vicissitudes, and so forth" (p. 39).

Granat (1998) argued that the term "security" might mean different things to different people. To some of them it is a concern for preserving the "data" integrity of existing database records into the new millennium; to others, it is securing privacy for proprietary and restricted information; to yet others, it means preserving original records and protecting their integrity.

The International Information Technology Guidelines issued by the International Federation of Accountants (IFAC) in 1998 stated that, "The concept of security applies to all information. Security relates to the protection of valuable assets against loss, disclosure and damage. In this context, valuable assets are data and information recorded, processed, stored, shared, transmitted, or retrieved from electronic media. The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure".

2021/2022 2021/2022 2021/2022

However, most of the literature defines information security as the protection of information confidentiality, integrity and availability. This definition is used as equivalent to "prevention against security breach". Accordingly, information

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

security could be also defined as "the prevention of the unauthorized disclosure, modification or withholding of information". For example, Marro (1995) defined information security as: "the protection of, and recovery from unauthorized disruption, modification, disclosure or use of information and information resources, whether accidental or deliberate".

Joy and Bank (1992) defined the security of an information system as: "the ability to ensure that only legitimate, authorized transactions and / or data are input to, and output from, a system with no unauthorized, illegitimate insertions, deletions, modifications or repays occurring between the time of input, and the time of receipt by the intended recipient".

Reviewing the available literature, it seems that there is some confusion regarding the terms "security", "information security" and "information systems security". Most of the previous literature used these terms interchangeably to mean the protection of information confidentiality, integrity and availability in an organization. According to the information security glossary, however, there are clear distinctions between the terms "Security"; "Information Security"; "IT System Security"; and "Information Systems Security". "Security" is defined as "the protection of information availability, integrity and confidentiality". This definition is exactly equivalent to both "the prevention of a breach of security" and "the prevention of the unauthorized disclosure, modification or withholding of information". According to this glossary, the term security is used here in the sense in which it is most commonly used in military and government circles (ftp://ftp.cordis.lu/pub/infosec/docs/s2001en.txt).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

The term “Information Security” is defined as “the combination of confidentiality, validity, authenticity, integrity and information availability”. Therefore, the term “Information Security” is not as wide as “Information Systems Security”, since it does not address the security issues related to the protection of the facilities used in handling information. However, it addresses all the other security issues associated with the protection of the information (information availability, integrity, confidentiality, authenticity and validity); and is thereby wider than the definition of “security”, which is designed to cover the principal concerns of the military and government sectors (confidentiality, integrity and availability, but not validity or authenticity) (see: ftp://ftp.cordis.lu/pub/infosec/docs/s2001en.txt).

On the other hand, the term “IT System Security” could be defined as “the combination of system availability and of the information security of the software and associated parameters forming part of the IT system itself”. Finally, “Information Systems Security” is defined as “the combination of information security and IT system security for a given information system”. Therefore, the term “information systems security” is the widest in meaning of this set of terms, covering all aspects of the security of the information and data handled by the information system, as well as the IT resources themselves (including software and associated control tables). The definition covers all aspects of security relevant to an information system (see, again, ftp://ftp.cordis.lu/pub/infosec/docs/s2001en.txt).

Although protecting data / information should be considered regardless of the nature of the accounting information systems (manual, computerized), the vast majority of authors and researchers have used the term “information system security” as

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

an equivalent to computer security or computerized information system security. Jenkins et al. (1992) mentioned that “computer security, or information system security, is a term used to cover the security of all the information processed by an organization's computer system, and of the equipment and facilities used to process the information. Therefore, the security of computerized information systems means that, data is processed completely and accurately, that access is restricted to appropriate people and that the computer facilities, and the information they hold, are available at all required times. These three elements of security are referred to as integrity, confidentiality, and availability”.

Thus The Security of Information should be regarded as an integrated part of an overall information security system in an organization (other systems being, *inter alia*, the purchasing information system, marketing information system, production information system, financial information system, or the managerial information system). In the next section the importance of and the real need for sound and appropriate security of information will be highlighted.

2021/2022 2021/2022 2021/2022

1-4. The Need for Information Security

Information security has become one of the most important issues of information in most organizations, since their survival and success depends in large extent on the confidentiality, accuracy, integrity, and availability of their critical and sensitive information. Most recent surveys show that information security is ranked high in the list of critical success factors in the majority of organizations.

The Organization for Economic Co-operation and Development (OECD, 1992) also confirmed that the explosive

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعيد

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

growth in use of information systems for all manner of applications in all parts of life has made provision of proper security essential. Security of information systems is an international matter, because information systems themselves often cross national boundaries and the issues to which they give rise may most effectively be resolved by international consultation and co-operation.

In February 1992, the OECD, through the Committee of Information, Computer and Communication Policy (ICCP), approved guidelines for the security of information systems. The guidelines provide a foundation from which countries and the private sector, acting singly and in concert, may construct a framework for security of information systems. The framework includes laws, codes of conduct, technical measures, management and user practices, and public education and awareness activities. These guidelines are intended to serve as a benchmark against which governments, the public sector, the private sector and society may measure their progress.

2021/2022 2021/2022 2021/2022

The above information systems security guidelines have been issued recognizing the following points:

- The increasing use and value of “information systems” which involve computers, communication facilities, computer and communication networks; and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance.
- The international nature of information systems and their world-wide proliferation.
- The increasingly significant role of information systems and the growing dependence on them in national and

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

international economies and trade and in social, cultural and political life call for special efforts to foster confidence in information systems.

- In the absence of appropriate safeguards, data and information in computerized information systems acquire a distinct sensitivity and vulnerability as compared with paper documents, due to risks arising from available means of unauthorized access, use, misappropriation, alteration, and destruction;
- There is a need to raise awareness of risks to information systems and of the safeguards available to meet those risks.
- The present measures, practices, procedures and institutions might not adequately meet the challenges posed by information systems and by the concomitant need for clarity, predictability, certainty, and uniformity of rights and obligations, of the enforcement of rights, and of recourse and redress for any violation of rights relating to information systems and the security of information systems.
- Greater international co-ordination and co-operation is desirable in meeting the challenges posed by information systems, the potential detrimental effects of a lack of co-ordination and co-operation on national and international economies and trade, on participation in social, cultural and political life and the common interest in promoting the security of information systems.

Regarding the importance of information security in organizations, the Comptroller of the Currency Administrator of National Banks (1998) revealed that “Information, regardless of

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

its source, is a valuable asset to the bank; its accuracy and confidentiality is essential to the business. Accordingly, it must be protected from abuse such as inadvertent or intentional misuse, disclosure, fraud, and error. Information systems, both data and software that creates and stores that data, must be secured". The practical needs for securing an organization's information will be covered in the following sub-sections:

1-4-1. New Technology Creates New Risks

Jenkins et al. (1992) argued that for all information systems, whether computerized or non-computerized, there is always security risk. However, computerized information systems are more likely to have greater security risks as a result of the following factors:

- The physical concentration of data processing and storage in one or a small number of locations. As a result the disruption of a relatively small physical unit can have a disproportionate effect on the general data processing of the organization.
- The complexity of computer processing. This leads to a concentration, in the hands of a relatively small number of people, of the knowledge of a company's computer system, and thus of the ability to create and modify it.
- The development of networks to provide real-time and on-line systems where remote users communicate directly with centralized, distributed and local data processing facilities.
- The use of computers to carry out processes which cannot easily be performed by manual systems. This increases the dependence on computers in performing many accounting

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

tasks. Therefore, a dangerous situation could result if such systems and data processing were interrupted, especially in cases where alternative manual procedures were not available.

- The scale of operation of many computer systems, while providing greater reliability, speed and accuracy, together with the large scale and inter-connected nature of modern systems, also introduces the risk that processing failure will have a more significant and widespread effect than failure in a corresponding manual system.
- In the move towards the "paper-less office", businesses are increasingly relying on computers, rather than paper documents, to initiate and record transactions (pp. 512-513).

Clay (1995) argued that there is a huge hole in the data security of many corporations. Mission-critical applications could be damaged intentionally by virus programs or innocently by well-intentioned employees (p. 27).

2021/2022 2021/2022 2021/2022

Again, the Comptroller of the Currency Administrator of National Banks (1998) mentioned that data are created and stored in substantial volume, often representing millions of bank records and transactions. Correspondence and bank strategies also are created and stored though text processing. Bank and customer funds are routinely transferred via computerized payment networks. Transmission of such data regularly occurs over public communication links, such as telephone lines and satellites. In addition, many users, including employees and organization customers, can directly access the data through computer terminals or telephones. Some of them have the ability to change information or create new data. These activities, while improving

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

customer services and internal operations, have also increased the risk of error and abuse of organization information.

1-4-2. Information Security Issues are not Seriously Addressed by Management

West and Zoladz (1993) declared that security issues of information are not often addressed by management. Many organizations do not realize the importance of their information security until an unauthorized modification to payroll files or some other event occurs. Since information has become one of the most valuable organization's assets, leaving it unprotected is tantamount to underinsuring fixed assets or inventory. Organizations can no longer afford to ignore the importance of computerized information system security in light of computer fraud, hackers, and computer viruses.

1-4-3. The Globalization of Computer Crime

2021/2022 2021/2022 2021/2022

Computer crime is almost inevitable in any organization unless adequate protections are put in place. Since traditional mechanisms of financial control are usually insufficient to guard against these sophisticated crimes, the computer controller must get involved. However, in addition to computer crime, controllers also need to worry about the growing computer virus problem. Some virus attacks are directly associated with computer crime attacks.

While technically skilled hackers and others from outside the company can be quite dangerous, potentially more dangerous criminals are authorized users committing unauthorized acts (Shriven, 1991).

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Sherizen (1992) confirmed that the computer crime problem is no longer a local problem and that the security solution cannot be viewed only from national perspective. Computer crime and information security have expanded from relatively limited geographical boundaries to become global issues. This world-wide growth has very direct implications for information security management.

1-4-4. Security Breaches Leads to Great Financial and Non-Financial Losses

Safeguarding a organization's information has significant business implications. The loss or theft of customers' personal and financial information and the manipulation or unauthorized alterations of organization's records could lead to considerable financial or reputational losses to the organization.

In Williams' (1995) opinion, any type of security breach, however minor, can become disruptive and expensive: so it must make better business sense to take a preventive approach. Therefore the sooner an organization takes action to safeguard its information systems, the cheaper it will be for that organization in the long run.

1-4-5. Security Countermeasures Involve Additional Expense, Which might not Directly Generate Revenue

Dorey (1991) mentioned that, since security countermeasures always involve additional expenses and this expenditure does not directly generate revenue, it must be carefully considered. Wong (1993) argued that the objective of information security should not be to provide too much or too little security, but to go for the right level of security. Where

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

appropriate, one should explore ways to cost-justify security spending, based on potential business losses. The security framework should not be construed as an unproductive overhead. Prudent security practice should aim to add value to business applications by reducing fraud, cutting down on reworking, and ensuring a good and reliable service. Ultimately, he argued, good security equals good business management.

1-4-6. Many Organizations Do Not Introduce Appropriate Security Measures Until a Major Breach in Security Occurs

The total loss resulting from security breaches is unknown: public knowledge of security violations and resulting losses is often suppressed. This lack of information concerning the total cost and the number of actual incidents of security abuse may promote an erroneous level of comfort regarding system security. Many organizations do not introduce appropriate security measures until a major breach in security occurs (Ryan and Bordoloi, 1997, p. 138).

1-4-7. Information Security is needed to fulfill Some Legal Requirements

In many cases, information and data security should be implemented to fulfill legal acts and requirements. Dorey (1991) presented some examples of the minimum security requirements that have been defined by particular items of legislation in relation to the UK as follows:

- The Data Protection Act that requires personal data to be kept securely and confidentially. This implies that some

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

mechanisms must exist to authorize and control access to such data.

- The Companies Acts require the directors of the companies to ensure the security of their information exists, in order to provide accurate accounting information. For a computerized system, this has implications for the control of the integrity of accounting data.
- Specific industries, such as the financial services industry, have particular laws relating to their obligations. For example, the Bank of England's guidelines, arising from the
- Banking Act, make clear recommendations on the minimum requirement for the back-up and contingency of computer systems.
- Legal contracts made between the company and third parties may also have security implications. Many companies sign non-disclosure agreements where they agree to keep information strictly confidential. Other contracts may specify service level requirements, and may invoke penalty clauses if any systems become unavailable or if a service of sufficient quality and integrity cannot be offered. However, it is rare that these requirements are passed on to those determining security implementation.

2021/2022 2021/2022 2021/2022

Information systems professionals have always recognized the importance of security measures; however, with the increase of computer crime and abuse and the detailed recollections of underground networks, security is being elevated to a higher priority. The complexity of a firm's system and the nature of the data it maintains will dictate the level of security employed (Marro, 1995).

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعيدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Improved security of information systems, by enhancing the accuracy, completeness and availability of data and information in the information system and, accordingly, by increasing the ability to rely on data and information in the system, may assist the introduction and use of such evidence in legal and administrative proceedings (OECD, 1992).

1-4-8. Information Systems Security is an Essential Element for an Organization's Survival and Success.

The International Federation of Accountants (1998) raised the following points to emphasize the great importance and critical the need for information security:

- Organizations depend on timely, accurate, complete, valid, consistent, relevant, and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment.
- While there are many direct and indirect benefits from the use of computerized information systems, there are also many direct and indirect risks relating to those information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied.
- Security failures may result in both financial losses and / or intangible losses such as unauthorized disclosure of competitive or sensitive information.
- Threats of information systems may arise from intentional acts or unintentional acts and may come from internal or external sources. The threats may emanate from, among others, technical conditions (program bugs, disk crashes), human factors (lack of training, errors and omissions),

سليمان طارق عبد الرحيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

unauthorized access (hacking), or viruses. In addition to those, other threats, such as business dependencies (reliance on third party communications carriers, outsource operations) that can potentially result in a loss of management control and oversight are increasing in significance.

- Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss or embarrassment caused by security failures.

Ryan and Bordoloi (1997) confirmed that "Today's security managers must grapple with the challenge of developing a security strategy that achieves balance between security precautions and excessively costly measures. When managers do not implement adequate security measures, they place their organizations at risk" (p. 138).

Schweitzer (1987) argued that the conversion of information to electronic forms has changed the vulnerabilities of business information and has made the job of the security manager more complex. However, electronic information forms, if properly managed, could be made far more secure than manual or written forms. The use of computers has not, in itself, increased information risk; but if they are improperly implemented, computer systems can present critical exposures. Therefore, it would be more accurate to say that the use of computers has changed information vulnerabilities: the risks are more glamorous and more complex (p. 11).

Greengard (1998) recommended paying more attention to the growing risk related to information. Only a quarter-century ago, most organizations conducted the vast majority of their

2021/2022 2021/2022 2021/2022 30006101601571 30006101601571 30006101601571 سليمان طارق شبل ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

business on paper. Important files and documents containing sensitive information were usually kept under lock and key. Whenever something was sent to someone across the office or in another part of the country, a set of security precautions was almost always used. In most instances, a document was sealed and sent by courier or registered mail, with a signature required at the other end. Paper shredders helped ensure that sensitive documents did not appear in front of people who were not entitled to access and use this information. However, moving from paper-based systems to electronic data management has changed security entirely. Although breaches have always been part of the corporate landscape (a dishonest or inattentive employee presents a serious concern in any environment) digital data is far easier to duplicate and disseminate.

Information in all forms (mental, written, and electronic) is subject to three vulnerabilities (Table 3-1):

1- Information might be exposed to an unauthorized person.

2- Information might be destroyed or access to it denied.

3- Information might be changed in an unauthorized way.

2021/2022 2021/2022 2021/2022

For example, mental information can be denied if the person having the data leaves the company or refuses to reveal it; it can be lost if the person forgets it; and it can be changed if the processor decides to lie about the actual content. Written information can be denied if someone steals the document; it can be changed if a document is secretly rewritten; and it can be exposed if someone gives it to an unauthorized party. Electronic information can be exposed or modified through penetration of the computer system or network where it is stored or processed; service can be denied through the same process or as the result of physical attack (Schweitzer, 1987, p. 11).

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

(Table 1-1)

Security Threats in Different Accounting Information Systems

Security Threats	Mental	Written	Electronic
Destruction	• Memory Loss	• Fire • Misplacement • Theft of Paper	• Logical Attack • Erroneous Erasure • Fire • Theft of Media
Disclosure	• Talking • Publication	• Careless Handing • Trash • copying	• Careless display • Unauthorized Display • Penetration by Unauthorized Persons • Copying
Unauthorized Modification	• Falsification	• Re-creation • Copying; and Change	• Penetration by Unauthorized Persons • Carelessness • Errors

(Source: Adapted from Schweitzer, 1987)

In the next section, the main objectives of information security and its components will be discussed.

2021/2022 2021/2022 2021/2022

1-5. The Objectives of information Security

The International Federation of Accountants (1998) had stated the main objectives of information security as "the protection of the interests of those relying of information, and the information and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity". According to the International Federation of Accountants, the security objectives for an organization are achieved when:

- Information systems are available and usable when required (availability);

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Data and information are disclosed only to those who have a right to know it (confidentiality); and
- Data and information are protected against unauthorized modification (integrity).

However, the relative priority and significance of availability, confidentiality, and integrity vary according to the data within the information system and the business context in which it is used (IFAC, 1998).

The Organization for Economic Co-operation and Development (OECD, 1992) also confirmed that the objective of security of information systems is the protection of the interests of those relying on information systems, from harm resulting from failures of availability, confidentiality, and integrity. Therefore, security of information systems is the protection of availability, confidentiality and integrity, although the relative priority and significance of these three elements vary according to the information system.

Peltier (1994) believes that the general objectives of a comprehensive information security program should be to:

- Ensure the accuracy and integrity of data.
- Protect classified data.
- Protect against unauthorized access, modification, disclosure, or destruction of data.
- Ensure the ability of the organization to survive the loss of computing capacity (disaster recovery planning).
- Prevent employees from probing the security controls as they perform their assigned task.
- Ensure management support for development and implementation of security policies and procedures.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم الصعيدى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Protect management from charges of imprudence in the event of any compromise of the organization's information or computer security controls.
- Protect against errors and omissions (p. 7).

Stahi (1993) considers the main goals of an information security program are to achieve the:

- Privacy of information stored and processed in computer and communications system;
- Integrity of information stored and processed in computer and communications system;
- Availability of information stored and processed in computer and communications system;
- Detection and control of privacy, integrity and denial of service violations (p. 117).

However, from Stahi's point of view there are no systems that can assuredly provide complete protection. Consequently, information security must be viewed in the context of an organization's business or other mission. This means that, in the case of business, for example, a fundamental decision, regarding how much security is appropriate, and what the organization is willing to pay to achieve it, must be approached from a business perspective. This means the organization must, to be the greatest extent possible, have firm measures of its risks, its vulnerabilities and the cost-effectiveness of potential countermeasures.

Again, Ryan and Bordoloi (1997) confirmed that the goal of information security is to ensure the availability of information and information processing resources, and to provide means to establish and retain the integrity and confidentiality of information within the system (p. 138). According to The Institute for Certification of Computer Professionals (ICCP), the

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

fundamental security objectives of information are: Integrity; Confidentiality; Reliability; Availability; Authentication and Functionality

Fried (1994) stated that information security is concerned with protecting: the availability of information and information processing resources, and the integrity and confidentiality of information. He argued that unless adequate protection is in place when new business applications are developed, one or both of these characteristics of information security may be threatened (p. 57).

The Comptroller of the Currency Administrator of National Banks (1988) mentioned that various processes are available to strengthen information security in the banks. The most fundamental requirement is sound, written management policies for internal controls.

These include physical security, separation of duties, quality controls, hardware and software access controls and audit. Therefore, information security controls should be designed to:

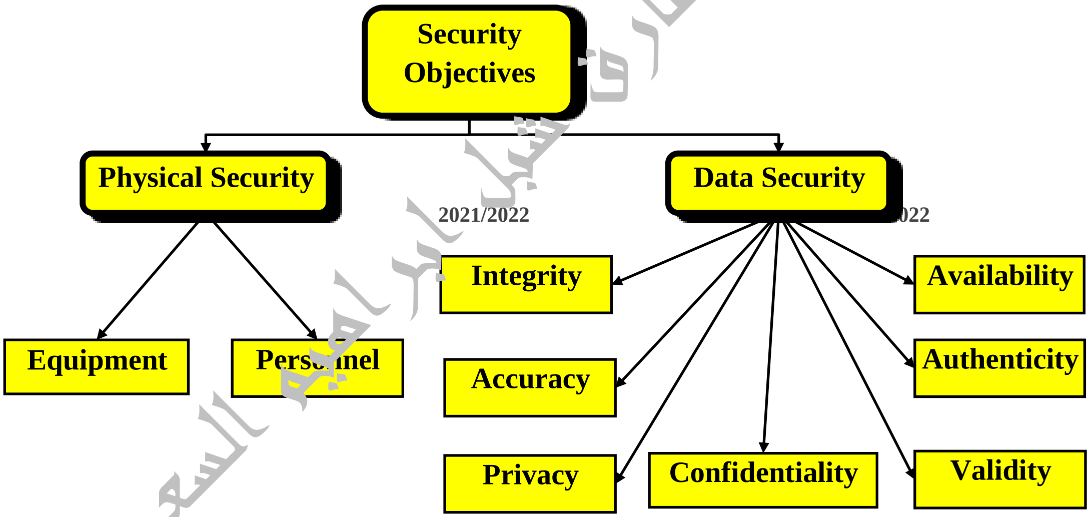
2021/2022 2021/2022 2021/2022

- Ensure the integrity and accuracy of management information systems,
- Prevent unauthorized alteration during data creation, transfer, and storage,
- Maintain confidentiality,
- Restrict physical access,
- Authenticate user access,
- Verify accuracy of processing during input and output
- Maintain backup and recovery capability,
- Provide environmental protection against information damage or destruction.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

In reviewing this literature, it seems that there has been some confusion regarding the objectives and the components of information systems security. While there is agreement that confidentiality, integrity and availability are the main objectives of information security, there is considerable argument regarding the inclusion of accuracy, privacy, validity and authenticity of information among the main objectives and essential components of information security. Moreover, little attention has been directed to the security of information systems themselves, as used to record, process, store and produce data, as well as the IT resources and facilities actually used in handling data. Physical security and data/ information security are the two fundamental elements of information security.



(Figure 1-1)
(The Objectives of information Security)

In the following parts, the researcher will briefly highlight the main components of physical security, data and information security as the two principal areas of information security

سليمان طارق شبل ابراهيم السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1-5-1. Physical Security

As argued earlier, the security of information systems involves the protection of information as well as the computerized systems used to record, process, and store these information, in addition to all other facilities and personnel involved in handling these information. Baskerville (1988) stated that “It would be an understandable misconception to believe that the physical protection of computing resources is the central focus of computer security. While it is the physical aspects of computer security, which are the most readily apparent, these represent only one class of security elements. Still, physical security is often the “first line of defense” raised in the protection of computer systems” (p. 11).

1-5-1-1. Equipment and Facilities Security

An organization’s computerized accounting system should be protected against prospective damage and espionage arising from theft, fire, loss, or damage of its facilities. Protection should be extended to cover all the organization’s PCs, equipment, disks, system manuals, accounting records and files and output forms such as organization check-books, Visa cards or Smart Cards, in addition to secure the necessary environmental conditioning machinery such as heating, cooling, dehumidifying, ventilating and lighting associated with the computerized information systems.

2021/2022 2021/2022 2021/2022

1- 5-1-2. Personnel Security

Well-educated and trained employees are a valuable human resource, which can play an important role in the success and survival of an organization. Therefore, these valuable assets

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

should be protected and secured. Baskerville (1988) again argued that “The tremendous degree of training and expertise required in the operators, technical engineers, programmers, analysts and administrators in computer information systems has increased in a critical nature of protecting these individuals as an essential asset to the organization.

Two major aspects in protecting personnel must be considered from the organization's viewpoint. Of course the primary concern is the safety of the staff: personnel must be protected from injury. However, loss of personnel due to dissatisfaction is also a threat.

Heavy employee turnover can disrupt system development projects and the routine operation or maintenance of existing systems” (p. 11). Accordingly, information security system should have the ability to protect honest employees from the illegal acts of dishonest employees, by implementing security counter measures and through accountability for actions. Every employee should be responsible and accountable for their actions and their specified duties.

2021/2022 2021/2022 2021/2022

1-5-2. Data and Information Security

Data and information security are the central concern of information security. The information owned by an organization has become recognized as a vital element for its survival and success. Therefore, the ultimate objective of any information security policy should be to protect the integrity, availability, and confidentiality of the electronic data and information held within an organization's information. Harris and Sidwell (1994) suggested that “Preserving availability and integrity are themselves important security considerations, especially in

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

commercial business environments where they may sometimes outweigh the importance of preserving confidentiality" (p. 548).

In the following sections the researcher will discuss the confidentiality, integrity, availability, privacy, authenticity, and accuracy of information as the main components and qualities of information systems security.

1-5-2-1. Confidentiality

Confidentiality is one of the principal components of information security. Confidentiality could be defined as the avoidance of the disclosure of information without the permission of its owner. Unauthorized disclosure of information covers any disclosure other than to authorized users, at the authorized times and in the authorized manner. Confidentiality is not strictly a property of the information itself. After a loss of confidentiality, the information is unchanged and it would be impossible to determine by any means of inspection that confidentiality had indeed been lost. Once lost, confidentiality cannot easily be regained (ftp://ftp.cordis.lu/pub/infosec/docs/s 2001en. txt).

Again, both OECD (1992) and The International Federation of Accountants (1998) stated that "confidentiality means the characteristic of data and information being disclosed only to authorized persons, entities, and processes at authorized times and in an authorized manner".

Jenkins et al. (1992) confirmed that confidential information must be protected no matter what the form it is in. It will be necessary to consider data, whether input, output, stored, transmitted along communication links or displayed on a screen (p. 515).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Kulczycki (1997) argued that ten years ago, the theft of 1,000 pages of confidential information would have required the use of a small handcart. Today, advances in electronic and computer technology have made these data more powerful, easier to store and manipulate; and, therefore, more easily slipped into a shirt pocket, copied, mailed, or maliciously damaged while in place.

1-5-2-2. Integrity

The concept of data integrity means the avoidance of the unauthorized modification or alteration of information. Integrity ensures that information is added to, altered or deleted only by authorized users. Integrity is regarded as indeed a property of the information itself.

It is also interesting to note that, although integrity prevents the intentional and accidental additions, alterations or deletions of information by unauthorized users, it does not guarantee that such modifications have been performed by authorized users (people or entities), or according the information owner's wish. According to the glossary of information systems security, "integrity does not therefore address the content of the modifications, but merely who can undertake them. Integrity is therefore less all embracing than authenticity. Integrity is a necessary, but insufficient condition to preserve the authenticity of information" (for more details see: ftp://ftp.cordis.lu/pub/ infosec/docs/ s2001en.txt).

Baskerville (1988) stated that an organization must be protected from perils arising from missing, incomplete, or inconsistent data. Therefore, from his point of view the term integrity is used to mean preservation of the data from corruption

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

or loss (p. 12). According to List (1994) the integrity of information means that "information is sufficiently right at the time of use for the purpose to which the user wishes to put the output" (p. 295).

Integrity is one of the most important characteristics of information security. Jenkins et al. (1992) confirmed that integrity is about ensuring that information is complete, not duplicated, accurate, authorized and kept secure. Integrity is considered first because it is perhaps the most familiar to the auditor (p. 514). The International Federation of Accountants (1998) confirmed the previous point of view by stating that "Integrity means the characteristic of data / information being accurate and complete and the preservation of accuracy and completeness by protecting the data and information from unauthorized, unanticipated, or unintentional modification".

1-5-2-3. Availability

2021/2022 2021/2022 2021/2022

Information availability is one of the main components of information systems security. Information availability could be defined as the avoidance of the temporary or permanent withholding of information from those users who have received authorization to access and use it. In other words, information availability ensures that authorized users can access and use information (that they have received authorization to access and use it) in the authorized manner at the authorized times.

Information availability and confidentiality seem to be complementary concepts. While information availability ensures that individuals who are authorized to access and use specified information can do so, information confidentiality ensures that

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

individuals who are not authorized to access and use certain information are prevented from accessing and using it.

However, a violation of information availability could occur due to the following reasons:

- The information system could fail to recognize that an authorized user does indeed have authorization;
- The IT system could itself have suffered a violation of system availability, such as through breakdown;
- Loss of integrity could be regarded as a special example of a violation of information availability, where the information no longer exists in the required form.

According to the OECD (1992) and The International Federation of Accountants (1998), information availability means the characteristic of data, information and information systems being accessible and useable on a timely basis in the required manner. Again, it should be noted that information availability is not strictly a property of the information itself. The term relates to what can be done with the information.

2021/2022 2021/2022 2021/2022

For Jenkins et al. (1992), information availability indicates that information should be accessible when it is required. The major aspects of "availability" are described below:

- ***Response time****:* The response time is the delay between pressing the "enter" or "return" key on a terminal and obtaining a response back from the computer (an error or confirmation that the transaction has been accepted).
- ***Back-up procedures:*** All parts of a system require regular back-up in case they are lost or damaged. Potentially this includes data, application software and system software; although in practice software packages and system software

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

may be standard and a replacement therefore easily obtainable from the original suppliers.

- ***Fallback arrangement:*** A fallback arrangement is needed to offer an alternative means of operation if the normal computer system in not usable, for some reason such as a fire. Fallback arrangements can range in sophistication from a paper-based manual operation to a complete duplication data centre, which can be "switched in" at a moment's notice.
- ***Redundancy / resilience:*** It is desirable, wherever possible; to design ***the*** hardware configuration such that loss of one component is tolerable. For example, if three computers are linked together in a ring rather than a line, loss of any one link will not prevent them from communicating with one another. If several disk drives are used, then two disk controllers rather than one will allow at least some of the disk drivers to be usable if one controller fails (p. 516).

Jenkins et al. (1992) commented, "Availability requirements will vary considerably according to the type of system. These requirements may also vary with time in any particular system. For example, response or turnaround time may become quite critical for a general ledger or consolidation system at the financial year-end, whereas process control systems are likely to have very high availability requirements at all times. Availability requirements need to be considered from the user's perspective. If response time exceeds a certain level, for example, the user may consider the system to be unavailable since it is of no practical use. The assumptions made in setting up fallback arrangements such as the order of priorities in application system reinstatement, or the length of time before systems are working again must be understood and agreed by the users" (p. 516).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Based on the above discussion, the availability of accounting systems means that these systems are accessible to authorized users and usable by them in the authorized manner at the authorized times. In other words, the availability of accounting systems means the avoidance of unacceptable delay in obtaining authorized access to information or IT resources.

Information availability should consider the aspect of timeliness in achieving access to the information or the IT resources. However, what constitutes an “unacceptable” delay will depend upon circumstances. In some cases, merely a slowed response time may be considered unacceptable (for example, several seconds on a foreign exchange dealing system, or within an air traffic control system). The notion of “delay” includes the permanent withholding of information or resources as well (for more details, ftp://ftp.cordis.lu/pub/infosec/docs/s2001en.txt).

1-5-2-4. Validity

The validity of information could be defined as “the total accuracy and completeness of information. This definition and the concept behind it should be compared and contrasted with the related concepts of information integrity and authenticity”.

However, it is now common for many groups of users to have only read access to a particular information system. Therefore, such users have no direct influence on integrity or authenticity but they are extremely concerned with validity of information. According to the information security glossary, the difference between validity and the sum of integrity and authenticity arises where the priorities of the information owner (responsible for updating the information) and the user (responsible for exploiting it) are different.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعيد

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

However, different users may have different criteria for acceptable timeliness in the update of information. For example, a foreign exchange dealer requires financial information to be up to the second but a tax advisor requires it to be up to the day. In this example a system could have validity for the second group while lacking it for the first.

1-5-2-5. Authenticity

Authenticity means the avoidance of a lack of completeness or accuracy in authorized modifications to data and Information. Authenticity is concerned solely with use of the system in the authorized manner, such as with updates through which the intended information flows. It includes an element of timeliness, in that adequate completeness requires the system to be updated before decisions are made on the basis of stored information. It also addresses some aspects of illegitimate usage, in that fraudulent transactions could be entered by an authorized user in the authorized manner without breaching integrity. In this case they would not have authenticity.

According to the information security glossary, authenticity has previously been regarded as part of integrity, but the two concepts, while linked, are complementary. Integrity is necessary to preserve authenticity. However, integrity does not ensure that the modifications carried out by authorized users are in themselves accurate and complete. Violations of authenticity and integrity have a similar impact as far as the information owner is concerned.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1-5-2-6. Privacy

Parker (1981) mentioned that "Security, confidentiality, and privacy are often confused. For example the term or "computer privacy" is often incorrectly used to mean computer security. Privacy, however, refers to a social issue involving a human right and is not to be confused with security. Confidentiality is the state of being private and secret.

Confidentiality is established in relation to particular classification of data and a corresponding set of rules authorizing and limiting collection, dissemination, and storage of data. In other words, privacy is assured by imposing rules of confidentiality for the use of personal data that are safeguarded by security actions and functions" .

According to Baskerville (1988) an organization should be protected against prospective threats arising from the exposure of its data to unauthorized parties. Privacy has become of great concern as more and more confidential personal information is being kept about the general population in society's computer systems. However, in this context, the concept includes the privacy of all data from costly disclosure (p. 12).

The Comptroller of the Currency Administrator of National Bank has recommended the following safeguards to improve privacy of customer information at banks and credit unions:

1. Give accountholders better passwords (abandon Social Security numbers and mothers' maiden names),
2. Routinely test security systems by calling employees and trying to obtain confidential member information.
3. Hire outsiders to conduct pretext-calling tests (Thompson, 1999).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1-5-2-7. Accuracy

Accuracy refers to the maintenance of the data's legitimate relationship to what it represents. The accuracy of data and information are essential in controlling the organization. Data accuracy is also essential in protecting the assets of the organization.

For example, inaccurate calculating of an account's interest or the due dates of a bank's loans, as well as making decisions according to inaccurate data and information, could lead to great financial and non-financial losses.

Harris and Sidwell (1994) mentioned that security in IT systems is a broad concept, encompassing not only the consideration for privacy and keeping information secret (confidentiality), but also the issues of system integrity and availability. The need to preserve the accuracy of information and integrity of data transactions can fall under the need to preserve security. The need to ensure the continued availability or continuity of services of the system can also be a security consideration. Conversely, threats to a system's security can threaten the integrity and accuracy as well as the availability of that system and its data (p. 548).

2021/2022 2021/2022 2021/2022

1-6. The Main Principles of Information Security

The information systems security objectives should be supported by ten major security principles. These main principles of information systems security are: accountability, awareness, multidisciplinary, cost effectiveness, integration, reassessment, timeliness, proportionality, democracy and social factors (see figure 1-2).

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1-6-1. Accountability: *Responsibility and Accountability must be Explicit*

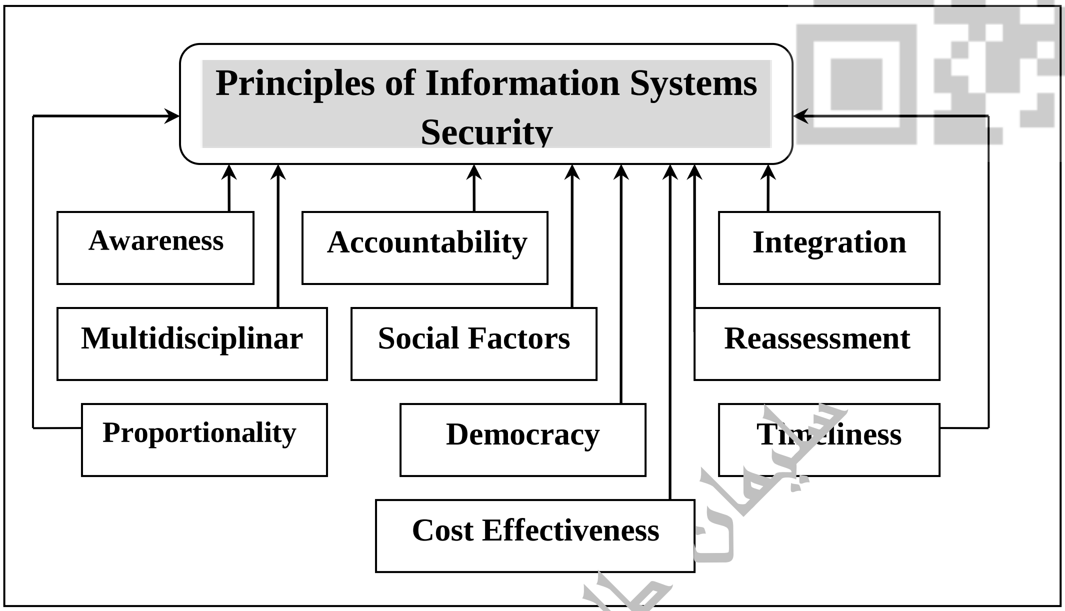
The International Federation of Accountants (1997) stated that security of information requires a specification and timely apportionment of responsibility and accountability among data owners, process owners, technology providers, and users. This accountability should be formalised and well communicated. The main issues that should be considered regarding responsibility and accountability include:

- The fundamental principles of information security will be briefly discussed in the following sections:
- Specification of ownership of data and information;
- Identification of users and others who access the system in a unique manner;
- Recording of activities through the provision of management audit trails;
- Assignment of responsibility for maintenance of data and information; and
- Institution of investigative and remedial procedures when a breach or attempted breach of the security objective occurs.

- Therefore, the security system should be able to associate each job or transaction with the person or department initiating the job. Provision should be made for each user to have a unique identifier, which enables the tracing of all attempted and unauthorized accesses to a particular individual. However, it should be noted that a user might be assigned more than one identifier, each with different attributes (Jenkins et al., 1992, p. 243).

سليمان طارق شكر ابراهيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg



(Figure 1-2)
(The Principles of Information Systems Security, Adapted from OECD, 1992 and IFAC, 1998)

2021/2022 2021/2022 2021/2022

According to the Advisory Committee for the Co-ordination of Information Systems (ACCIS) (1992) people will be less likely to make mistakes or be dishonest if they knew that they can, and will, be held accountable for their actions. Individual accountability can only be achieved if the system can uniquely identify people and keep detailed record of their actions.

1-6-2. Awareness: *Awareness of Risks and Security Initiatives must be Disseminated*

Individuals responsible for the organization should realize the complexity of the information security and the potential losses if the system is breached. Weiss (1990) argued that no computer security system would be effective unless corporate

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

management is willing to initiate user education programs, establish effective policies and enforce compliance.

The OECD (1992) mentioned that the lack of training and follow-up about security and its importance perpetuate ignorance about proper use of information systems. Without proper training, operators and users might not be aware of the potential for harm from system misuse. Poor security practices abound and operators and users might not take even the most rudimentary security measures.

The International Federation of Accountants (1997) suggested that “In order to foster confidence in information, data owners, process owners, technology providers, users, and other parties with a legitimate interest to learn or be informed, must be able to gain knowledge of the existence and general extent of the risks facing the organization and its systems and the organization's security initiatives and requirements. Security measures are only effective if all individuals involved in the process are aware of their proper functioning and of the risks they address”.

Issues that should be considered include the following:

- The level of detail disclosed must not compromise security;
- Appropriate knowledge should be available to all parties, not just to users, who have legitimate right to be informed;
- Awareness should be part of the induction program for new recruits to an organization so as to build security awareness as part of the corporate culture; and
- There should be recognition that maintaining security awareness is an on-going process (ibid.).

سليمان طارق شبل ابراهيم السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1-6-3. Multidisciplinary: *Security must be Addressed Taking into Consideration Both Technological and Non-Technological Issues*

According to the International Federation of Accountants (1997) security is more than just technology. It also covers administrative, organizational, operational, and legal issues. Accordingly, technical standards should be developed with, and, be reinforced by codes of practice, audit, legislative, legal and regulatory requirements, awareness, education and training. Issues to consider include:

- Business value or sensitivity of the information asset;
- Impact of the organizational and technological changes on the administration of security;
- Technologies that are available to meet the security objectives;
- Requirements of legislation and industry norms; and
- Requirements to carefully manage advanced security techniques.

The OECD (1992) suggested that when devising and maintaining measures, practices and procedures for the security of information systems, it is important to review the full spectrum of security needs and available security options. In an organization, for example, this would involve consultation with technical personnel, management, the legal department, users and others. All these groups would have different perspectives, requirements and resources that should be consulted and combined to produce an optimal level of security for the information system. Similarly, on a policy level, technical standards, codes of practice, legislation, public awareness,

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدي
30006101601571 30006101601571 30006101601571

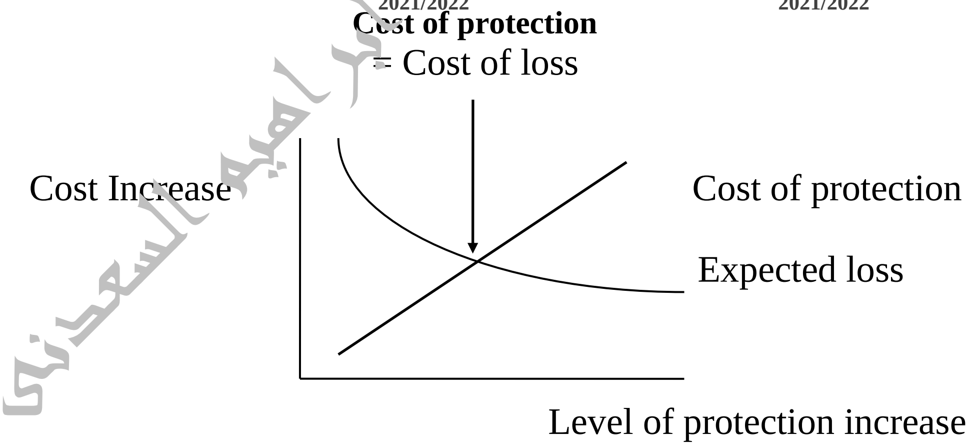
soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

education and training for security of information systems may be mutually reinforced.

1-6-4. Cost Effectiveness: *Security must be Cost-Effective*

Implementing information security measures and controls is not without cost. Rainer et al. (1991) argued that the cost of security measures should be weighed against their effectiveness in reducing risk. Since achieving 100 percent information systems security is impossible, managers must evaluate the choice of security measures. In general, any security measure or combination of such measures should not cost more than what it would cost to tolerate the problem addressed by the measure. The following figure indicates the trade-offs between increased costs and increased security measures. This figure also shows that there is some optimal point of trade-off between security and cost.

2021/2022 2021/2022 2021/2022



(Figure 1-3)

The Cost / Benefit Relationship of information Security

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

The OECD (1992) stated that the goals of information confidentiality, integrity and availability must be balanced against other organizational priorities, such as cost-efficiency, and against the negative consequences of security breaches. The cost must not exceed the benefit. Similarly, from the viewpoint of deterring those who would attempt to enter information systems to view, manipulate or obtain information, security controls should be sufficient to render the costs or the amount of time required greater than the possible value to be gained from the intrusion. Moreover, adequate measures for security of information systems help to ensure the smooth functioning of information systems.

Again, the International Federation of Accountants (1997) suggested that different levels and types of security might be required to address the risks to information. Security levels and associated costs must be compatible with the value of the information. The following issues should be considered:

- Value to and dependence of the organization on particular information assets;
- Value of the data or information itself, based on a pre-defined level of confidentiality or sensitivity;
- Threats to the information, including the severity and probability of such threats;
- Safeguards that will minimize or eliminate the threats, including the costs of implementing the safeguards;
- Costs and benefits of incremental increases to the level of security;
- Safeguards that will provide an optimum balance between the harm arising from a security breach and the costs associated with the safeguards; and

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Where available and appropriate, the benefit of adopting established minimum security safeguards as a cost-effective alternative to balancing costs and risks.

1-6-5. Integration: *Security must be Co-Ordinated and Integrated*

The OECD (1992) recommended that the security of information systems be considered when the system is being designed. Measures for security might be formulated and tested to avoid incompatibility. Overall costs of security may also be reduced. Security is required at all phases of the information cycle: gathering, creating, processing, storing, transmitting and deleting. Therefore, the security of the system may be determined by the weakest point in the system.

The Advisory Committee for the Co-ordination of Information systems (ACCIS) (1992) recommended that information system security planning should be an integrated part of overall corporate planning. The security program should identify the security measures that are necessary to safeguard the part that information systems play in the achievement of corporate objectives. The security policy should provide a framework for the security program, to ensure that it reflects corporate policy. The security policy should be endorsed by the head of the organization (p. 1).

The International Federation of Accountants (1997) stated that "Measures, practices, and procedures for the security of information should be co-ordinate and integrated with each other and with other measures, practices, and procedures of the organization, and third parties on whom the organization's business processes depend, so as to create a coherent system of

سليمان طارق شبل ابراهيم السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

security. This requires that all levels of the information cycle - gathering, recording, processing, storing, sharing, transmitting, retrieving and deleting are covered".

According to the International Federation of Accountants (1997) the following security issues should be considered:

- Security policy and management included as an integral part of the overall management of the organization;
- Concurrent development of security systems with information systems; or, at least, harmonization of all security processes to provide a consistent security framework;
- Review of inter-related systems to ensure that the level of security is compatible; and
- Third party risks on which the organization's business processes depend.

1-6-6. Reassessment: *Security must be Reassessed Periodically*

2021/2022 2021/2022 2021/2022

This principle recognizes that information systems are dynamic. System technology and users, the data and information in the system and, accordingly, the security requirements of the system are ever changing. Information systems, their value, and the severity, probability and extent of potential harm should, therefore, undergo periodic reassessment.

Follow-up is as important as implementation, especially in light of new technological developments, whether those adopted by the system owner or those available for use by others (OECD, 1992).

According to the International Federation of Accountants (1997) the security of information systems should be reassessed periodically, as information systems and the requirements for

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

their security vary over time. Issues that should be considered include:

- Increase in dependence on information systems, requiring an upgrade to the business continuity plans and arrangements;
- Changes to information systems and their infrastructure;
- New threats to information systems, requiring better safeguards;
- Emerging security technologies, providing more cost effective safeguards than were earlier possible; and
- Different business focus, organizational structure, or legislation, necessitating change in the existing level of security.

1-6-7. Timeliness: *Security Procedures must Provide for Monitoring and Timely Response*

In the modern environment where interconnected information systems span the globe, the importance of time and place are diminished. It is possible to gain access to information systems regardless of physical location. The timeliness principle acknowledges that, due to the interconnected and transborder nature of information systems and the potential for damage to systems to occur rapidly, parties may need to act together swiftly to meet challenges to the security of information systems. Depending upon the security breach, the relevant parties might be members of the public and private sectors and may be located in different countries or jurisdictions. This principle recognizes the need for the public and private sectors to establish mechanisms and procedures for rapid and effective co-operation in response to serious security breaches (OECD, 1992).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

The International Federation of Accountants (1997) confirmed that organizations must establish procedures to monitor and respond to real or attempted breaches in security in a timely manner and in proportion with the risk. The increasingly interconnected real-time and trans-border nature of information and the potential for damage to occur rapidly require that organizations react swiftly. Issues to consider include:

- The instantaneous and irrevocable character of business transactions;
- The volume of information generated from the increasingly interconnected and complex information systems;
- Automated tools to support real-time and after-the-fact monitoring; and Expediency of escalating breaches to the appropriate decision making level.

1-6-5-8. Social Factors: *Ethics must be Promoted by Respecting the Rights and Interests of Others*

2021/2022 2021/2022 2021/2022

Information and the security of information should be provided and used in such a manner that the rights and interests of others are respected. The level of security must be consistent with the use and flow of information that is the hallmark of a democratic society.

According to the International Federation of Accountants (IFAC, 1998), the following issues should be considered here:

- Ethical use and/or disclosure of data or information obtained from others;
- Fair presentation of the data or information to users; and
- Secure destruction of data or information that is sensitive but no longer required.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Again, OECD (1992) argued that information systems pervade our societies and cultures. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information systems. This principle supports the development of social norms in these areas. Important aspects are the expression of these norms to all members of society and inculcation of these concepts from a very young age.

1-6-9. Proportionality

Not every information system requires maximum security. Just as it is important that systems be sufficiently secure, so is it futile to provide security beyond the reasonable requirements of the system. Rather, there is a hierarchy of information systems and their security needs that differs for each organization. For this reason, there is no unique security solution (OECD, 1992).

Therefore, in assessing security needs, the information at risk should be first identified and its value should be estimated. Possible security measures, practices and procedures available to protect the various elements of the information system should be enumerated and the costs of implementing and maintaining each of these security options should be calculated. The level and type of security should then be weighed against the severity and probability of harm and its costs, as well as the cost of the security measures. This analysis should be carried out for the information system in the context of all other relevant procedures and systems, including other information systems (OECD, 1992).

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1-6-10. Democracy

The security interests of owners, developers, operators and users of information systems must be weighed against the legitimate interests in the use and flow of information, with the aim of striking a balance in accordance with the principles of a democratic society.

Those unfamiliar with security of information systems might presuppose that security of information systems might lead only to restrictions to access to and movement of data and information. On the contrary, security may enhance access and flow of data and information by providing more accurate, reliable and available systems. For example, harmonization of technical security standards could help to prevent data and information islands and other barriers to data and information flows (OECD, 1992). In the next section, an integrated approach to information security will be presented.

2021/2022 2021/2022 2021/2022

1-7. An Integrated Approach to Information Security

The main security objectives could be achieved through adopting adequate security controls which comply with generally accepted information security principles. In addition, an ongoing and integrated security approach should be implemented. Executive management support is an essential element for the successful development, design, implementation and monitoring of information security controls. The fundamental steps of developing an integrated security approach of information are illustrated in Figure 1-4.

In order to preserve adequate security of information, financial institutions should implement a sound information program that identifies, security measures, monitors and manages

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

the potential risk exposures. An effective information security program should implement an ongoing risk assessment of security threats and vulnerabilities surrounding the information.

The organization should consider the various measures available to support and enhance information security programs. The main elements of the integrated information security approach will be discussed in the following sub-sections.

1-7-1. Policy Development

The security objectives and principles could provide a framework for the organization's development of its security policy. The security policy should support and comply with the existing organizational polices. An information security policy statement is needed to make explicit the underlying value of, and dependence on, the information within the organization.

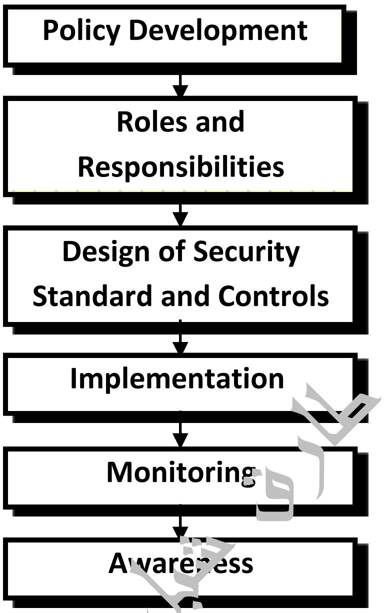
The security policy should concentrate on the importance of information security to the organization. Definitions of responsibilities and accountabilities for the information security, with appropriate separation of duties, should be clear and well published among the organization’s employees and other users of the organization’s information.

The Comptroller of the Currency Administration of National Banks (1988) confirmed that the Board of Directors should require that information security policies exist throughout the bank. These policies must be in writing and communicated to all personnel and other authorized users of bank information systems. Examiners may periodically target reviews of information security in the bank’s supervisory strategy. These reviews may include:

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- The adequate of the “corporate information security policy”;
- Compliance with the security standards and management’s supervision of these activities.


Policy Development
Roles and Responsibilities
Design of Security Standard and Controls
Implementation
Monitoring
Awareness

2021/2022 2021/2022 2021/2022

(Figure 1-4:“An Integrated Approach of information Security Adapted from IFAC, 1998)

1-7-2. Roles and Responsibilities

For information security purposes, the roles, responsibilities and authority in the organization should be clearly defined, communicated and understood by all the organization’s employees and staff. Each individual in the organization should be responsible and accountable for his or her actions.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1-7-3. Design of Security Controls

Once an organization’s information security policy has been approved by the organization’s management and related roles and responsibilities are clearly assigned, it is necessary to design and develop effective security controls to protect information against potential security threats.

When designing new or improved security standards, measures, practices and procedures for information systems, it is important to consider individual business requirements and the risks related to the particular system, in order to identify the specific security requirements. Assessment of the risks must include both business and technical risks and the analysis of security control objectives, standards, and techniques needed to provide an integrated information systems security control framework.

1-7-4. Implementation

2021/2022 2021/2022 2021/2022

Once the design of the security standards, practices and procedures have been approved by the organization’s management, the system should be implemented on a timely basis and then carefully maintained. According to the International Federation of Accountants, the security standards, practices and procedures should cover a number of subject areas:

- Managerial controls, such as span of control, separation of duties, background checks, and personnel awareness, training and education to ensure that personnel act appropriately to prevent, detect, or correct problems;
- Identification and authentication controls to establish accountability and to prevent unauthorized persons from

سليمان طارق شبل ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

gaining access to the systems through, for example, passwords and smart cards;

- Logical access controls to establish who or what has access to a specific type of information resources and the type of access permitted, such as read, write, update, or delete;
- Accountability controls through management audit trials that maintain a record of all user and system activity;
- Other controls, such as cryptography, over information transmitted and stored to ensure confidentiality, authenticity, integrity, and non-repudiation;
- System development life-cycle process controls to ensure that security is considered as an integral part of the process and explicitly considered during each phase of the process;
- Physical and environmental controls to ensure that routine but critical activities (user support, software support, change management, configuration management media controls, backups, documentation and maintenance) enhance the overall level of security; and
- Business continuity planning controls to ensure that an organization can prevent interruption and can recover and resume processing in the event of a partial or total interruption to information system availability (IFAC, 1998; Para., 29).

2021/2022 2021/2022 2021/2022

1-7-5. Monitoring

Monitoring of the implemented security measures and controls should be established to detect and correct security breaches. Actual and suspected information security breaches should be promptly identified, investigated, and acted upon,

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

ensuing ongoing compliance with policy, standards, and with minimum acceptable information systems security practices.

According to the Advisory Committee for the Co-ordination of Information Systems (ACCIS) (1992) the security controls and operating procedures in the security program should be based on the results of risk analysis and risk management. If the value of the assets protected, the threats facing the assets or the vulnerability of the asset to those threats changed, then the risk analysis should also be changed. Risk management involves selecting the most effective set of countermeasures from the different sets that could protect an asset from a given threat. If organizational or technological changes affect the relative costs of security countermeasures, then it may be that a different set of countermeasures should be introduced.

1-7-6. Awareness, Training and Education

The International Federation of Accountants (1998) stated that human factors are usually the major source of information security problems: “People are often the weakest link in securing information. Awareness of the need to protect information, training in the skills needed to operate information systems securely, and education in security measures and practices are of critical importance for the success of an organization's security program”. The overriding benefits of awareness, training and education are in improving employees’ behavior and attitudes towards information security and increasing the ability to hold employees accountable for their actions.

However, the success of implementing any information security program relies to a large degree on the level of security awareness and compliance by employees. Therefore, the

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

organization’s management should promote and enforce - if necessary - implementation of the information security program. The organization’s management should also motivate the employees to comply with the organization’s information security programs and procedures, to improve the information security posture.

Lee (1995) mentioned that information security should be regarded as an organizational problem. Thus, it is not only restricted to the information technology (IT) department. The function of an IT department is to implement the facilities, hardware or software for security; but the awareness, implementation, co-operation and execution of security depends on the awareness, co-operation and execution of every employee who has access to information or system within the organization.

The OECD (1992) stated that “In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems”.

2021/2022 2021/2022 2021/2022

1-8. Summary

In this chapter, the concepts of “security”, “information security” and “information system security” have been discussed. The concept of “information systems security” seems to be wider than that of “information security”, since it covers all the issues concerned with the information security (availability, integrity, confidentiality, authenticity, validity, privacy, and accuracy of information), in addition to preserving the other security aspects

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

related to the protection of the computer system itself and the facilities used to record, process and store that information. The objectives of information security and its main components have been highlighted. The main security principles of information were briefly addressed and finally, an integrated approach to information security has been introduced. In the next chapter, the perceived security threats that might face or challenge information security will be discussed.

سليمان طارق شبل ابراهيم السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Questions

1. Identify the type of information below that is least likely to be considered "sensitive" by an organization.
   a. financial statements
   b. legal documents
   c. strategic plans
   d. product cost information

2. Classification of confidential information is the responsibility of whom, according to COBIT5?
   a. external auditor
   b. information owner
   c. IT security professionals
   d. management

3. Which of the following is not one of the basic actions that an organization must take to preserve the confidentiality of sensitive information?
   a. identification of information to be protected
   b. backing up the information
   c. controlling access to the information
   d. training

4. Classification of confidential information is the responsibility of whom, according to COBIT5?
   a. external auditor
   b. information owner
   c. IT security professionals
   d. management

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعيدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

5. Encryption is a necessary part of which information security approach?
    a. defense in depth
    b. time based defense
    c. cloud quarantine
    d. synthetic defense

6. Information rights management software can do all of the following *except*
    a. limiting access to specific files.
    b. limit action privileges to a specific time period.
    c. authenticate individuals accessing information.
    d. specify the actions individuals granted access to information can perform.

7. Identify the first step in protecting the confidentiality of intellectual property below.
    a. Identifying who has access to the intellectual property
    b. Identifying the means necessary to protect the intellectual property
    c. Identifying the weaknesses surrounding the creation of the intellectual property
    d. Identifying what controls should be placed around the intellectual property

8. What confidentiality and security risk does using VoIP present to organizations?
    a. Internet e-mail communications can be intercepted.
    b. Internet photographs can be intercepted.
    c. Internet video can be intercepted.
    d. Internet voice conversations can be intercepted.

2021/2022 2021/2022 2021/2022

سليمان طارق شعبان ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

9. After the information that needs to be protected has been identified, what step should be completed next?
   a. The information needs to be placed in a secure, central area.
   b. The information needs to be encrypted.
   c. The information needs to be classified in terms of its value to the organization.
   d. The information needs to be depreciated.

10. Which of the following is *not* one of the 10 internationally recognized best practices for protecting the privacy of customers' personal information?
    a. Provide free credit report monitoring for customers.
    b. Inform customers of the option to opt-out of data collection and use of their personal information.
    c. Allow customers' browsers to decline to accept cookies.
    d. Utilize controls to prevent unauthorized access to, and disclosure of, customers' information.

2021/2022 2021/2022 2021/2022

11. In developing policies related to personal information about customers, Folding Squid Technologies adhered to the Trust Services framework. The standard applicable to these policies is
    a. security.
    b. confidentiality.
    c. privacy.
    d. availability.

سليمان طارق شبل ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

12. Which type of software blocks outgoing messages containing key words or phrases associated with an organization's sensitive data?
    a. anti-virus software
    b. data loss prevention software
    c. a digital watermark
    d. information rights software

13. A client approached Paxton Uffe and said, "Paxton, I need for my customers to make payments online using credit cards, but I want to make sure that the credit card data isn't intercepted. What do you suggest?" Paxton responded, "The most effective solution is to implement
    a. a data masking program."
    b. a virtual private network."
    c. a private cloud environment."
    d. an encryption system with digital signatures."

2021/2022 2021/2022 2021/2022

14. The first steps in protecting the privacy of personal information is to identify
    a. what sensitive information is possessed by the organization.
    b. where sensitive information is stored.
    c. who has access to sensitive information.
    d. All of the above are first steps in protecting privacy.

سليمان طارق شبل ابراهيم السعدى

15. It is impossible to encrypt information
    a. transmitted over the Internet.
    b. stored on a hard drive.
    c. printed on a report.
    d. None of the above

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

16. Data masking is also referred to as
    a. encryption.
    b. tokenization.
    c. captcha.
    d. cookies.

17. Identify the item below that is *not* a step you could take to prevent yourself from becoming a victim of identity theft.
    a. Shred all documents that contain your personal information.
    b. Only print your initial and last name on your personal checks.
    c. Do not place checks in your outgoing mail.
    d. Refuse to disclose your social security number to anyone or any organization.

18. These are used to create digital signatures.
    a. asymmetric encryption and hashing
    b. hashing and packet filtering
    c. packet filtering and encryption
    d. symmetric encryption and hashing

2021/2022 2021/2022 2021/2022

19. If an organization asks you to disclose your social security number, but decides to use it for a different purpose than the one stated in the organization's privacy policies, the organization has likely violated which of the Generally Accepted Privacy Principles?
    a. Collection
    b. Access
    c. Security
    d. Quality

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

20. All of the following are associated with asymmetric encryption *except*
    a. speed.
    b. private keys.
    c. public keys.
    d. no need for key exchange.

21. If an organization asks you to disclose your date of birth and your address, but refuses to let you review or correct the information you provided, the organization has likely violated which of the Generally Accepted Privacy Principles?
    a. Collection
    b. Access
    c. Security
    d. Choice and consent

22. If an organization asks you to disclose your date of birth and your address, but fails to take any steps to protect your private information, the organization has likely violated which of the Generally Accepted Privacy Principles?
    a. Collection
    b. Access
    c. Security
    d. Quality

23. An electronic document that certifies the identity of the owner of a particular public key.
    a. asymmetric encryption
    b. digital certificate
    c. digital signature
    d. public key

سليمان طارق شبل ابراهيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

24. If an organization asks you to disclose your date of birth and your address, but fails to establish any procedures for responding to customer complaints, the organization has likely violated which of the Generally Accepted Privacy Principles?
    a. Collection
    b. Access
    c. Security
    d. Monitoring and enforcement

25. The system and processes used to issue and manage asymmetric keys and digital certificates are known as
    a. asymmetric encryption.
    b. certificate authority.
    c. digital signature.
    d. public key infrastructure.

2021/2022 2021/2022 2021/2022

26. Identify one weakness of encryption below.
    a. Encrypted packets cannot be examined by a firewall.
    b. Encryption provides for both authentication and non-repudiation.
    c. Encryption protects the privacy of information during transmission.
    d. Encryption protects the confidentiality of information while in storage.

سليمان طارق شبل ابراهيم السعدنى

27. Using a combination of symmetric and asymmetric key encryption, Sofia Chiamaka sent a report to her home office in Bangalore, India. She received an e-mail acknowledgement that her report had been received, but a few minutes later she

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

received a second e-mail that contained a different hash total than the one associated with her report. This most likely explanation for this result is that

a. the public key had been compromised.
b. the private key had been compromised.
c. the symmetric encryption key had been compromised.
d. the asymmetric encryption key had been compromised.

28. Information encrypted with the creator's private key that is used to authenticate the sender is

a. asymmetric encryption.
b. digital certificate.
c. digital signature.
d. public key.

29.11) Which of the following is *not* one of the three important factors determining the strength of any encryption system?

a. key length
b. key management policies
c. encryption algorithm
d. privacy

2021/2022 2021/2022 2021/2022

30. Which of the following descriptions is *not* associated with symmetric encryption?

a. a shared secret key
b. faster encryption
c. lack of authentication
d. separate keys for each communication party

سليمان طارق عبد ابراهيم السعيدي

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

31. What is a denial of service attack?
    a. A denial of service attack occurs when the perpetrator sends hundreds of messages from randomly generated false addresses, overloading an Internet service provider's e-mail server.
    b. A denial of service attack occurs when an e-mail message is sent through a re-mailer, who removes the message headers making the message anonymous, then resends the message to selected addresses.
    c. A denial of service attack occurs when a cracker enters a system through an idle modem, captures the PC attached to the modem, and then gains access to the network to which it is connected.
    d. A denial of service attack occurs when the perpetrator e-mails the same message to everyone on one or more Usenet newsgroups LISTSERV lists.

32. Why are threats to accounting information systems increasing?
    a. Many companies do not realize that data security is crucial to their survival.
    b. LANs and client/server systems are easier to control than centralized, mainframe systems.
    c. Many companies believe that protecting information is a strategic requirement.
    d. Computer control problems are often overestimated and overly emphasized by management.

2021/2022 2021/2022 2021/2022

سليمان طارق شلبى ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Chapter Two:
Security Threats to Information

2-1. Introduction

In the previous chapter, the concept, objectives and principles of information security have been discussed. In this chapter a general overview of the information security threats will be presented, the different classifications of security threats will be outlined and causes of security violation will be briefly highlighted. Finally, the approaches and techniques of information security abuse will be discussed in some details.

2-2. Security Threats to Information: A General Overview

The rapid change in computer technology, the wide spread of user-friendly systems and the great desire of organizations to acquire and implement up-to-date computerized systems and software have made computers much easier to use and enabled accounting tasks to be accomplished much faster and accurate than hitherto. On the other hand, this advanced technology has also created significant risks related to ensuring the security and integrity of information. The technology, in many cases, has been developed faster than the advancement in control practices and has not been combined with similar development of the employees’ knowledge, skills, awareness, and compliance.

Parker (1983) argued that, according to Jackson’s law, anything hit with a big enough hammer would break! When it comes to computers, their facilities, storage media, computer programs, people, or data, the hammer need not be very large, because they are all fragile and becoming more so. In addition,

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعيدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

because of their great processing capabilities, the concentration of data and the speed of operation there are many possibilities to do harm in, to, or with a computer. These possibilities are also extended over great geographic distances by the increasing use of data communications capabilities that connect many computers and terminals in a network (p. 41).

Davis (1996) mentioned that great changes in computer technology are occurring with greater frequency than ever before, and many of these changes are being adopted into organizations' accounting information systems. These technological advancements have created new security threats to information. Davis developed a list of sixteen security threats to be investigated in the real world. The results of Davis' study have been discussed in chapter two.

Schweitzer (1987) considered the main security threats of electronic information to be:

- Loss of information privacy;
- Theft of information;
- Unauthorized use of information;
- Fraudulent use of information and computers;
- Loss of information integrity as a result of unauthorized intentional change or manipulation of data;
- Loss of computing services due to unauthorized or intentionally malicious actions.

Haugen and Selin (1999) classified the common types of computer-based fraud under the following six categories:

1. **Altering input:** Altering input does not require extensive computer skills; the perpetrators only need understand how the system operates to cover their tracks.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

2. **Theft of computer time:** Using a computer system for unauthorized purposes, such as running a personal business or keeping little league statistics, constitutes fraud, even though in many cases the individual is not aware that they are doing anything wrong.
3. **Software piracy:** It has been estimated that for every legal copy of software there are from one to five illegal copies, costing the software industry between $2 and 4 billion a year (Levi, 1993).
4. **Altering or stealing data files:** Data can be changed, deleted, scrambled or manipulated, often by disgruntled employees, to reduce value or eliminate derogatory impact. It can also be stolen or replicated and marketed to competitors, or to others that could gain a competitive advantage.
5. **Theft or misuse of computer output:** Local area networks expose computer-generated output to a larger audience with shared printers, usually maintained in a public location for ease of access. Desktop screens are often easily observable, and output sent through interoffice mail is subject to interception. The more sensitive the information contained on the output, the more care and control is needed.
6. **Unauthorized access to systems or networks:** With the proliferation of Internet usage, and the flexibility and ease of use found with most networked systems, care needs to be taken to restrict and protect sensitive files. Networks are particularly vulnerable to hackers taking advantage of the weak security provided for dial-in and remote access. In the next sections, the potential causes

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

of information security threats will be briefly highlighted.

2-3. The Causes of Information Security Violations

There are many internal and external forces which could cause security breach of information. Most of the internal reasons relate to internal employees and staff, who can access the organization's assets and accounting systems. Internal organizational and technical problems, such as poor internal controls, poor personnel policies and practices, and poor examples of honesty at the top levels of an organization are essential causes of security threats. They might include inadequate rewards and compensation plans, inadequate management controls, inadequate reinforcement and performance feedback mechanisms, inadequate support, inadequate operation reviews, lax enforcement of disciplinary rules, fostering of hostility and other motivational issues.

According to Haugen and Selin (1999) there are many reasons that might make employees commit computer crimes and steal from the business for which they work, the more common reasons being revenge, overwhelming personal debt, substance abuses and lack of internal controls. Business today is very competitive, and employees can feel very stressed. As a result, they have feelings of being overworked, underpaid and unappreciated.

2021/2022 2021/2022 2021/2022

If employees are also struggling with serious personal problems, their motivation to commit fraud may be very high. Add to the equation poor internal controls and readily available computer technology to assist in the crime, and the opportunity to commit fraud is now a reality. Assessing the risk to the organization of computer crime is sometimes difficult, but by

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

initiating a proper internal control system, including good employment practices and training programs, organizations can take a proactive stance in warding off computer crime and keep losses to a minimum level.

The following list of violation causes is based on the work of many experts in the field of electronic information security:

1. Inadequate or incomplete system design, which fails to provide effective checks and controls throughout the system's operating cycle. In manual systems, controls are self-evident; automated systems may fail to provide replacement controls and procedures. In too many cases, applications systems are developed without even the cursory consideration of security.
2. Programming errors that may allow trap doors or program faults (intentional or otherwise) that allow uncontrolled or improper activity during system operation. Almost all software has errors; repairs to applications program code may create a thicket of patches or corrections that is difficult to understand and impossible to analyze to ensure integrity and correctness.
3. Weak or inadequate logical system access controls, which might allow easy penetration or which fail maintain activity logs so that developing attacks might be recognized. Until recently, most computer manufacturers offered security as an option; one had to pay extra to get the software to protect the system and its data. Now some manufacturers are putting significant efforts into security software and hardware, which are sold as an integral element of computer packages.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدني
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4. Absent or poorly designed procedural controls, which fail to maintain strictly defined and current access authorization: such procedures must relate those individuals with access privileges to their respective job assignments (subject to management approval).
5. In the absence of formal procedures and responsibilities, the authorization for-use table will quickly become out of date.
6. Ineffective employee supervision and management control, which allows people to do things outside the specific system operation procedures or activities or inimical to the best interests of company: small violations can quickly grow into fraud (Schweitzer, 1987, pp. 16 - 17).

Again, the Council of the OECD (1992) confirmed that security threats to information might result from intentional or unintentional acts and might come from internal or external sources. They range from cataclysmic events to minor, daily inefficiencies. Downtimes, for example, might be caused by one large breakdown or frequent slow-ups or service degradation. The frequency and duration of these disturbances, however minor, should be considered when planning for information security. Large and small events might be equally disruptive to system functioning and use and equally debilitating to the organization's effective operation. In the next section, the researcher will present the different perspectives of information security threats classifications.

2021/2022 2021/2022 2021/2022

2-4. The Classification of Information Security Threats

30006101601571 30006101601571 30006101601571

Information systems might be targets of a range of serious security threats, including computer-based fraud, espionage,

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

sabotage, vandalism, viruses, computer hackers and other sources of failure or disaster. Information security threats are expected to become more widespread, more ambitious and increasingly sophisticated.

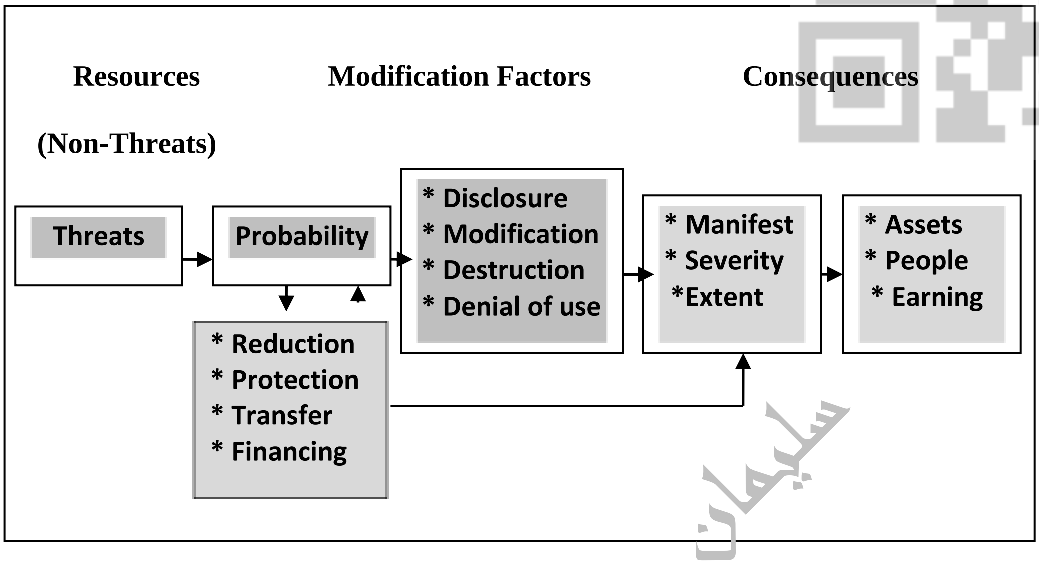
Information security threats might be classified as passive and active security threats. Passive threats are unpredictable natural or physical disasters and accidental human errors occurring completely at random, such as fires or floods, while active threats are deliberate and malicious attacks on information systems. These can potentially be predicted and avoided. They might be carried out by insiders or outsiders and they might be the result of direct or indirect actions (Mitchell et al., 1999).

Parker (1981) stated that security threats could be classified according to the type of act into three categories: natural disasters; errors and omissions, and intentional acts. The last two categories also include disasters that might be caused by people such as fires, floods and explosions. For protection purposes, these types of acts could be classified simply as accidental and intentional. However, many intentional acts are classified as crimes, such as fraud, theft, embezzlement, extortion, larceny and mischief (p. 44).

According to Crockford (1980), security threats are a broad range of forces capable of producing adverse consequences on the organization's resources, including its assets, people, and earnings. However, “modifying factors” are internal and external factors that influence the probability of threats occurrence incidence or the severity of consequences when the threat does occur. Consequences are the ways a realized threat impacts the organization's resources, as illustrated in the following figure.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg



(Figure 2-1)
(Source: Adapted from Crockford 1980 Risk Analysis Model)

Rainer et al. (1991) classified security threats of information under three main groups: physical threats; unauthorized access; and authorized access, which may be caused by internal or external sources. They consider the security threats arising from authorized access to be the most difficult to locate and assess.

Loch et al. (1992) presented a four-dimensional information systems security model. Loch et al. included twelve security threats, derived from the MIS literature and informal interviews of MIS academic faculty. According to Loch et al. (1992) the source of security threats may be "internal" to an organization, as a result of its employees' actions or failure of organization process, or "external", such as hackers' actions or natural disasters like fires, floods and earthquakes. Another dimension of the threat is the perpetrator; some threats are the

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

result of human actions, while others result from natural or non-human events. Finally, the action of perpetrators could be accidental or intentional, irrespective of the source (figure 2). Jenkins et al. (1992) stated that “There are many factors, internal and external to an organization, which may threaten its security. The threats might be accidental, such as air conditioning failure, or deliberate, such as computer assisted fraud. In some cases, the same event can be caused either accidentally or deliberately; a fire which destroys the whole data centre may be the result of a chance electrical short circuit, or a deliberate act of a disaffected security guard. It will often be the case that deliberate acts are the more serious, as they will have been planned to avoid detection and cause the maximum damage. A computer operator who deliberately destroys important data files may also be in position to destroy the back-up files as well” (p. 519).

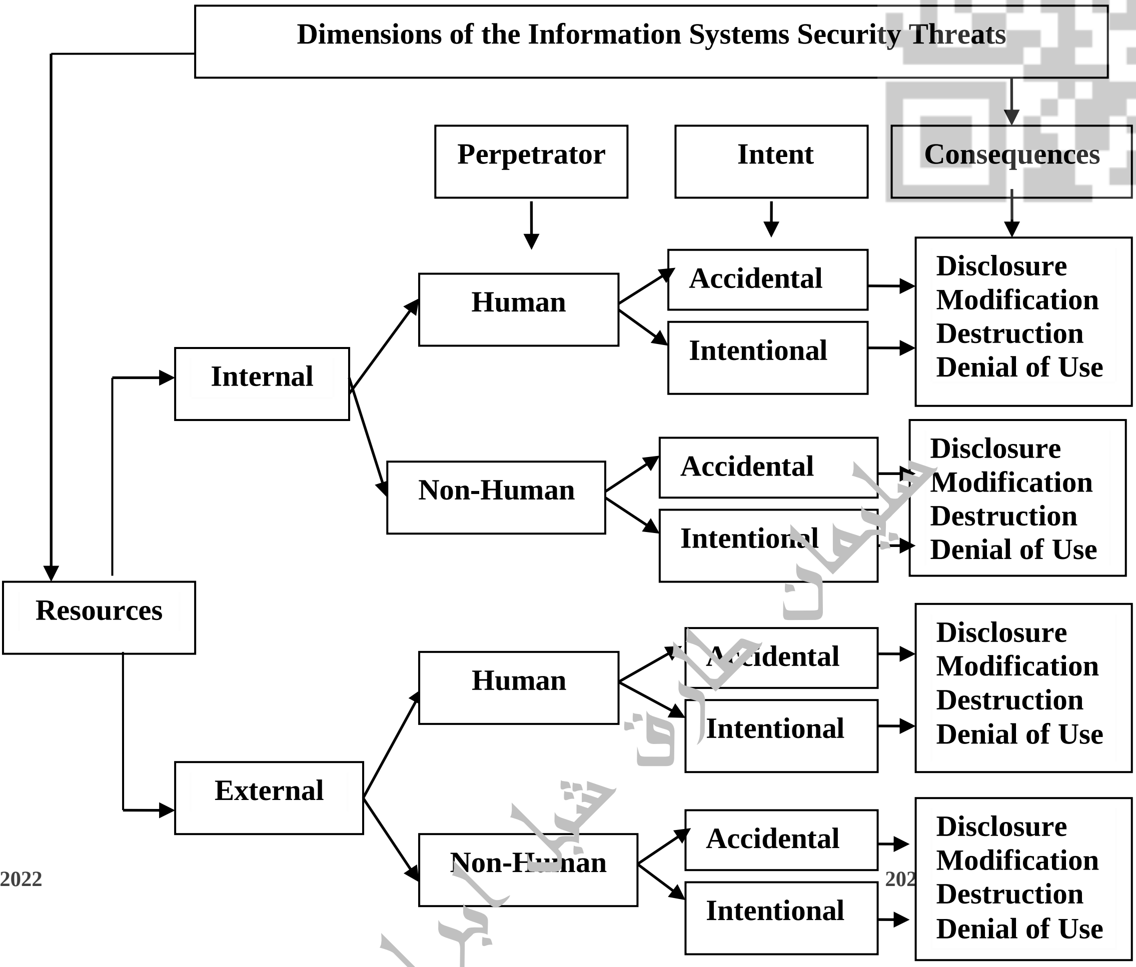
However, in organizations and accounting, embezzlement is usually the greatest perceived threat to computer security. Comprehensive control of the privileges of the users and detailed audit trails are reasonable security features to handle this threat Weiss, 1990).

2021/2022 2021/2022 2021/2022

In the following sections, information security threats will be classified according to their source (internal versus external); the perpetrator (human versus non-human); the intent of perpetrators’ actions (accidental versus intentional); and, finally, the consequential damage to information (physical sabotage versus logical sabotage). The security threats of each stage of information (input, processing and output) will be discussed in more details in a separate section.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg



2021/2022

(Figure 2)

The Four Dimensions of the Information Systems Security Threats (Source: Adapted from Loch et al., 1992, p.176)

2-4-1. Internal versus External Security Threats

The security threats to information could be classified according to *source* into “internal” and “external” security threats. The organization's employees and staff are usually regarded as the main source of internal security threats, while

سليمان طارق شبل ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

hackers and natural disasters are considered the main source of external threats to information security.

Weingartner and Burton (1991) argued that the big security headaches are now perceived to come from within, not outside. The organization's own employees are potentially its own worst enemies, posing the most serious risk to security (p. 33).

The results of Loch et al.'s (1992) survey revealed that 62.4 percent of their survey respondents suffered from the internal security threats and the vast majority of these threats (almost 72 percent) were caused by human factors. The comprehensive results of the Loch et al. (1992) survey, concerned with the information Security threats, are presented in Table 2-1.

External threats to information might arise from external sources such as natural disasters, acts of competitors, hackers or computer viruses. Internal threats to IT assets might come from authorized and unauthorized physical access, sabotage and technical failures leading to system abuse. These threats could damage or destroy IT assets such as hardware, software, data, personnel and facilities (Rainer et al., 1991; Bandyopadhyay et al., 1999).

Loch et al.'s (1992) empirical study reveals that at the application level, information systems' managers consider natural disasters and employee accidental actions to represent the greatest level of risk. Smith (1995) also argued that "creating a secure environment is complicated by the fact that workers must support security efforts for them to be effective, but it is often employees that pose the greatest threat to security. Most workers, however, are not actively trying to breach security. Often,

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

careless mistakes and indiscriminate access to information are at the root of security problems. Therefore, the more informed users are, the more likely they are to accept the policies".

(Table 2-1)

(The Results of Loch et al. 1992 Survey Regarding The Threats of Information Systems Security)

Source	Perpetrators Human (71.8%)		Non-Human (27.6%)	
Internal Threats (62.4%)	Accidental entry of bad data	(16.5%)		
	Accid.dest.Data by employees	(16.5%)		
	Weak/ineffect. Physical control	(9.1%)		
	Intent.dest.Data by employees	(3.5%)		
	Unauth.access by employees	(5.7%)		
	Intent. entry bad data by employees	(2.2%)		
	Inadequate control over media	(5.9%)		
	Poor control of I/O	(4.1%)		
	Total	***(62.4%)***		
External Threats (37.0%)	Access by competitors	(1.9%)	Natural disaster	(19.8%)
	Access by hackers	(7.5%)	Computer viruses	(7.8%)
			Total	***(27.6%)***
	Total	***(9.4 %)***		

Anderson (1994) confirmed that many thefts in banks, as well as many frauds in other industries, are carried out by staff and employees who have inside knowledge and access. He reported that British banks dismiss about one percent of their staff every year for disciplinary reasons. Many of these sackings are for petty thefts by tellers, and many ATM related thefts go undetected because of the banks' policy of denying that they are

سليمان طارق شبل ابراهيم السعيدي
2021/202
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

even possible. Anderson presented the following examples of internal computer fraud and security breaches:

- A housewife from Hastings had £8,600 stolen from her account by a bank clerk who issued an extra card for it. The bank's systems did not control address changes, so he was able to change her address to his, issue a new card, and change it back again. When she finally noticed the loss and complained, she was not believed; the thief was only discovered because he suffered an attack of conscience and owned up.
- At another bank, an installation blunder let technicians work out PINs on their test equipment. The bank's programmers had not bothered to set up the encryption keys properly, with the effect that the live and test systems shared the same set of keys. Eventually, some of the technicians started charging the local underworld £50 a time to calculate PINs for stolen cards; and when the bank's security manager found out what was going on, he was killed in an accident, in which organized crime may have been involved. The bank did not bother to send its customers new cards.
- One make of ATMs would output ten banknotes when a 14 digit sequence was entered at the keyboard, and a bank which used these machines printed this sequence in its branch operations manual. Three years later, there was a sudden spate of losses, which went on until all the banks using the machine put in a software patch to disable the test transaction.
- In another bank, a protege of the deputy managing director sent a circular to all branches announcing that to cut costs,

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق سليمان عبد الحميد السعيدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

> a number of dual control procedures were being abolished, including that on handling ATM cards and PINs. Losses increased tenfold; but managers in the affected departments were unwilling to risk their careers by making a fuss.

Price et al. (1989) mentioned that institution insiders dominate the number of EFT(electronic fund transfer) frauds. They argued that the methods implemented for this purpose range from altering and copying software to transferring customers' funds into secret accounts. For example, a California bank employee discovered a "secret" transfer code and imperceptibly transferred $10 million into his Swiss bank account before being discovered. In another case, data processing employees at a Citibank Silver Credit Card location issued themselves credit account numbers. These employees then spent the limit on each card and sent the billing to fictitious addresses.

In another case, computer engineer Anthony Pratt admitted to stealing more than £17,000 through ATMs in Scotland over two years. Anthony, who worked for Clydesdale Bank, used a hand-held computer to record transactions at ATMs. He noted customers' PINs (personal identification numbers) and later used them on plastic cards with magnetic strips. Clydesdale customers complained about so-called "phantom" withdrawals, where money disappeared from accounts without explanation. They were told by bank officials that the bank's systems were infallible, and they were also warned that they were responsible for the cash withdrawn. Faced with increasing customer complaints, Clydesdale called in the police fraud squad. However, a bank projects manager noticed that complaints had come from ATMs in areas serviced by Pratt. He was watched by

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

police, who saw him taking cash from a machine in Glasgow. Pratt then admitted his guilt and co-operated with the investigation (Collins, 1992).

Moss (1996) mentions that "Several European banks are said to have been the victims of extortion claims from computer hackers during the past 12 months. Neil Barrett, a former hacker and now a consultant for Bull Information Systems in Britain, said the British arm of one US bank was forced to pay out £50,000 in 1996 but, like the other banks, it has avoided making any public admissions of the attack in order to maintain its reputation within the financial community".

2-4-2. Human versus Non-Human Security Threats

Again, the security threats of information could be classified according to the *perpetrator* into human security threats and non-human security threats. Human security threats are those which originate from the actions of a human being. However, human security threats might be either accidental threats (such as human error) or deliberate threats (such as input fraud).

2021/2022 2021/2022 2021/2022

According to the Council of the OECD (1992) human beings and the institutions they establish to reflect their values, whether social, economic or political, as well as the lack of such institutions, all contribute to security problems. The diversity of system users (employees, consultants, customers, competitors or the general public) and their various levels of awareness, training and interest, compound the potential difficulties of providing security.

30006101601571 30006101601571 30006101601571

Davis (1996) mentioned that it is an accepted fact that new technology increases the security risks in accounting information

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

systems. Even with all the advances in security measures, there remains the risk associated with humans who use these measures. The majority of respondents in Davis' survey ranked a human factor as one of the top information security threats. A control system is only as good as those who use it; and users must be educated in the use and importance of information security measures (p. 40 - 41).

Human errors can take the form of omission or commission. Errors of omission occur when a person fails to take a correct action that is prescribed or required. For example, an error of omission would be the failure of a user to back up a hard disk. Error of commission occurs when a person executes a prohibited or incorrect action. An error of commission would be the transposition of two digits by a data entry operator composing a wire transfer message, or deleting an important file which cannot be restored or reproduced (Wood and Banks, 1993, p. 52).

Errors and omissions may occur in gathering, creating, processing, storing, transmitting, and deleting data and information. Failure to back up critical files and software multiplies the negative effects of errors and omissions. If files have not been backed up, the organization may incur significant expense in time and money in recreating them (OECD, 1992).

Again, Wood and Banks (1993) confirmed that one of the major and most serious threats to information security (human error) is often ignored or dismissed with statements such as “it’s inevitable” or “there is not much we can do about it”. This type of thinking runs counter to reality, since studies have shown that, of all systems threats, human error has the highest probability of occurring. These studies also indicate that, with the right

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدني

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

professional assistance, human errors could be easily corrected or significantly reduced (p. 51).

On the other hand non-human security threats to information security are usually related with technical threats of the IT (such as technical failure of the system or hard disk failures) or the other technical facilities (such as software problems). Non-human security threats might also arise from natural disasters (such as floods, earthquakes or failure of a power supply of the information).

The OECD (1992) suggested that technical factors leading to failures of information systems are numerous, sometimes not well understood, and constantly changing. They might be computer and communications hardware or software faults and malfunctions, caused by bugs, overloads or other operational or quality problems.

It is interesting to note that some information technical problems are actually connected with human action. Some technical problems might be caused as a result of intentional attacks of information, either by internal (employee) or external (hacker) attackers. Some technical problems caused by human actions include introducing viruses into the information via infected software. Trap doors, Trojan horses, worms, and logic bombs are some of the technical means used to disrupt, distort or destroy normal system functions. Loss of power supply could also result from intentional human actions.

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدي

2-4-3. Accidental versus Intentional Security Threats

Another perspective for classifying the security threats of information could be the *intention* underling perpetrators' actions. Accordingly, security threats could be classified into

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

intentional and accidental. Accidental security threats are those security threats whose origin does not involve any malicious intent, such as human error and some physical natural security threats. On the other hand, intentional security threats involve malicious intent, such as sabotage and computer fraud.

According to OECD (1992) intentional security threats include the intentional misuse of authorized system access and unauthorized system access ("hacking") for the purposes of mischief, vandalism, sabotage, fraud or theft. Popular conception holds that the greater part of threats to information systems comes from external sources. On the contrary, persons who have been granted authorized access to the system might pose a larger threat to information systems. They might be honest, well-intentioned employees who, owing to fatigue, inadequate training or negligence, commit an inadvertent act that deletes massive amounts of data. They may be disgruntled or dishonest employees who misuse or exceed authorized access to tamper deliberately with the system for their own enrichment or to the detriment of the organization.

Haugen and Selin (1999) argued that unintentional acts, while costly at times, could be corrected or avoided through training and supervision. On the other hand, intentional acts are generally fall into the designation of computer crime. These crimes might be acts of sabotage intended to destroy the information components or acts of computer fraud where the intent is to steal money, data, computer time and/or services. They would also include manipulative activities such as deleting or altering records and files to remove damaging information or create false information.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

The main characteristics of accidental versus intentional security threats of information have been discussed by Parker (1981) as the following:

2-4-3-1. Frequency

Errors and omissions in computers can occur due to several reasons, such as lack of awareness, knowledge, or skills. On the other hand, most intentional acts, especially those involving significant losses, are infrequently detected. Therefore, attempts to calculate probability, expected loss, nature, patterns of location, and source are difficult.

2-4-3-2. Unsolved Problems

Parker argues that few cases of accidentally-caused losses remain unsolved. Efforts to control unintentional losses have been made throughout the development of electronic data processing, so that adequate solutions are known for most common errors and omissions.

In contrast, significant security problems concerning intentionally caused losses remain unsolved. The technical security of currently available computer systems is inadequate against attack from potential perpetrators (such as systems programmers) who have sufficient skills, knowledge, and opportunity (Parker, 1981, p. 45).

2-4-3-3. Act Complexity

Accidentally caused losses usually derive from single, isolated acts. Each incident is, in general, unrelated to other loss incidents. On the other hand, an intentionally caused loss commonly results from sequences of dependent and independent

سليمان طارق شبل ابراهيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

authorized and unauthorized acts. Many perpetrators might be involved in intentionally caused losses, which might increase the complexity of intentional acts in order to avoid detection or apprehension (Parker, 1981, p. 45).

2-4-3-4. Singularity of Source

One person is usually responsible for an error or omission, even though other people might cause extenuation; whereas several individuals are frequently involved in perpetrating an intentional act. Half of all known cases of computer abuse have involved collusion.

Compared to manual, or non-computer fraud, embezzlement, and other such acts, collusion is more prevalent in computer crime, primarily because computer crimes require more skills, knowledge, access, time or resources than any one person usually possesses in the technically-oriented environment of computer systems (Parker, 1981, p. 45).

2021/2022 2021/2022 2021/2022

2-4-3-5. Complexity of Perpetrator Behavior

Behavior that causes errors and omissions is relatively simple, for it is related to conditions prevailing at the instant of the act. After the act the perpetrator need, at most, defend only the weakness that resulted in the error. In contrast, the behavior of most people performing intentional acts is highly complex (Parker, 1981, p. 45).

2-4-3-6. Using Errors for Intentional Acts

An error threat could be applied to each loss, which could also have an intention threat associated with it. The error threat could easily become intentional, as demonstrated by the

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعيدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

following example. A person who has committed an error might conclude that if it recurred, it could result in advantage to them. They could subsequently "let the error happen again," and thus would convert the erroneous act into an intentional one, even though it might be considered a passively intentional act. Their next move might be to compromise or avoid a safeguard designed to detect and record "error". This move would convert his act to an active one, the prevention of which must include protection from compromise of the safeguard, as well as protection of the asset subject to loss (Parker, 1981, p. 46).

2-4-3-7. Sources of Security Assistance

As Parker (1981) reports, accidentally caused losses have been extensively studied and discussed in the technical literature for many years. However most technical literature that claims to treat accidental and intentional acts primarily addresses accidentally caused losses. Professional societies and governmental organizations dedicated to the prevention of intentionally caused losses have only recently focused on the problems associated with computer technology.

2-4-3-8. Strategy and Safeguard Independence

Each possibility for error or omission can effectively be treated in isolated ways, because one loss would be unrelated to any further loss. On the other hand, each possibility for intentionally caused losses must be covered comprehensively to have any effect: all possible acts leading to the loss should be taken into account. Safeguards against an intentional act would often have impact on other types of acts or losses, but it might only partially supply adequate protection (Parker, 1981, p. 47).

سليمان طارق شعبان ابراهيم السعيدي
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

2-4-3-9. Achievable Protection Level

In Parker's (1981) view, accidental losses can largely be prevented or, at least, can be minimized for a wide range of possibilities. But a high level of protection from intentionally caused losses is difficult to achieve due to inadequate and incomplete knowledge of vulnerabilities. An individual estimate of loss could be affected by many factors, including the difficulty of determining the completeness of protection (p. 48).

2-4-3-10. Potential Perpetrators

The potential perpetrators of accidental loss can be easily identified. They are individuals who have access and authorization to perform an act that might cause an accidental loss. Conversely, potential perpetrators of intentionally caused losses are difficult to identify. They include not only those identified in connection with accidentally caused losses, but also the larger numbers of people who might have an opportunity to gain the necessary skills, knowledge, and opportunity to perform an unauthorized act (Parker, 1981, p. 45).

2021/2022 2021/2022 2021/2022

2-4-3-11. Potential Perpetrators Capabilities

Accidentally caused losses tend to correlate with minimum skills, knowledge, and resources of potential perpetrators; and of course opportunity is a significant factor. Intentionally caused losses, however, can be correlated with maximum possible skills, knowledge, opportunity, resources and time to commit the act (Parker, 1981, p. 48).

30006101601571 30006101601571 30006101601571

سليمان طارق شعبان ابراهيم السعدني

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

2-4-3-12. Detection

Perpetrators of accidentally caused losses have no conscious intention of erring before and during their acts. Therefore, if an attempt is made to avoid detection, it occurs after the loss. Less fear of detection, less reluctance to report the loss and greater co-operation with the victim in recovery are evident in accidental loss situations than in intentional acts.

Interviews have revealed that perpetrators greatly fear unanticipated detection before, during, and after their acts, so that much of their efforts and resources go into prevention of detection. Thus, detection of intentionally caused losses become a greater challenge than it is for accidentally caused losses and should occupy a greater amount of the security specialist’s attention (Parker, 1981, p. 48 - 49).

2-4-4. Physical versus Logical Information Security Threats

Physical security threats could be regarded as threats whose consequences would consist of physical damage to an information system. The physical damage might affect either the IT assembly part of an information system or the structures and environmental control systems housing it. However, physical threats might arise either from naturally occurring phenomena or from accidents involving failure in technical systems or in components external to the information system. Examples of physical security threats are flood, earthquakes and air crashes. Events internal to the information system, such as hard disk failures, are considered technical or logical security threats.

2021/2022 2021/2022 2021/2022

Sabotage is one of the main security threats to information. However, sabotage is regarded as an expected result of lack of systems security. Physical damage and logical damage are two

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

types of sabotage that might occur to information which will be briefly highlighted in the following sections:

2-4-4-1. Physical Security Threats to Information

Physical damage is one of the important security threats to information. Physical damage of the information might occur as a result of natural disasters (floods, fires, or earthquakes). It could also occur as a result of intentional or accidental human actions (fires, again, or electromagnetic discharge). However, sabotage might cause total or partial physical damage to the computer hardware, tapes and disks.

According to the OECD (1992) physical threats to information systems fall into two broad categories: extreme environmental events and adverse physical plant conditions. Extreme environmental events include earthquake, fire, flood, electrical storms and excessive heat and humidity. The information system might be housed in a building in which, in addition to computers and communication lines located throughout the building, there might be dedicated computer rooms and data storage rooms. Connections for power supply and communication may lead to and from the building. Adverse physical plant conditions might arise from breach of physical security measures, power failures or surges, air conditioning malfunction, water leaks, static electricity and dust. An organization might be affected by lapses either directly at its premises or indirectly at a vital point outside the organization, such as power supply or telecommunication channels.

Rainer et al. (1991) listed the physical security threats of information as the following:

- Equipment failure

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Power interruption
- Contaminants in the air
- Weather
- Fire
- Humidity
- Destruction or damage to facility or equipment by humans
- Death or injury to key personnel
- Personnel turnover

Parker (1976) mentioned that "Natural disasters caused by fire, water, wind, power outages, lightning, and earthquakes could cause significant disruption (or even destruction) of computer facilities, or at least crucial parts of computer facilities" (p. 14).

According to Parker (1983) the main security threats to software, tapes and disks are physical damage, magnetic damage, identity loss, and logical damage. Besides the obvious crushing, warping, melting, cutting, and scoring, the bonding of magnetic material to Mylar deteriorates at high level of humidity. The surface can also be contaminated with almost any other substance. Strong magnetic fields can be used to erase data (p. 43).

The OECD (1992) recommended that "Proper security procedures must extend beyond the computer terminal and communication lines to the entire information arena. Improper handling of data and information storage media (whether paper, magnetic or other) and improper handling and disposal of discarded computer printouts might lead to security breaches. Computer printouts might contain proprietary or competitive information or clues regarding system access. Yet, many companies have no policy for their disposal.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعدني

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Once used for the organization's purpose, they are considered worthless and discarded along with the day’s used envelopes and pencil shavings. There might, however, be no expectation of privacy in trash, at least in trash that is outside the premises”.

2-4-4-2. Logical Security Threats of Information

Logical security threats of the information includes the logical damage of the software, programs and data stored either on the hard disks or floppy disks. Magnetic tapes and disks might have both internal and external labels. Internal labels are data stored magnetically that identify the contents of the computer and disks or tapes. External labels are affixed to the tape reel or disk hub or cover that identify a tape or disk visually. Highly systematized computer centers identify tapes externally with a serial number and rely upon the computer system and computer file of tape number and their contents to identify data. In this mode of operation, the computer outputs instructions to operators to mount tapes by serial number alone. Destroying the external labels of a few hundred or thousands of tapes could result in great cost to re-label by having the computer read internal labels; when internal labels are not used, it could represent a total loss of data (Parker, 1983, p. 42).

In Parker’s (1983) view, “Logical damage could be far subtler than label damage and cause even greater loss. It requires the use of a computer and program to modify data on a tape or disk, making the effort greater than for other methods but possibly more damaging”.

Again, the OECD (1992) argued that computer programs are an important element of information systems and a

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

potentially fertile terrain for threats to information systems. A program containing a virus that is introduced into an information system may affect the availability, confidentiality and integrity of that system by overloading the system, changing the list of authorized users of certain parts of the system or by altering data or information in the system. Violations of provisions of licensing agreements relating to the information system (such as software licensing agreements and database-licensing agreements) may pose an additional security threat. Unauthorized alteration of the licensed programs, for example, may trigger malfunctions as the modified software interacts with other parts of the system. Disclosure of proprietary information may damage an organization's competitive position.

Insufficient use of systems might also lead to information security problems, such as maintaining information availability or integrity in the event of shortages of qualified personnel, whether as a result of employees changing jobs, the introduction of new technologies requiring new skills, or work slowdowns, stoppages or strikes (OECD, 1992).

Anderson (1994) referred to a number of technical attacks that occurred due to blunders and serious mistakes in the design and operation of the bank’s systems. He also argued that most of them could have been avoided if competent security consultants had been hired to look the system over:

- Two men were convicted at Winchester in England over a simple but effective fraud. They would stand in ATM queues, observe customers’ PINs, pick up the discarded ATM tickets, copy the account numbers from the tickets to blank cards, and use these to loot the customers’ accounts. This trick had been well known in the security community since it was

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعيدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

experienced in New York in 1985. It can be stopped by very simple measures, such as not printing all of the account numbers on the ticket; yet it was not until October 1993 that the last UK bank took these measures. In 1994, it was reported that some individuals have been caught using exactly the same trick in San Jose, California.

- One UK bank's cash machines were fooled by telephone cards. When one of these was inserted, the ATM software believed that the previous card had been put in again. Street youths stood in line, observed customers' PINs, and helped themselves to cash.
- Some banks have schemes which enable PINs to be checked off-line. For example, customers of one large English bank got a credit card PIN with digit one plus digit four equal to digit two plus digit three; and a debit card PIN with one plus three equals two plus four. Villains eventually found out that they could use stolen cards in off-line ATMs by entering a PIN such as 4455.
- One of the largest London banks wrote the encrypted PIN on the card strip. Villains found by trial and error that it was possible to change the account number on their own card's magnetic strip to that of the target, and use it with their own PIN to loot his account. A document about this technique circulated in the prison system, and two men were convicted at Bristol Crown Court of conspiring to steal money in this way. They caused consternation to police and prosecutors by calling an eminent banking industry expert to testify that what they had planned was impossible, but a newspaper journalist discredited his testimony by demonstrating the trick, and the defendants agreed to plea-bargain.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعيدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- The use of store-and-forward processing has caused some problems. Anyone can open an account, get a card and PIN, make several copies of the card, and get accomplices to draw cash from a number of different ATMs at the same time. This was a favorite modus operandi in Britain in the 1980s and remains a problem in Italy.

4-5. Approaches of Abusing the Security of Information

Whenever a security threat to a corporate information is realized, the nature of the damage to information should be recognized as one of the following types:

- Interruption, where an information asset becomes lost, unavailable or unusable;
- Interception, where an unauthorized party gains access to an information asset;
- Modification, where an unauthorized person not only accesses but also tampers with an information asset; or
- Fabrication, where an unauthorized party introduces forged and false objects to an information system (Mitchell et al., 1999).

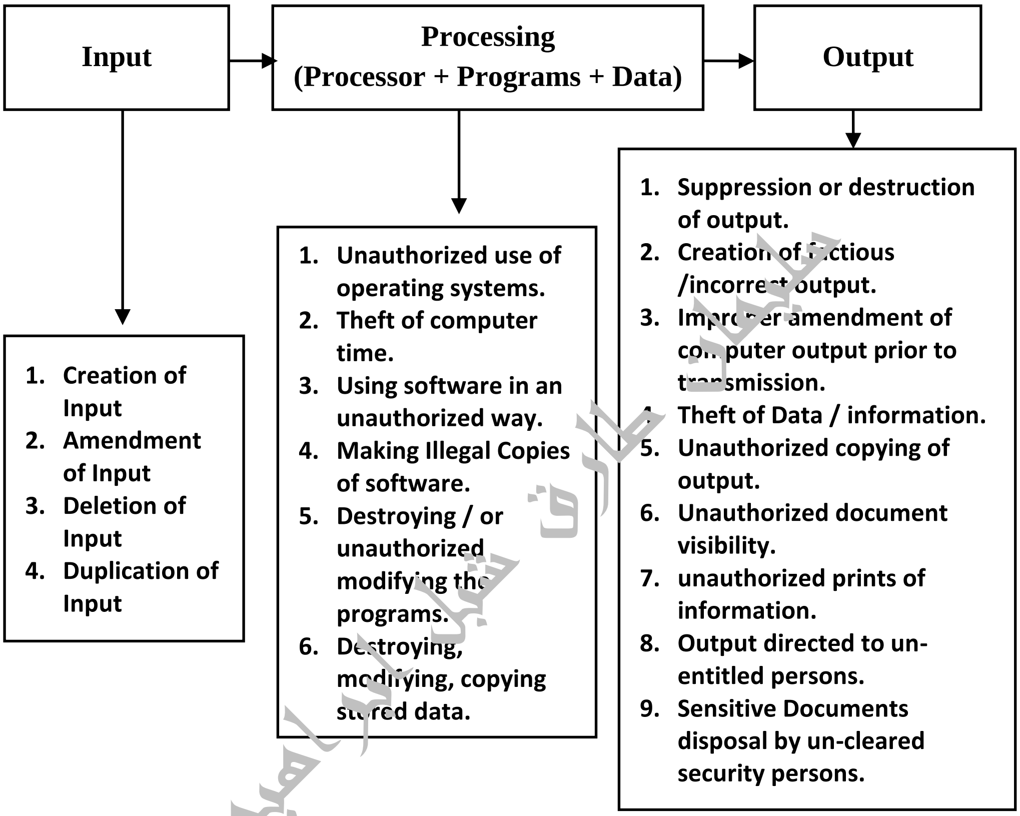
In Huntington and Davies' (1994) view, there are three main types of computer fraud, which are related directly to the key stages of information. They are:

- Input-related (usually involving the manipulation of the data to be input into the computer);
- System-related (unauthorized changes to the programs or systems used to process the information); and
- Output-related (the manipulation or suppression of computer output).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق سليمان ابراهيم السعدني

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Internal and external perpetrators might abuse security at any of the three stages of information (input, processing and output). The security threats of information related to each stage are illustrated in the following figure:



1. Creation of Input
2. Amendment of Input
3. Deletion of Input
4. Duplication of Input

1. Unauthorized use of operating systems.
2. Theft of computer time.
3. Using software in an unauthorized way.
4. Making Illegal Copies of software.
5. Destroying / or unauthorized modifying the programs.
6. Destroying, modifying, copying stored data.

1. Suppression or destruction of output.
2. Creation of fictious /incorrect output.
3. Improper amendment of computer output prior to transmission.
4. Theft of Data / information.
5. Unauthorized copying of output.
6. Unauthorized document visibility.
7. unauthorized prints of information.
8. Output directed to un-entitled persons.
9. Sensitive Documents disposal by un-cleared security persons.

2021/2022

(Figure 3)
(Approaches of Abusing the Security of CAIS)

2-5-1. Input Security Threats

One of the most common ways to abuse security of information is by altering computer input. Input fraud is the easiest way to commit a computer fraud because it does not require great skills or sophisticated knowledge in computers. Thus, the perpetrator might breach the security of information

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

and commit a computer fraud by altering or modifying the data before its entry to the information.

Huntington and Davies (1994) argued that "Where it is possible to amend or alter input, prior to or during its capture by the computer systems, there is a potential for fraud. Accordingly, it is important that adequate controls should exist over the input sources to prevent or detect the unauthorized alteration, addition, deletion or duplication of input".

Therefore, the "Input" related fraud might include one or more of the following:

1. Creation of input
2. Amendment of input
3. Deletion of input
4. Duplication of input

2-5-1-1. Creation of Input

This involves the creation of input in the correct format and type to be included with existing inputs (or submitted on its own) without detection. This could be as simple as inserting an additional expense requisition into an existing batch or the direct entry of a sales order into a sales entry system. There may be no paper copy of the input, as many modern systems allow direct on-line entry of data (Huntington and Davies, 1994, p. 109).

The creation of false input is one of the most common and simple ways of perpetrating a fraud, particularly when carried out in conjunction with a related change to standing data such as payroll file, sales file, or commission file.

Huntington and Davies (1994) presented the following two examples of creation of false input:

1. An employee of an insurance company used a colleague's passwords to reactivate

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شلبي إبراهيم السعدي

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

2. annuity interest payments on deceased client files and divert them into a bank account to which he had access.
3. A payment clerk in a bank discovered his supervisor's password which made it possible for him to prepare, authorize and send payment instructions for over £10 million. The attempted fraud was detected because staff at the receiving bank realized the instruction was unusual and queried it with the originating bank's management (p. 110).

2-5-1-2. Amendment of Input

Amendment of existing input involves making a fraudulent change to the original input, after the item has been approved but before its input to the computer system: for example, increasing an expense claim, or changing the name and address of a loan applicant, or changing the interest rate to be applied in a transaction. For example, a data entry clerk reduced the interest rate on specific personal loan application forms when entering them into the bank's computer. In return the applicants paid the clerk 50 percent of the value of the interest saved (Huntington and Davies, 1994. p.111).

2-5-1-3. Deletion of Input

The deletion of input prior to its entry or capture into the system could be as simple as the removal of an item from a batch of records or the deletion of the entire batch. For example, a payroll employee regularly destroyed employee termination notices and then changed the bank account details for the payment of salary. The fraud was not detected until he was taken ill (Huntington and Davies, 1994, p. 111).

سليمان طارق شبل إبراهيم السعيدي
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

2-5-1-4. Duplication of Input

Duplication of data is a simple and effective way of committing computer fraud through selecting specific data and information (such as requests for payment or stock shipment) to be processed more than once, with the extra transactions being channeled to the credit of the perpetrator. The process of duplicating input may involve copying input and submitting both the original and the copy or simply re-inputting the original document in a later cycle if there is no cancellation of processed items.

Huntington and Davies (1994) reported that "It is important to distinguish between the alteration of different types of input as the risk associated with each may be considerably different, requiring different levels of controls to prevent and detect. The alteration of standing input is typically more difficult to detect, as the source of the fraud is a single act rather than the recurring action required to fraudulently alter transaction data alone (e.g. fraudulently increase the hours worked on weekly timesheet)".

The following table provides some examples of the alteration, addition, deletion and duplication of both standing and transaction data (Huntington and Davies, 1994, P. 112).

Again, Cushing and Romney (1994) presented the following examples of committing computer input fraud:

- To steal inventory, a perpetrator might enter data into the system to show that stolen inventory has been scrapped. For example, at a railroad company on the UK East Coast, several employees entered data into their employer's system to show that over railroad cars were scrapped or destroyed. They repainted and sold them.

سليمان طارق شعلان ابراهيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- To commit payroll fraud, perpetrators enter data to increase their salary, to create a fictitious employee, or to keep an employee who has been terminated on the records. Under the latter two approaches, the perpetrator intercepts and cashes the check.
- In cash receipts fraud the perpetrator hides the theft of the cash by falsifying system input. For example, an employee at the Arizona Veteran's Memorial Coliseum in the USA sold customers full-price tickets, entered the sale as a half-price ticket and pocketed the difference (p. 654 - 655).

Fraudulent Procedure	Example Involving Standing Data	Example Involving Transaction Data
Creation of invalid input data	Creation of a bogus employee	Creation of a fictitious invoice from supplier
Amendment of existing input data	Changes to a customer's discount percentage	Increasing the discount offered to a customer on a one-off order entry form
Deletion of valid input data	Deletion of a valid notice of death of a registered shareholder to enable diversion of dividends	Deletion of a stop payment instruction on a cheque already written but not banked
Duplication of valid input data	Duplication of new insurance policy details (to inflate new business statistics)	Duplication of an invoice for services (as no check against goods received)

2021/2022

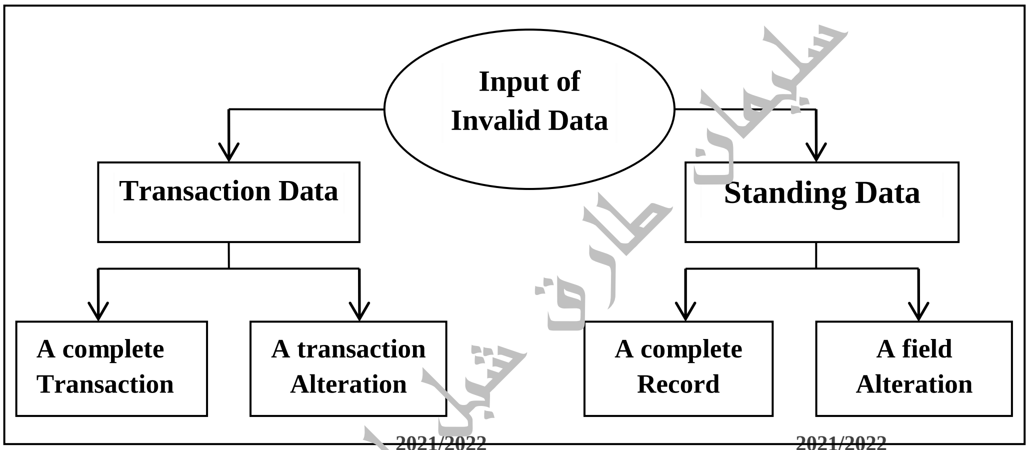
(Table 2)
Types of Input Security Threats
(Source: Huntington and Davies, 1994)

30006101601571 30006101601571 30006101601571

Jenkins et al. (1992) confirmed that "The input of invalid data might be of either transaction data or standing data. Invalid

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

transaction data would normally be a complete transaction either to add to a balance, such as a supplier's invoice, or to alter the effect of a transaction already recorded, for example a credit note to match a sales invoice. Invalid standing data might be a complete record, such as a fictitious supplier's account, or a field, such as rate of pay or interest rate. The potential to alter fields is usually increased where files are on-line and records can be displayed at terminals" (p. 236).



2021/2022 2021/2022 2021/2022

(Figure 4)
(Input of Invalid Data)

2-5-2. Processing Security Threats

Perpetrators might breach information security and commit computer crimes in the processing stage. They might conduct unauthorized changes and alterations in computer programs and in accounting software. Perpetrators might also destroy or modify the stored data and cause great damage to the organization and its information. The main processing components (the processor, computer instructions, programs and stored data) through which

سليمان طارق شبل ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

the perpetrators might abuse information will be briefly highlighted in the following sections:

2-5-2-1. The Processor

A further computer fraud and security breach could be committed by operating the system in an unauthorized way. This abuse might include the theft of computer time and services as well as the use of the system in unauthorized purposes. For example the employees might use the company's computer to do their personal work and to keep personal records. Some employees might even use the company systems to play computer games during working hours.

2-5-2-2. Computer Instructions

Computer fraud could be also accomplished by affecting the software used in processing an organization's data. This might involve modifying the software, making illegal copies of the software, or using the software in an unauthorized manner. It might also involve developing a software program or module to perform unauthorized activity links, inserting logic bombs or computer viruses, as well as altering the programs with a Trojan horse or Salami technique. However, this might require a specialized knowledge and advanced skills in computing.

According to Huntington and Davies (1994), program and system related fraud involve the illicit manipulation of computer programs or computer operations. Unlike input or output related fraud, system-related fraud requires a thorough understanding of the information being processed and a sound knowledge of computer systems involved. Not surprisingly, such fraud only

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

accounted for less than one percent by value of all cases reported in the 1993 survey (p. 113).

Huntington and Davies presented the following two examples of program-related computer fraud:

- Tampering with a computer program so that it only generates dispatch documentation and does not record any entries in financial records when goods are delivered to a particular customer;
- Changing the computer programs so that commission is calculated on the basis of gross sales figures before credit notes have been applied (Huntington and Davies, 1994, p.111).

The above computer frauds could occur as a result of lack of physical security over access to computer facilities, or poor control over changes related to computer programs, or inadequate quantitative control over file contents.

4-5-2-3. Stored Data

2021/2022 2021/2022 2021/2022

Information could be abused and fraud committed by altering or damaging an organization's data files or by copying, using, or searching them without authorization. This approach needs fewer skills than modifying software, but more skills than modifying input.

There have been numerous instances of data files being scrambled, altered, or destroyed by disgruntled employees. In one incident, the employee took off all external labels from hundreds of tape files. In another case, an employee used a powerful magnet to scramble all the data magnetic tape files. Parker (1983) has commented that modification of data could cause as much damage as its erasure. However, undetected

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعيدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

modification could cause much greater damage by affecting the results of computer usage and subsequent activities that rely on computer usage and subsequent activities that rely on computer output (p. 43).

2-5-3. Output Security Threats

The last but not least way of abusing the information and committing a computer fraud could be carried out by stealing, misusing, misrouting, or unauthorized copying of information output. System output is usually displayed on monitors or printed on paper. Accordingly, individuals who are near the screen might visually read anything on a monitor. In cases where many people share printers, then unless the printer is properly safeguarded, information output would be subject to prying or curious eyes or to unauthorized copying. McIntyre (1991) argued that one particularly notable weak link in the security chain in many computers is that sensitive documents are handed to non-security cleared personnel for shredding (p. 42).

2021/2022 2021/2022 2021/2022

Document visibility could also be considered to be one of the important information security threats. Thus, there is a need for a proper policy and proper procedures for printing and disseminating information. Printing and distribution of information should be done only by certain authorized persons and should be directed precisely to those people entitled to receive it.

Again, Huntington and Davies (1994) stated that computerized system fraud could involve the misuse of output and typically involves suppression, fraudulent creation of misleading output or theft of output, which could be used to create value. Like input-related computer fraud, this type of fraud

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

does not require a detailed knowledge of the actual computer systems and the supporting clerical and approval processes (for example, who receives exception reports or which printer generates pre-signed checks) (p. 114).

Moreover, when high-resolution printers or scanners fall into the wrong hands, disaster could result. LaPolla (1992) reported that high-resolution printers and scanners are being used by criminals to counterfeit checks and to commit other acts of forgery. American Microsystems Inc discovered four counterfeit checks returned to the company from its bank, Nations Bank in Atlanta, totaling $1,300, but the loss to the company was actually much higher, because it had to cancel its checking account and resubmit credit applications to all its customers. The following table presents some examples of information output security threats and misusing the computerized system output:

2021/2022

Types of Misuse	Examples
Suppression or destruction of output	Suppression of specific entries on a report highlighting delinquent loan customers at a bank
Creation of fictitious output	Creation of a report containing fictitious or duplicated insurance policies to support inflated new business claims
Improper amendment of computer output prior to transmission	Amendment of payee details on BACS payment tapes between preparation and transmission (for example, by unauthorized access to computer libraries)
Theft of output	Theft of computer generated checks

(Table 3)
(Types of Output Security Threats)

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Huntington and Davies (1994) mentioned several reasons that might lead to adverse consequences:

- Sharing of passwords might be common practice (and therefore password users are not uniquely accountable for their activities);
- Staff might have excessive levels of access (usually justified as essential when someone is absent or something goes wrong, but again raising the question of accountability and division of duties);
- Apparent problems with processing might continually require fixing by a particular member of staff and are therefore not checkable by others;
- Staff might make improper use of computer resources (for example, by accessing the computer system out of working hours);
- Improper use might be made of dial-in lines to computers without proper investigation; and
- There might be large volumes of items or unusual transactions occur in reconciliation
- or suspense accounts (a natural location for hiding irregular transactions) (p. 114).

2-6. Techniques of Committing Computer Fraud and Abusing information Security

Roufaiel (1990) argued that the only way for auditors to detect crimes is to think as criminals. Therefore, how crime is committed could be the key point in designing effective internal controls to search for any weakness that might contribute to making the arena for perpetrating such crimes easier for the

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق سليمان ابراهيم السعدني

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

criminal. Roufaiel has classified the techniques of committing computer crimes under four groups:

Program Alteration, which includes a variety of techniques to commit computer crimes such as Salami, Trojan horse, Virus, Logic bomb, Trap Doors and Asynchronous attack;

Data Manipulation, which includes Data diddling, Data leaking, Superzapping, simulation, Degausser, and damaging file labels;

Malicious Access, a group including impersonation, Piggybacking, wire-tapping, and scavenging;

Hardware and Software Destruction, through vandalism, sabotage and malicious mischief are related acts: deliberate physical action causing destruction or damage of equipment, programs, supplies, facilities or data (see: Roufaiel, 1990, p. 20).

Parker (1981) noted that "Neither practical prevention nor adequate detection capabilities are currently known for such sophisticated attacks as Trojan Horse method, Salami technique, data leakage, logic bombs, asynchronous attacks, or post system failure attacks (p. 45). Perpetrators have developed many techniques that might be used to abuse information security. The most common techniques are briefly presented in the following:

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدني

2-6-1. Trojan Horse

A Trojan Horse, in the information security context, is a set of unauthorized computer instructions within an authorized and properly functioning program. It performs some illegal act at a pre-appointed time or in a pre-appointed set of conditions. In this technique the perpetrator might insert several illegal

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

instructions amongst the millions of instructions in a computer program, which could be activated when accounts are updated or under any other predetermined conditions. An example would be one of the first known computer frauds, committed in 1966 by a computer programmer for a bank in Minneapolis. The programmer instructed the computer to ignore an overdraft on his account when it occurred (Cushing, 1994, p. 656; Haugen and Selin, 1999).

According to Qureshi and Siegel (1997) the Trojan Horse is a hidden program within the normal programs of the business. The computer continues to function normally, while the hidden program is free to collect data, make secret modifications to programs and files, erase or destroy data, and even cause a complete shutdown of operations. Trojan Horses can be programmed to destroy all traces of their existence after execution.

2-6-2. The Round-Down Technique

2021/2022 2021/2022 2021/2022

The round-down technique is one of the earliest approaches to computer fraud. This technique is used most frequently in financial institutions that pay interest. In a typical scenario the programmer instructs the computer to round down all interest calculations to two decimal places. The fraction of a cent that is rounded down on each calculation is put into the programmer’s account, or into one that he or she controls. No one will notice, since all the books will be balanced. Over time, these fractions of a cent can add up to a significant amount, especially when interest is calculated daily (Cushing, 1994, p. 656).

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

2-6-3. Salami Technique

The Salami Technique comprises secret program changes (perhaps accomplished by an authorized employee). It can cause very small changes that are unlikely to be noticed but, overall, can have substantial effects for the miscreant. For example, the perpetrator can delete one cent from every paycheck and transfer that amount to his / her own paycheck.

In the Salami Technique the fraud takes advantage of small sums gained when rounding thousands of transactions, diverting only part of a cent for each one every time accruals or financial calculations are done. Another approach is to slice off a small sum, a few cents or a few dollars, from accounts that are generally not carefully checked (Haugen and Selin, 1999).

Cushing (1994) reported that "With the Salami Technique tiny slices of money are stolen. The disgruntled chief accountant for a produce-growing company in California used the salami technique to get even with his employer. He used the company's computer system to falsify and systematically increase all the company production costs by a fraction of a percent. These tiny increments were put into the accounts of dummy customers and then pocketed by the accountant. Every few months the percentage was raised another fraction of a percent. Since all expenses were rising together, there were no accounts or expenses that brought attention to him. He was caught when another bank teller did not recognize the name of the company on the check he was trying to cash and called his employer to enquire about it" (p. 656).

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

Qureshi and Siegel (1997) suggested that in the Salami Technique the perpetrator can make secret changes to the computer program that cause very small changes that are unlikely

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

to be discovered, but whose cumulative effect can be very substantial. For example, the perpetrator might steal ten cents from the paycheck of each individual and transfer it to personal account.

2-6-4. Trap Door

A Trap Door is a set of computer instructions that allows a user to bypass the system's normal controls, allowing him / her to modify programs after they have been accepted and made operational. Trap doors are routinely placed in programs by system developers to allow them to modify a program during system development: they are normally removed before the system is put into operation. However, sometimes this code may remain in the program, either accidentally or intentionally. Attackers rely on their knowledge of this extra code to bypass security controls. When these trap doors are used for an unauthorized purpose; they can cause a great deal damage (Cushing, 1994, p. 656; Qureshi and Siegel 1997; Haugen and Selin, 1999).

2021/2022 2021/2022 2021/2022

2-6 -5. Data Diddling

Data diddling is changing data before it enters, as it enters, or after it has already been entered into the INFORMATION. The change can be made to delete data, to alter data, or to add data to the system. Parker (1983) has pointed out that data diddling is the simplest, safest, and most common method used in computer- related crime. It involves changing data before or during its input to computers or during output from computer. The changes can be made by anybody associated with or having access to the processes of creating recording, transporting,

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

encoding, examining, checking, converting, or transforming data that ultimately enter a computer. Examples include forging or counterfeiting documents; exchanging valid computer tapes, cards or disks with prepared replacements; data entry violations, punching extra holes or plugging holes in cards; and neutralizing or avoiding
manual controls (p. 71).

Roufaiel (1990) confirmed that “Data diddling is unauthorized modification, replacement, insertion or deletion of data can occur before or during data input to a computer. This can be done by altering the input media or by direct keying a terminal or console (p. 20).

Cushing (1994) presented the following example of data diddling: “In Denver, a clerk for brokerage altered a transaction to record 1700 shares of Loren worth about $ 2,500 as shares in Long Island Lighting worth more than $ 25,000” (p. 657). Again, Parker (1983) argued that “It is easy to see why data diddling is by far the most common method among known reported cases of computer crime. Why would a crook want to go to all the trouble, complexity and danger of programmed fraud when simply modifying data before or during computer input might accomplish the same results? Crooks are usually not interested in elegance, artistry, or innovation in their crimes, but only in success and the ways they use the gains from their crimes. In choosing methods they are interested in safety, success, and leverage, satisfying their needs for the least effort. The only exceptions to this are those who are more often interested in challenging methods than in gain, or some elite career criminals who take pride in their skills as much as in their gain” (p. 71).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعيدي

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

2-6-6. Data Leakage

According to the Oxford Popular English Dictionary, data leakage is a disclosure of secret information. Cushing (1994) stated that "Data leakage refers to the unauthorized copying of company's data, often without leaving any indication that it was copied. For example, the Encyclopaedia Britannica Company claimed losses in millions of dollars when several of its employees made a copy of its customer list and began selling it to other companies (p. 657). Roufaiel (1990) mentioned that data could be obtained from a computer system by "leaking" it out in small amounts. This might be done by coding the data in a computer in the form of different length of printed lines on the output printer (p. 20).

2-6-7. Logic Time Bomb

A logic time bomb is a program that lies idle until some specified circumstance or particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs or data or both. Most time bombs are written by disgruntled programmers who want to get even with the company.

Cushing (1994) reported that in one case Donald Burleson allegedly broke into his former employer's system two days after he was fired in September 1985. As a former security officer at USPA and IRA Company, he knew everyone's passwords. Using these passwords and his knowledge of computer programming and system controls, he broke into the computer's system and crashed 168,000 records of sales commissions. As a result, company paychecks were held up for a month. The program, which was attached to a legitimate program, was designed to go off at certain time and erase more records every month. The

سليمان طارق شعلان ابراهيم السعدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

bomb was discovered before it could go off by a fellow programmer who was testing a new bonus system for employees. The company had to shut down its computers for two days to find the bomb and diffuse it (p. 657).

2-6-8. Scavenging

Scavenging is unauthorized access to confidential information by searching corporate records. Scavenging methods range from searching trash-cans for printouts or carbon copies of confidential information, to scanning the contents of computer memory. In one of the most famous cases, Jerry Schneider noticed a trash-can full of paper on his way home from a Los Angeles area high school. Rummaging through them, he discovered they contained operating guides for Pacific Telephone and Telegraph's computers. Over time, his scavenging activities resulted in a technical library that later allowed him to steal a million dollars worth of electronic equipment (Cushing, 1994, p. 657).

2021/2022 2021/2022 2021/2022

Parker (1983) reported that "Scavenging, sometimes called browsing, is a method of obtaining information that might be left in or around a computer system after execution of a job. Simple physical scavenging could be the searching of trash barrels for copies of discarded computer listings or carbon paper from multiple-part forms. More technical and sophisticated methods of scavenging involve searching for residual data left in computer after a job is completed" (p. 77, where some examples are presented).

Again, Roufaiel (1990) confirmed that scavenging is the obtaining of data that might be left in or around a computer after execution of the job. Such data includes improperly erased buffer

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعيدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

storage areas used for the temporary storage of input or output data; read data before written on the tape, and discarded computer listings or carbon paper from multiple part forms (p. 20).

Qureshi and Siegel (1997) mentioned that a computer normally does not erase data that is no longer needed. When the user “deletes” some data, that information is not actually destroyed: instead, that space is made available for the computer to write on later. A scavenger may thus be able to steal sensitive data, which the user thought had been deleted, but was actually still available on the computer.

2-6-9. Hacking

Hacking is unauthorized access to and use of computer system, usually by means of personal computers and the telecommunications network. Some hackers do not intend to cause any damage. They are usually motivated by the challenge of breaking and entering into supposedly secure systems and just browsing or looking for things to copy and keep (Cushing, 1994, p. 658; Haugen and Selin, 1999).

Moss (1996) mentioned that in 1995, Citibank revealed that a Russian computer hacker had breached the security system for the US bank’s cash management service, which lets customers move their money electronically to other banks. Once inside the system, using a computer from a remote location, he proceeded to steal more than $10 million by transferring money into the accounts of his accomplices. Citibank said that its control procedures were alerted and the bank was able to monitor the movement of the cash until the criminals had been located. The bank said it recovered most of the money, but lost about

سليمان طارق شبل ابراهيم السعيد
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

$400,000. It was a rare example of a bank admitting it had fallen prey to the growing problem of computer crime.

2-6-10. Computer Viruses

A computer virus is a segment of executable code which attaches itself to an application program or some other executable system component. Viruses are contagious and may easily spread from one system to another. A virus creates copies of itself and inserts them into other programs or data files (Cushing, 1994, p. 659). According to Haugen and Selin (1999), viruses are destructive programs, which attach to a legitimate program and can do significant damage to hard disks, memory and files.

Many viruses lie dormant for extended periods of time without doing any specific damage except propagating themselves. When the hidden program, which leaves no external sign of infection, is triggered, it makes unauthorized alterations to the way the system operates and may cause widespread damage. For example, a virus may destroy or alter data or programs. It can take control of the computer, destroy the hard disk's file allocation table, or keep users from booting the system or accessing the data on a hard disk. Viruses can intercept and change transmissions, print disruptive images or messages on the screen, or cause the screen image disappear. As the virus spreads, it takes up space, clogs communications, and hinders system performance (Cushing, 1994, p. 659).

2021/2022 2021/2022 2021/2022

2-6-11. Computer Worm

A computer worm is similar to a virus, except that it is a program, rather than a code segment hidden in a host program. A worm typically also copies itself and actively transmits itself

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

directly to other systems. It usually does not live very long, but it is quite destructive while it is alive. One of the more destructive worms, written by Robert T. Morris, affected 6,000 computers in a very short time (Cushing, 1994, p. 659).

2-6-12. Superzapping

Superzapping is unauthorized use of utility computer programs to modify, destroy, copy, insert, or deny use of data stored in a computer or computer media. Superzapping derives its name from superzap, a macro / utility program used in many computer centers as a systems tool. Any computer centre that has a secure computer-operating mode needs "break glass in case of emergency". Computer program that will bypass all controls to modify or disclose any of the contents of the computer. (Parker, 1983, p. 75)

Utility programs such as superzap are powerful and dangerous tools in the wrong hands. They are normally used only by systems programmers and computer operators who maintain computer systems. They should be kept secure from unauthorized use. However, they are often placed in program libraries, where they can be obtained by any programmer or operator who knows of the presence and how to use them. Superzapping is regarded as the unauthorized use of special system programs to bypass regular controls and perform illegal acts (Parker, 1983, p 75; Roufaiel, 1990, p. 20; Cushing, 1994, p. 657 and Haugen and Selin, 1999).

A classic example of superzapping, resulting in a $128,000 loss, occurred in a New Jersey bank. The manager of computer operations was using a superzap program to make changes in account balances to correct errors as directed by management.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

The regular error correction process was not working correctly because the demand - deposit accounting system had become obsolete and error- ridden through inattention in expectation of a computer changeover. The operation manager discovered how easy it was to make changes without the usual controls or journal records, and he made changes transferring money to the accounts of three friends. They engaged in the fraud long enough for a customer to find a shortage. Quick action in response to the customer's complaint resulted in indictment and conviction of the perpetrators. The use of the superzap program without any evidence of change to the data files made discovery of the fraud through technical means highly unlikely (Parker, 1983, p 75).

2-6-13. Impersonation (Masquerading)

Impersonation is the taking and using the identity of an authorized person to gain access to a computer, abuse the INFORMATION and commit illegal acts. Haugen and Selin (1999) reported that masquerading occurs when an unauthorized user uses a legitimate user's identification numbers and passwords to gain illegal access to a computer system. According to Qureshi and Siegel (1997) masquerading is use of a written computer program that masquerades or simulates the real program. For example, a program may be written to simulate the log-in screen and related dialogue. When a user attempts to log-in, the program captures the user's identification number and password and displays some error message prompting the user to log-in again. The second time, the program allows the user to log-in and the user may never know that the first log-in was fake.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

2-6-14. Piggybacking

Piggybacking is frequently used to gain access to controlled areas. Physical piggybacking occurs when an authorized employee goes through a door using magnetic ID card and an unauthorized employee behind him / her also enters the premises. The unauthorized employee is then in a position to commit a crime. Electronic piggybacking may also occur. For example, an authorized employee leaves his terminal or desktop on-line and an unauthorized individual uses that opportunity to gain access (Roufaiel, 1990; Qureshi and Siegel, 1997; Haugen and Selin, 1999).

2-6-15. Degausser

Degausser, a device, which looks like a record player without a pickup arm, can be used to create an efficient magnetic field that instantly erases millions of data characters from a disk or tape (Roufaiel, 1990, p. 20).

2021/2022 2021/2022 2021/2022

2-6-16. Damaging File Labels

Internal labels identify the contents of a file to the computer. External labels are affixed to the tape reel or disk cover, to identify the storage device visually. If the external label is destroyed, without the internal label it could be a complete disaster. Internal and external labels can be removed manually or electronically (Roufaiel, 1990, p. 20).

2-7. Summary

In this chapter the physical and information security threats to information were discussed. Sabotage and physical

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

damage of information, which may occur as a result of natural disasters (floods, fires, earthquakes) are major security threats to information. Intentional and accidental human actions might also cause physical destruction of the information, while, sabotage might cause total or partial physical damage to the computer hardware as well as to tapes and disks.

Data modification, destruction, disclosure, and denial of use are the fundamental data and information security threats to information. Most of these security threats result from accidental or intentional human actions. However, the source of information security threats might be “internal” to an organization as result of management and employees’ actions or organization process; or “external”, such as hackers’ actions or natural disasters.

Approaches to abuse the security of information through its main three stages (input, processing, and output) were presented, with examples, illustration and practical cases. Finally, some techniques that have been developed and used by perpetrators to abuse information security were highlighted. In the next chapter, potential security controls that could be used to safeguard Information and to protect information against the various security threats will be discussed.

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Questions of Chapter Two

Please select the correct answer of each of the following questions:

1. Perhaps the most striking fact about natural disasters in relation to AIS controls is that
   a. many companies in one location can be seriously affected at one time by a disaster.
   b. losses are absolutely unpreventable.
   c. there are a large number of major disasters every year.
   d. disaster planning has largely been ignored in the literature.

2. Which of the following is the greatest risk to information systems and causes the greatest dollar losses?
   a. human errors and omissions
   b. physical threats such as natural disasters
   c. dishonest employees
   d. fraud and embezzlement

2021/2022 2021/2022 2021/2022

3. Identify the threat below that is *not* one of the four types of threats faced by accounting information systems.
   a. natural and political disasters
   b. software errors and equipment malfunctions
   c. unintentional acts
   d. system inefficiency

4. A power outage is an example of a(n) ________ threat.
   a. natural and political disasters
   b. software errors and equipment malfunctions
   c. unintentional acts
   d. system inefficiency

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

5. Excessive heat is an example of a(n) ________ threat.
   a. natural and political disasters
   b. software errors and equipment malfunctions
   c. unintentional acts
   d. system inefficiency

6. Which type of threat causes the greatest dollar losses?
   a. software errors and equipment malfunctions
   b. unintentional acts
   c. intentional acts
   d. system inefficiency

7. Logic errors are an example of which type of threat?
   a. natural and political disasters
   b. software errors and equipment malfunctions
   c. unintentional acts
   d. system inefficiency

2021/2022 2021/2022 2021/2022

8. Sahr wants to open a floral shop in a downtown business district. She doesn't have funds enough to purchase inventory and pay six months" rent up front. Sahr approaches a good friend, Zhou, to discuss the possibility of Samr investing funds and becoming a 25% partner in the business. After a lengthy discussion Samr agrees to invest. Eight months later, Samr and Sahr have a major argument. In order for Samr to sue Sahr for fraud, all the following must be true *except*
   a. Zhou's decision to invest was primarily based on Sahr's assertion that she had prior floral retail experience.
   b. Sahr told Samr she had worked at a floral shop for several years, when in fact she did not have any prior experience

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

in floral retail.

c. before Samr invested, Sahr prepared a detailed business plan and sales forecasts, and provided Samr with copies.
d. Zhou's 25% share of the business is worth substantially less than her initial investment.

9. Perpetrators do not typically
   a. attempt to return or pay back stolen amounts soon after the initial theft, but find they are unable to make full restitution.
   b. use trickery or lies to gain the confidence and trust of others at the organization they defraud.
   c. become bolder and more greedy the longer the theft remains undetected.
   d. begin to rely on stolen amounts as part of their income.

10. "Cooking the books" is typically accomplished by all the following *except*
    a. overstating inventory.
    b. accelerating recognition of revenue.
    c. inflating accounts payable.
    d. delaying recording of expenses.

11. SAS No. 99 requires that auditors
    a. plan audits based on an analysis of fraud risk.
    b. detect all material fraud.
    c. alert the Securities and Exchange Commission of any fraud detected.
    d. take all of the above actions.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

12. Intentional or reckless conduct that results in materially misleading financial statements is called
    a. financial fraud.
    b. misstatement fraud.
    c. fraudulent financial reporting.
    d. audit failure fraud.

13. All of the following are required for an act to be legally classified as fraudulent *except*
    a. a falsehood is made.
    b. about a material fact.
    c. to inflict pain.
    d. resulting in a financial loss.

14. Misappropriation of assets is a fraudulent act that involves
    a. dishonest conduct by those in power.
    b. misrepresenting facts to promote an investment.
    c. using computer technology to perpetrate.
    d. theft of company property.

15. *Lapping* is best described as the process of
    a. applying cash receipts to a different customer's account in an attempt to conceal previous thefts of cash receipts.
    b. inflating bank balances by transferring money among different bank accounts.
    c. stealing small amounts of cash, many times over a period of time.
    d. increasing expenses to conceal that an asset was stolen.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

16. Which of the following is *not* an example of the fraud triangle characteristic concerned with rationalization?
    a. revenge against the company
    b. intent to repay "borrowed" funds in the future
    c. sense of entitlement as compensation for receiving a lower than average raise
    d. belief that the company won't suffer because an insurance company will reimburse losses

17. Insiders are frequently the ones who commit fraud because
    a. they are more dishonest than outsiders.
    b. they need money more than outsiders.
    c. they are less likely to get caught than outsiders.
    d. they know more about the system and its weaknesses than outsiders.

18. Which of the following is *not* a management characteristic that increases pressure to commit fraudulent financial reporting?
    a. close relationship with the current audit engagement partner and manager
    b. pay for performance incentives based on short-term performance measures
    c. high management and employee turnover
    d. highly optimistic earnings projections

19. Researchers have compared the psychological and demographic characteristics of white-collar criminals, violent criminals, and the general public. They found that
    a. few differences exist between white-collar criminals and the general public.

سليمان طارق شعبان ابراهيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

b. white-collar criminals eventually become violent criminals.
c. most white-collar criminals invest their illegal income rather than spend it.
d. most white-collar criminals are older and not technologically proficient.

20. Identify the *opportunity* below that could enable an employee to commit fraud.
a. An employee's spouse loses her job.
b. An employee has a close association with suppliers or customers.
c. An employee suddenly acquires lots of credit cards.
d. An employee is upset that he was passed over for a promotion.

21. Which of the following is a financial pressure that could cause an employee to commit fraud?
a. a feeling of not being appreciated
b. failing to receive a deserved promotion
c. believing that their pay is too low relative to others around them
d. having a spouse injured in a car accident and in the hospital for several weeks

22. Which of the following fraudulent acts generally takes most time and effort?
a. lapping accounts receivable
b. selling stolen inventory to get cash
c. stealing inventory from the warehouse
d. creating false journal entries to overstate revenue

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شعبان ابراهيم السعدني

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

23. In many cases of fraud, the ________ takes more time and effort than the ________.
    a. concealment; theft
    b. theft; concealment
    c. conversion; theft
    d. conversion; concealment

24. Which of the following is the *best* way to hide theft of assets?
    a. creating "cash" through the transfer of money between banks
    b. conversion of stolen assets into cash
    c. stealing cash from customer A and then using customer B's balance to pay customer A's accounts receivable
    d. charging the stolen asset to an expense account

25. Which fraud scheme involves stealing customer receipts and applying subsequent customer cash payments to cover the theft?
    a. kiting
    b. laundering
    c. lapping
    d. bogus expense

26. One fraudulent scheme covers up a theft by creating cash through the transfer of money between banks. This is known as
    a. lapping.
    b. misappropriation of assets.
    c. kiting.
    d. concealment.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شعبان ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

27. Which characteristic of the fraud triangle often stems from a lack of internal controls within an organization?
    a. pressure
    b. opportunity
    c. rationalization
    d. concealment

28. Which situation below makes it easy for someone to commit a fraud?
    a. placing excessive trust in key employees
    b. inadequate staffing within the organization
    c. unclear company policies
    d. All of the above situations make it easy for someone to commit a fraud.

29. This component of the fraud triangle explains how perpetrators justify their (illegal) behavior.
    a. pressure
    b. rationalization
    c. concealment
    d. opportunity

30. The *most* efficient way to conceal asset misappropriation is to
    a. write-off a customer receivable as bad debt.
    b. alter monthly bank statements before reconciliation.
    c. alter monthly physical inventory counts to reconcile to perpetual inventory records.
    d. record phony payments to vendors.

سليمان طارق شلبي ابراهيم السعيدي
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

31. Which of the following is *least likely* to result in computer fraud?
    a. releasing data to unauthorized users
    b. allowing computer users to test software upgrades
    c. allowing computer operators full access to the computer room
    d. storing backup tapes in a location where they can be quickly accessed

32. How does the U.S. Justice Department define computer fraud?
    a. as any crime in which a computer is used
    b. as any act in which cash is stolen using a computer
    c. as an illegal act in which a computer is an integral part of the crime
    d. as an illegal act in which knowledge of computer technology is essential

2021/2022 2021/2022 2021/2022

33. Why is computer fraud often much more difficult to detect than other types of fraud?
    a. because massive fraud can be committed in only seconds, leaving little-to-no evidence
    b. because most perpetrators invest their illegal income rather than spend it, concealing key evidence
    c. because most computer criminals are older and more cunning than perpetrators of other types of fraud
    d. because perpetrators usually only steal very small amounts of money at a time, requiring a long period of time to pass before discovery

سليمان طارق شبل ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

34. Why is computer fraud often more difficult to detect than other types of fraud?
    a. Rarely is cash stolen in computer fraud.
    b. The fraud may leave little or no evidence it ever happened.
    c. Computers provide more opportunities for fraud.
    d. Computer fraud perpetrators are just more clever than other types of criminals.

35. Why do many fraud cases go unreported and unprosecuted?
    a. Major fraud is a public relations nightmare.
    b. Fraud is difficult, costly, and time-consuming to investigate and prosecute.
    c. Law enforcement and the courts are often so busy with violent crimes that little time is left for fraud cases.
    d. all of the above

36. The fraud that requires the least computer knowledge or skill involves
    a. altering or falsifying source data.
    b. unauthorized use of computers.
    c. tampering with or copying software.
    d. forging documents like paychecks.

37. The simplest and most common way to commit a computer fraud is to
    a. alter computer input.
    b. alter computer output.
    c. modify the processing.
    d. corrupt the database.

سليمان طارق شبل إبراهيم السعدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

38. Downloading a master list of customers and selling it to a competitor is an example of
    a. data fraud.
    b. output theft.
    c. download fraud.
    d. fraudulent financial reporting.

39. Most frauds are detected by
    a. external auditors.
    b. hotline tip.
    c. internal auditors.
    d. the police.

40. Which of the following will *not* reduce the likelihood of an occurrence of fraud?
    a. encryption of data and programs
    b. use of forensic accountants
    c. adequate insurance coverage
    d. required vacations and rotation of duties

2021/2022 2021/2022 2021/2022

41. ________ is a simple, yet effective, method for catching or preventing many types of employee fraud.
    a. Requiring all employees to take annual vacations
    b. Monitoring employee bank accounts and net worth
    c. Monitoring employee behavior using video cameras
    d. Explaining that fraud is illegal and will be severely punished to employees

سليمان طارق شعبان ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

42. Which of the following is *not* a way to make fraud less likely to occur?
    a. Adopt an organizational structure that minimizes the likelihood of fraud.
    b. Create an organizational culture that stresses integrity and commitment to ethical values.
    c. Create an audit trail so individual transactions can be traced.
    d. Effectively supervise employees.

43. Which of the following is not a way to reduce fraud losses?
    a. Conduct periodic external and internal audits.
    b. Maintain adequate insurance.
    c. Use software to monitor system activity.
    d. Store backup copies of program and data files.

سليمان طارق شبل ابراهيم السعدنى

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Chapter Three
Information Security Controls

3-1. Introduction

In the previous chapter the main security threats to information were discussed. In this chapter, potential security controls that might be implemented to eliminate these threats or reduce their expected losses will be presented. The arguments regarding the different perspectives of security controls classifications will be considered and the objectives of information security controls will be highlighted. The security controls will be classified under eleven main security control groups; and the individual countermeasures of security controls in each of these groups will be discussed in detail.

3-2. Information Security Controls: An Overview

The increased growth in real-time and on-line data processing in information has made access to these systems more available and easier for many users. Therefore, implementing adequate security controls over organizations information (especially programs and data files) and their related facilities used to handle, record, process, store and distribute information has become a necessity.

2021/2022 2021/2022 2021/2022

A review of the literature reveals diverse views regarding the classification of information security controls. Security controls of information could be classified according to their *purpose* to: deter, prevent, detect and correct security threats. The objective of deterrent security controls is to create an atmosphere of control compliance, while preventative security controls should be designed to reduce the possibility of an attack. Once a

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

system has been violated, detective controls could help in identifying the occurrence of harm and security breach. Corrective controls serve to reduce the impact of the threat after a loss has occurred.

Thus, the purpose of corrective controls is to aid in recovery from damage or in reduction of the harmful effects of its occurrence (for more details, see, Parker, 1981; or Qureshi and Siegel, 1997).

Security controls could also be categorized according to their association with the data *processing stages* into: input, processing, storing and output security controls. The purpose of input controls is to ensure that each transaction is authorized, processed correctly and processed only once. Processing controls should be used to ensure that transactions entered into information are valid and accurate, that external data are not lost or altered and that invalid transactions are reprocessed correctly. Output security controls are used to ensure that no unauthorized copies of output were made, and that the printouts are directed only to authorized persons. Storage security controls ensure that all stored data and programs are secured against unauthorized access, manipulation, alteration and disclosure.

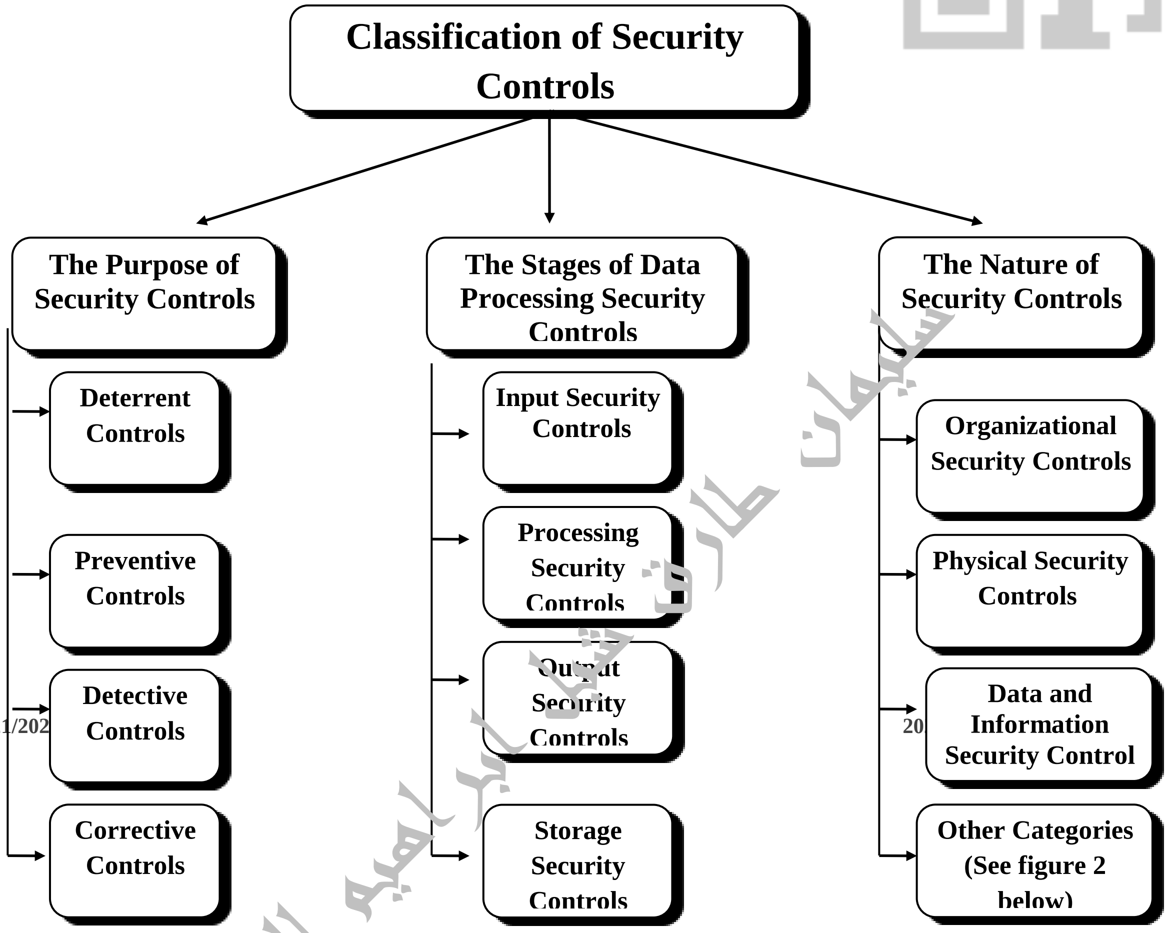
Alternatively, security controls could also be classified according to their *nature*, including for example, organizational, physical access, data and data integrity, software, off-line programs and data security controls (Figure 3-1).

Security controls are an especially important issue for banks and financial institutions. It is argued that security, mainly as the result of the Bank Protection Act, has focused on the physical protection of banks' assets and customers. Additionally, security has had responsibility for investigating losses, handling

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

matters of internal affairs and working with law enforcement agencies.


Classification of Security Controls
The Purpose of Security Controls
Deterrent Controls
Preventive Controls
Detective Controls
Corrective Controls
The Stages of Data Processing Security Controls
Input Security Controls
Processing Security Controls
Output Security Controls
Storage Security Controls
The Nature of Security Controls
Organizational Security Controls
Physical Security Controls
Data and Information Security Control
Other Categories (See figure 2 below)

(Figure 1)

(Classification of CAIS Security Controls)

However, information security has become a major management concern as organizations depend more on electronic data transactions. More concern should be directed to the identification and verification of transaction documentation, in addition to the protection of sensitive organization data and

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

information. The importance of security controls has increased in organizations as a result of the increasing security threats to organizations, as they grow geographically, create new products and services, acquire new businesses and harness emerging new technologies.

Hester (1998) has noted that since the dawn of the computer age over four decades ago, many tools have been developed to safeguard equipment and services. Concern has grown steadily regarding electronically stored and transmitted information. Older, conventional devices include locks, alarms, access controls and closed-circuit television monitors. More recent developments include specific methods such as passwords, encryption systems, electronic firewalls and complex systems for assuring authorization and protecting information against insiders and hackers.

Qureshi and Siegel (1997) argued that controls should be used and implemented to reduce the probability of attack on computer security. As additional controls are placed, the overall operating costs are more likely to increase. Therefore, cost-benefit considerations require a careful balance of controls.

2021/2022 2021/2022 2021/2022

In Boritz's (1999) view, testing should be carried out prior to full implementation of information security controls to ensure that the selected controls operate as specified and, in particular, that:

- Authorized users are accepted by the computer system;
- Unauthorized users are rejected by the computer system;
- Access times are within the acceptable range initially specified;

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Audit trials are adequate for detecting unauthorized access to the system and for identifying the individuals responsible; and
- Back-up and recovery procedures are operated correctly and are secured against unauthorized modifications of program and data files.
- In the following section, the main objectives of information security controls will considered.

3-3. The Objectives of Information Security Controls

As with classification of control types, there are rival depictions of the essential objectives of security controls. According to Cloud (1990) the formal dictionary meaning of control is to regulate, operate, direct or verify. In the realm of information resource controls, security, privacy, integrity, availability and recoverability are the factors that must be regulated.

2021/2022 2021/2022 2021/2022

Each element should be regulated by introducing its own particular blend of control mechanisms, such as software, hardware, and procedures. Therefore, information is being adequately controlled if each of these five elements is present at a sufficient level to fit each information component's specific needs (p. 14).

Again, Courtney (1987) confirmed that the common reasons for wanting adequate computer security control are to preserve the integrity, availability and the means for using the organization's data. He listed the objectives of security controls as follows:

سليمان طارق شبل عبد العليم السعيدي

30006101601571 30006101601571 30006101601571

- to limit data processing (DP) users to accessing only those resources and processes which they need to accomplish

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

their assigned tasks, thereby limiting the opportunities for potential abuse;

- to hold authorized users accountable for their activities;
- to preserve the confidentiality of data, which must not be disclosed to unauthorized persons;
- to protect honest, careful employees from suspicion about improper handling of the organization's data;
- to minimize the temptation for misuse of data processing facilities to which people might be inadvertently exposed;
- to limit the disruption of the organization's infrastructure due to DP malfunction;
- to preserve the continuity of the organization's computer dependent functions if that normal DP capability is lost (Lee, 1995).

Boritz (1999) believed that the objectives of computer security controls are to provide reasonable assurance that:

- Only valid /authorized data is collected and recorded;
- All such data are accurately recorded;
- Errors are detected and promptly corrected; and
- Results or summary figures can be traced to original source data.
- Accordingly, security controls provide a protection to an organization against:
- Unauthorized access to the information system by persons outside the entity;
- Unauthorized access to, and use of, the system by internal users; and
- Interruptions in information systems processing.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

However, information security controls should be designed to ensure that all accounting data on files are properly maintained between transaction updates (***File Controls***); and that valid transactions, and only valid transactions, are processed and recorded completely and accurately in the accounting records (***Transactions Controls***).

Again, Jenkins et al. (1992) have summarized the important security control considerations related to the application controls of the information as follows:

- **File continuity:** To ensure that, once data is updated to a file, it remains correct and current on the file. File continuity controls might operate over the total balances on the file, or over the detailed items recorded within the file.
- **Asset protection:** To protect assets, there may be both direct control over assets custody and movements and controls over the security of data stored on files (which seek to prevent misappropriation of assets or manipulation of data through unauthorized access).
- **Completeness of input:** Completeness of input is dealt with separately from accuracy of input. The distinction is made because different techniques are used to control completeness (that is, all the transactions) and accuracy (that is, the data for each transaction).
- **Authorization of transactions:** Checking and authorization in computer systems introduce new considerations of timing, on-line authorization, access controls and

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

whether the checking and authorization are programmed or manual.

- **Computer–generated data:** The computer itself might be programmed to generate data, either following the input of a signal or by processing of a transaction creating a specified condition. The completeness, accuracy and validity of generated data will depend on the effectiveness of controls over all of the data used in the generation process and the correct operation of the process itself.
- **Update of data onto files**: Following input data will be processed by the application program and updated into files. Control over the completeness and accuracy of updating may be ensured by the control over input. Where this is not the case, there may be separate controls over update and in some cases reliance may be placed on program procedures, particularly to ensure the accuracy of update of specific fields of data.
- **File creation:** When new applications are implemented, the auditor might wish to satisfy himself, during the audit of accounting period in which the file were initially created, that the opening transaction and standing data was completely and accurately set up within the new files.

Boritz (1999) stated that security control procedures are those policies and procedures that management has established, in addition to the control environment and accounting system, to provide reasonable assurance that an entity's established objectives would be achieved.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Control procedures have various objectives and are applied at various organizational and data processing levels. Generally, they might usefully be categorized as procedures pertaining to:

- Proper authorization of transactions and activities: such as general or specific approval of transactions and approval for the re-entry of transactions rejected by the computer;
- Adequate segregation of duties: such as separating the responsibility for custody of assets from the responsibility for the related record-keeping, and separating computer programming from computer operations;
- Adequate documents and records: such as pre-numbered documents;
- Adequate safeguards over access to and use of assets and records: such as secured facilities;
- Independent checks on performance: such as clerical checks, reconciliations, computer-programmed editing controls, management review of reports that summaries the detail of account balances (such as an aged trial balance of accounts receivable) and user review of computer-generated reports.

In the next section the main types of information security controls will be discussed. The security controls of information have been classified under eleven main security control groups.

3-4. The Main Types of Information Security Controls

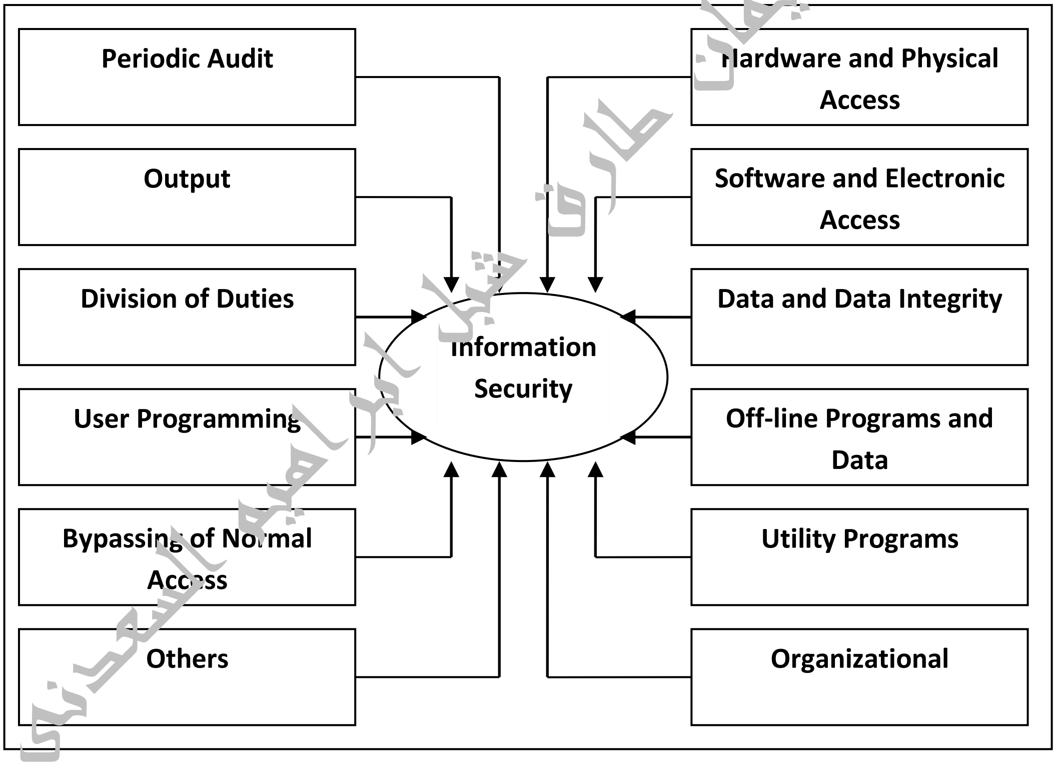
FFIEC (1996) stated that information is one of the most important of the organization's assets, therefore, protecting or securing information and facilities that process and maintain information is a vital operation. The consequences of security deficiencies are lost business, damaged reputation, fiduciary

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شلبى احمد السعدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

losses, lost assets, and possibly lost trade secrets. Security controls are needed to safeguard information from unauthorized or accidental modification, destruction, and disclosure, and ensure timeliness, availability and usability of data (Ch. 14).

Figure 3-2 represents the researcher's point of view regarding the classification of information security controls in the light of the classifications already discussed. The main categories of security controls concerned with the organization's information and all its elements will be discussed in the following sections.



2021/2022

سليمان طارق شبل ابراهيم السعدني

(Figure 3-2)
(Information Security Controls)

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

3-4-1. Organizational Security Controls

Buttross and Ackers (1990) argued that the majority of security problems of information have organizational aspects. However, most such problems result from a lack of segregation of duties. Rotation of duties and mandatory vacations could alleviate some security problems and enhance the likelihood of detecting errors and irregularities. However, if duties cannot be rotated, personnel controls such as background checks and bonding become more significant. The importance of employees' background checks cannot be overemphasized. Examination of fraudulent acts reveals that such acts are often committed by employees with histories of dishonesty; yet the backgrounds of these employees had never been checked.

Qureshi and Siegel (1997) suggested that specific procedures should be established for recruiting and hiring a organization's employees, especially accountants and computer data processing professionals. A security investigation should include contacting the applicant's work references, checking the applicant's background with the appropriate authorities and verifying the applicant's school references. Organizations should impress upon new employees the importance of computer security with respect to every phase of computer data processing.

Qureshi and Siegel also suggested that educational seminars should be scheduled to indoctrinate new employees, where security professionals could communicate the organization's rules and procedures. Employees should be informed of the negative impact that loss of data and equipment has on their organization. In addition, formal performance evaluation systems should be in place to ensure that the employees' performance and skills are routinely reviewed. An

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

effective review procedure can help prevent job frustration and stress. It can also help maintain employee morale (ibid.).

According to FFIEC (1996) control of sensitive forms is another important security concern. Printed forms of a negotiable nature (such as checks and stock certificates) and signature plates are vulnerable to misapplication and must be secured. Appropriate controls include dual control locks for forms within a secure location, and inventory records that specify data, time of access, and any personnel accessing the secure location.

The supply of forms should be issued according to scheduled production runs. Periodic inventories should be completed for all forms and any checks that are voided during processing should be distributed to appropriate users for accountability (Ch. 14).

3-4-2. Hardware and Physical Access Security Controls

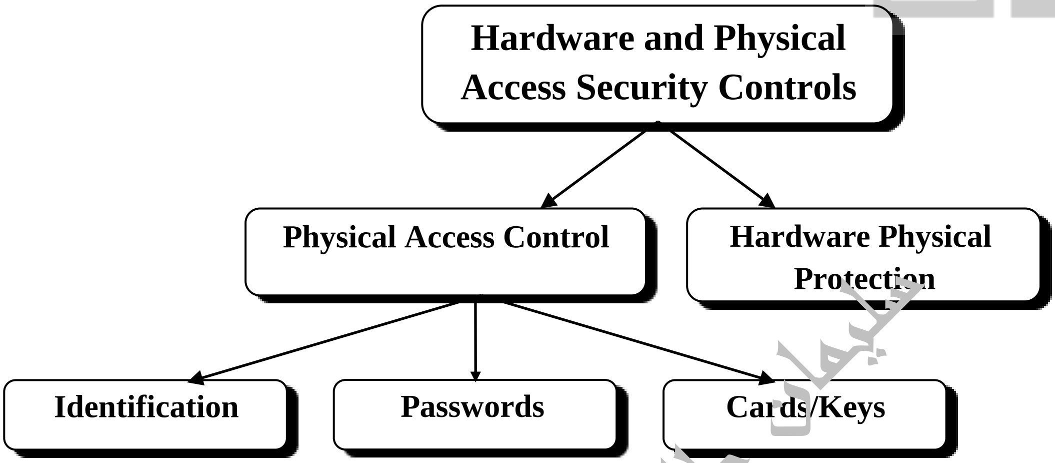
Physical access security controls are usually the first line of defense in an organization's information, usually used in conjunction with other types of access controls. The main objective of hardware and physical access security controls is physically to protect the organizations’ computer hardware and its related facilities from theft or other prospective damage that might occur as a result of sabotage or fire; further, to protect data and information held inside these computers from destruction, modification, alteration, unauthorized distribution and theft. Therefore, the two main areas of physical security controls are:

- Physical protection of the organization’s hardware from theft, fire, sabotage or other prospective damage;
- Protecting the data and information inside information against the various potential security threats (such as

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

destruction, modification, alteration and unauthorized distribution of data and information), by restricting physical access to authorized persons (see figure 3-3).


Hardware and Physical Access Security Controls
Physical Access Control
Hardware Physical Protection
Identification
Passwords
Cards/Keys

(Figure 3-3)
(Hardware and Physical Access Security Controls)

Henry (1997) argued that physical security of information and their related facilities is thus a fundamental element of information security controls. It encompasses the business, equipment and personnel. Computers and the information that they contain or process are valuable assets. Locking buildings and rooms that contain these assets is the most basic method of deterring losses. If not prohibitively costly, alarms, video cameras and motion detectors should be included as part of the security system, to monitor sensitive and high-risk areas against unauthorized individuals. As computers become more and more portable, it becomes a necessity to secure them to tables and desks with cables and plate locks.

2021/2022 2021/2022 2021/2022

Computer media such as disks and tapes should not be neglected in this process: locking these items in a secure storage

30006101601571 30006101601571 30006101601571

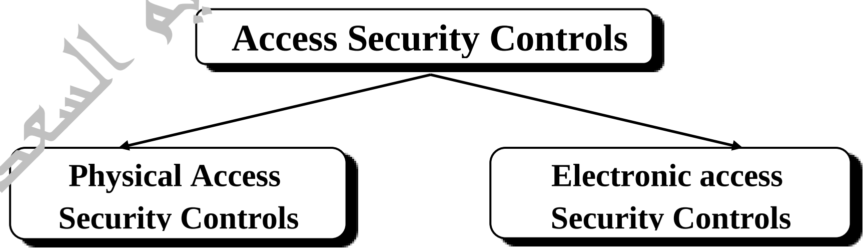
soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

area is recommended. It is extremely important to install some form of fire protection and detection, to safeguard both data and equipment; and to install an uninterrupted power supply to maintain processing and data integrity.

Buttross and Ackers (1990) have stated that computer and data, whether on diskettes or hard disk, are vulnerable to damage from electricity, fire, water, smoke and other pollutants. There are many security controls available to protect against these dangers.

Elementary surge suppressers or noise filtering devices could protect against power surge and spikes. Line conditioners might be used to smooth out power and uninterruptible power supply units could be used supply power during outages. Halon fire extinguishers could reduce losses from fire and water damage might be avoided or minimized by using waterproof covers and by placing the computers away from sprinkler systems. Finally, smoke, flood, even coffee and other potential pollutants, should be kept away from computers. If smoking is not prohibited, a small fan should be used to keep smoke away from the hardware and diskettes.

2021/2022 2021/2022 2021/2022


Access Security Controls
Physical Access Security Controls
Electronic access Security Controls

(Figure 4)
(Types of Access Security Controls)

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

In Boritz' (1999) view, the minimum physical security control standards are:

1. Hardware facilities within information systems processing should be physically separated from other departments in the entity.
2. Physical access to hardware facilities within information systems processing should be restricted to authorized personnel.
3. There should be procedures to ensure that environmental conditions (such as temperature and humidity) for hardware facilities are adequately controlled.

Boritz (1999) also argued that physical access controls play a crucial role in protecting computer-based systems. While, with the proliferation of microcomputers and the need to access information systems from remote locations, physical access controls are becoming relatively less important (with the focus of attention shifting towards electronic access controls), physical access controls still remain an important and an integral part of a comprehensive security system. Buttross and Ackers (1990) confirmed that whenever a hard disk is being used, security is a vital concern. In the absence of a hard disk, the ease and low cost of installation and replacement make elaborate precautions unnecessary.

When a hard disk is used, theft prevention techniques could include:

- Limiting computer access to employees with a defined need;
- Installing computers only in areas that are locked and kept under surveillance when not in use;
- Bolting computers to disks or tables;

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Placing lockable covers on computers;
- Installing alarms and motion detectors in areas with high concentration of computer equipment;
- Placing internal trip alarms inside computers.

Qureshi and Siegel (1997) suggested that physical access to information could be restricted using three general methods: identification, passwords and cards/keys. These methods will be briefly presented in the following:

Identification: Identification is based on comparing the physical characteristics of the individual with previously stored information. For example, an individual's signature, personnel number, code, voice print, palm print, fingerprint, teeth print or other personal trait should be verified before allowing access. Secondary authentication, such as the year the user was married or the mother's maiden name, might be required for highly sensitive information.

Passwords: Passwords could be used to restrict physical access to information to authorized users only. However, the use of passwords to restrict access to information will be discussed in more details in the software and electronic assess security controls section.

Cards/Keys: Physical access to computer terminals and computer rooms could be restricted by using cards, keys, or badges. Improper access might be signaled by an alarm.

Unauthorized access patterns should be evaluated. Smart cards could be also used, in which the user enters both the identification number and a randomly generated code, which changes each time it is used, or over a specified time period.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Adequate physical security controls should be implemented over access to computer resources. The degree of controls required will depend on the sensitivity of the processing data and files. Access to the computer room should be controlled so that only those staff who need to be there are able to enter. This includes operations staff and, on occasions and under supervision, system software staff for system maintenance purposes. Such access might be controlled by magnetic security badges, combination locks, keys or by intrusion detection systems.

According to Bortiz (1999) access security controls could be categorized in two main groups: physical access security controls and electronic access controls. Physical access controls are mainly used to ensure that an organization's computer resources and facilities are safeguarded against physical abuse, damage and destruction, while electronic access controls are used to safeguard the integrity and confidentiality of information in information. However, physical and electronic access security controls should be used in combination to achieve the appropriate security level for an organization.

Bortiz mentioned that an organization should consider the following points in selecting the appropriate access security controls:

- Compatibility of the control technique with the existing control system;
- Adaptability to future operating practices;
- Effectiveness for the intended purpose;
- Relative cost of the device or technique;

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعيدى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Number of Type I errors (that is, admitting the wrong users) and Type II errors (that is, rejecting the right users) incurred by the device or technique;
- Average response time to access the computer;
- Ability to manage the complexities of multiple users in a time-sharing computer environment; and
- Ability to satisfy ergonomic issues when using the particular authentication device or technique (Ibid.).

Physical security could be also achieved by restricting physical access to terminals and by requiring the use of an appropriate key or badge to activate the terminal. However, granting and revoking the means of physical access (such as organization badges, keys, or swipe cards) should be under the control of a sufficiently senior member of staff; and unissued keys or badges should also themselves be physically controlled.

3-4-3. Software and Electronic Access Security Controls

2021/2022 2021/2022 2021/2022

Controlling access to information is an important element of security controls. If access to computers is uncontrolled, a disgruntled employee could easily destroy what might have taken months to recreate. Controlling physical access to the computer and password protection would reduce this risk; while physical access controls are considered fundamental elements of physical security controls, electronic access controls and software security controls are equally important elements. Access to the organization’s information might occur internally by employees to perform their daily work, or externally, by the organization’s customers through the Internet, dial-up and ATMs.

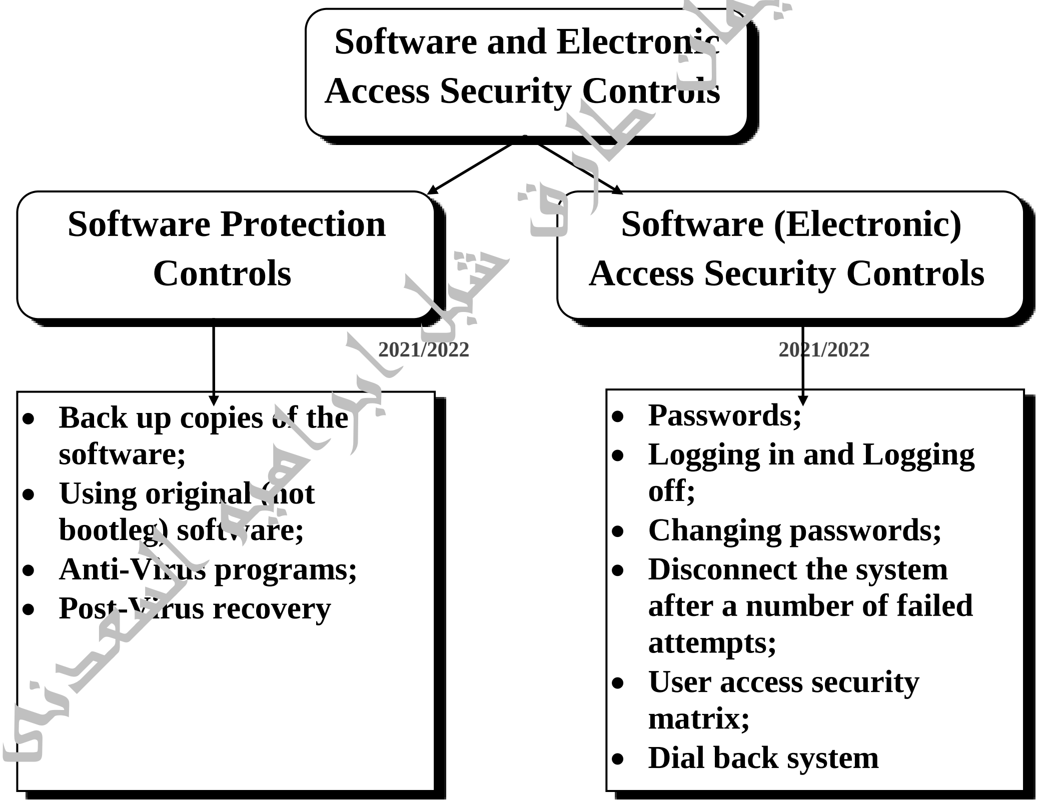
30006101601571 30006101601571 30006101601571

The spread of on-line banking makes it easier for banks to provide interactive, real-time payment and loan services to

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

consumers. Accordingly, cash deposits, withdrawals, transfers and granting of credit can be carried out electronically through the Internet. *Bank Management* (1990) mentioned that permitting customers to access bank's database creates serious risk exposure. Information security is critical under these conditions.

However, audit and security professionals must participate as these products and systems are developed. Involvement will mean making sure controls are in place to ensure the integrity and security of information, through the identification of authorized users.


Software and Electronic Access Security Controls
Software Protection Controls
Software (Electronic) Access Security Controls
Back up copies of the software;
Using original (not bootleg) software;
Anti-Virus programs;
Post-Virus recovery
Passwords;
Logging in and Logging off;
Changing passwords;
Disconnect the system after a number of failed attempts;
User access security matrix;
Dial back system

2021/2022 2021/2022 2021/2022

(Figure 3-5)
(Software and Electronic Access Security Controls)

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Securing electronic funds transfer (EFT) and credit card transactions on the Internet have become important security issues for banks. A customer's credit card is used to pay for electronic cash transactions conducted with online vendors. Through EFT, if properly implemented, buyers and sellers are able quickly and safely to exchange digital money. Encrypted monetary units are exchanged between the vendor, bank, and service company.

Authorizations are coded and decoded using a public key system which must be employed to protect them from misuse. Some controls are straightforward and obvious. For example, access to information and its related facilities should be disconnected after a prescribed number of unauthorized attempts to gain access by a user (using an invalid password or an incorrect PIN number). However, the underlying objectives of software and access security controls should be:

- Protecting the accounting software from prospective damage and possible risks; and
- Protecting information against unauthorized access to data, files and records.

2021/2022 2021/2022 2021/2022

The first objective could be achieved by using only the original copies of software (not bootleg software); by making at least two back-up copies of the new software when it is purchased; by installing Anti-Virus programs that automatically check memory every time a system is started; by scanning any media before using it; and by using Post-Virus recovery in the event of something wrong occurring with the accounting software. The second objective could be achieved by using unique passwords; by changing these passwords regularly; by ensuring that the system is automatically disconnected after a

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

prescribed number of failure attempts and by implementing a user access security matrix program, which could help in determining who accessed the system and when. The security controls in each group will be briefly discussed in the following sections:

3-4-3-1. Software Security Controls

The main objective of software security controls is to protect all programs and software packages from the potential security threats that might cause a total or partial damage to it.

The most important software security controls (creating backup copies of software, using original software and using virus protection / detection software) will be briefly discussed in the following subsections:

3-4-3-1-1. Create Spare Copies (Backups) of Software

Back-up copies of computer programs should be maintained to permit timely recovery in the event that the operational copy of the programs was corrupted or destroyed. Program back-ups should be made each time the software is modified. Henry (1997) argued that, as accounting systems become less and less document driven and place more reliance on electronically stored data, the concept of backing up the financial and non-financial data becomes very important to business survival. Most personal computer operating systems have a method of backing up the hard drive to floppy disks. However, as the size of storage on these machines continues to grow, this has become a slow process. Tape and Zip drives are now available at an affordable price to speed the backup process and supporting software enables the user to set a given interval or time to

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

perform a regular backup procedure. Several series of back up should be maintained for security purposes and should be stored off site.

Buttross and Ackers (1990) suggested that the best protection for software is to create working copies for daily use and backups for on-site storage in case the working copy is destroyed. Like the original, the backups should have write protection in place. This allows the originals to be stored off-site (for example, in a safe deposit box or at the nearest bank branch). Copying of software should be limited to that allowed by the licensing agreement. Unauthorized copies can subject the violator and organization to severe penalties (p. 32).

3-4-3-1-2. Avoiding Bootleg Software

Buttross and Ackers (1990) recommended that organizations should prohibit their employees from using bootleg software; such software could subject the organization to another potential problem, with dire consequences of computer viruses. Computer viruses could transfer themselves from a disk to the system and to all subsequently entered software disks without the knowledge of the user. These viral programs could destroy the software and data on every disk with which they come into contact (p. 32). Crucially, the organization would have no mechanism or redress, against either the supplier of the legal software or the bootlegger.

2021/2022 2021/2022 2021/2022

3-4-3-1-3. Virus Protection / Detection Software

As discussed in the previous chapter, computer viruses are lines of code that reproduce and attach themselves to other programs. In some cases they simply fill memory and slow down

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

system processing. In other cases they are designed to destroy or change data and programs. Viruses may be introduced through external communications systems or by using virus infected floppy disks or CD-ROM. Virus protection / detection software is usually included in newer computer operating systems, and is readily available from reputable vendors for older systems. Anti-virus utility programs provide protection by restricting viral access to the primary memory and hard disk, detecting the virus, and preventing damage to the system's files. They are recommended for testing new software and upgrades on an isolated computer. Anti-virus software should be updated on a regular basis to enable detection of newer viruses. Such software should be set to automatically scan computer files when the system is first turned on. Employees should also be trained to scan any external media they introduce to the system during the daily activities (Roufail, 1990 and Henry, 1997).

3-4-3-2. Electronic (Logical) Access Security Controls

2021/2022 2021/2022 2021/2022

Limiting and restricting logical access to data and programs through computer and communications devices is the second level of information security controls (the first line of defense is physical access controls). Logical access security controls become increasingly important with the growth of remote access to computers via modems. Passwords, user access control matrix, dial back techniques and security packages could be very useful tools to restrict logical access to information only to authorized individuals. Such logical access security controls will be highlighted in the following sections.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

3-4-3-2-1. Passwords

Kay (1994) argued that when one hears the term "security", the first thing which comes to mind is a password. However, there are at least three different methods by which systems can check on users at log-in time: by making use of something they know, something they have, or something they are. These three methods will be briefly described below:

1. Something They Know

The "something they know" method is typified by the user ID (the account number) and password. Some systems might ask for other personal information, such as a person's mother's maiden name. The idea is that this knowledge is not written down and is unlikely to be available to an intruder.

2. Something They Have

2021/2022 2021/2022 2021/2022

The "something they have" method adds a second level of confidence to the authentication process. It requires that the user possess some physical object in order to gain access to information. This object might be simple, such as a magnetic-stripe plastic card.

3. Something They Are

The third and most secure level of authentication is the "something they are" method. It involves some unique and unforgettable aspect of an individual's body. Kay (1994) mentioned that, in the past, biometric authentication such as fingerprints, palm prints, or retinal patterns of the eye, signature verification or voice recognition have been used. More recently,

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

a system that recognizes keyboard–typing patterns has appeared from Los Angeles–based Phoenix Software International. Another new technology can reportedly read infrared facial patterns from passers-by, using a simple video camera for image capture; it is being developed by Neurometric Vision Systems, of Deerfield Beach, Florida (p. 166).

Jenkins et al. (1992) argued that in simple information the use of the appropriate password might enable the user to obtain, by report or on screen any record on the file and to input any data.

In more complex information, the password system could be used both to limit users to specified terminals and data and to limit terminals to specific files. Thus, for example, in the case of an account receivable file, one password might permit the display or input of the name and address data while; another password might be needed to display or input credit limits. At the same time, only certain terminals might accept the second password needed to display or input credit limits. Attempted violations should be recorded, printed out and investigated promptly (p. 240).

2021/2022 2021/2022 2021/2022

Under no circumstances should a organization's employee hold two passwords which might enable him / her to perform different conflicting tasks. The additional passwords should be used only in emergency cases and under very conservative conditions. The organization should hold or maintain a password record, to control the handling and allocation of passwords (both essential and additional). This record should include data about the employee name and position; the user ID; the task that to be performed; the date of receiving the password; the password type (essential or additional); the employee's signature on receiving

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

the password; and his agreement to protect it and keep it secret. This record should be kept in the manager's office, under a double control by two responsible individuals in the organization; one of them should be the organization's manager.

There is a real need to implement suitable controls over the design, maintenance and issue of passwords. Password tables should be controlled, issued and amended by staff independent of computer operations and terminal usage. This activity is often reserved to internal audit.

According to Jenkins et al. (1992), it is necessary to ensure that passwords cannot be obtained by an unauthorized person. For this reason, details of passwords should not be printed on the terminal at the time they are input and the system should "log-off" a terminal after a limited number of failed attempts to input a password or after a limited period of inactivity. Password tables stored in a computer should preferably be held in unintelligible code form. It is also advisable to change passwords periodically, and they should be revoked immediately when the staff leave or transfer (p. 241).

2021/2022 2021/2022 2021/2022

3-4-3-2-2. User Access Control Matrix

A user access control matrix could be used to control the capability of security software. This program determines who has access to data and programs and defines what is the nature of that access (whether able to read data, able to change data, able to delete data). This is particularly important with the increasing use of databases and electronic data interchange. Security software can also record all user activities and the terminal used to access data or programs. However, this activity log must be carefully monitored to provide the security desired (Henry, 1997).

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Access to a particular type of information, as well as the functions that a particular user is allowed to perform upon it, should be based on the user's needs, responsibilities and position in the organization. Organizations should operate on a "need to know" basis, by restricting access to information to authorized individuals who are required to perform specific authorized tasks. Sharing of access paths by different users should be kept at the minimum level to avoid unauthorized access to information not required by users to complete their tasks or assignments.

Boritz (1999) argued that the various functions that a particular user might be permitted to perform upon the information include reading, adding, changing, creating, appending, and deleting. Additionally, a zero-level access function might be employed in instances where a user's authorization to access information has been revoked, either temporarily or permanently.

Again, Boritz (1999) confirmed that plastic magnetic-strip cards are increasingly used for controlling access and verifying the authenticity of the user. Bank credit cards, automatic teller machine cards, and cards for authorizing bank teller transactions are common examples. Plastic cards carry a fixed password that is invisible to the user and difficult to duplicate. Plastic cards are very appealing, due to their low cost and high security features. However, cards can be lost, stolen or duplicated, and therefore, are frequently used in conjunction with passwords or personal identification numbers (PIN).

2021/2022 2021/2022 2021/2022

3-4-3-2-3. Dial-Back (the call back) Technique

In phone banking services, dial-up facilities are provided to the bank's customers so that they can access the bank's

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

information and carry out some transaction on their accounts through telephone lines. Therefore, it is extremely important to ensure that there are adequate security controls, implemented through using passwords and restricting dial-up capabilities to authorized individuals. Assurance should be made that whenever a dial-up access occurs, the system will dial back the authorized user rather than permitting immediate access to the bank's information.

The call back technique could be used to prevent unauthorized dial-up access to a mainframe computer system, and to a LAN. Call back could be manual, by operator, or automated through special call back modems. Whenever sensitive data is transmitted through the network, security can be enhanced by encrypting data before it is transmitted.

Authentication routines enable the recipient of data to ensure that a message is authentic by the inclusion of control and identification data within it (Roufail, 1990 and Jenkins et al., 1992, p. 241).

2021/2022 2021/2022 2021/2022

3-4-3-2-4. Security Packages

Jenkins et al. (1992) reported that sophisticated security packages have been developed to assist in providing adequate program and data file security. The software assists security by providing control over: the users who might access the system, the resources within the system that each user might access; and the access authorities, or how each user might access those resources. This is accomplished by defining rules within the software that determine each user's authority and restrictions over each resource (p. 242).

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Again, according to Jenkins et al. (1992), controlling access to a system is on its own insufficient to provide an adequate level of control. Therefore, the following additional considerations are also appropriate:

- **Individual Accountability:** The security system should be able to associate each job or transaction with the person or department initiating the job. Provision should be made for each user to have a unique identifier, which enables the tracing of all attempted and unauthorized accesses to a particular individual. However, it should be noted that a user might be assigned more than one identifier, each with different attributes.
- **Auditability:** Security packages usually produce regular reports on who accessed what data. Often, the package will have a report writing capability, which could be used to generate the information needed for an adequate audit trail. Special reports may also be available to assist in the maintenance of security systems (p. 243).

2021/2022 2021/2022 2021/2022

3-4-4. Data and Data Integrity Security Controls

Data file security controls are those controls designed to ensure that unauthorized changes cannot be made to data. The auditor might wish to place reliance on data file security controls to reduce the risk of misappropriation of assets or financial data by unauthorized access to data files. The need to place reliance on data file security controls has been increased due to the growing and sophistication of information.

30006101601571 30006101601571 30006101601571

Jenkins et al. (1992) mentioned that in real-time and on-line information, data is frequently stored in a database and made

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

available to many users through terminals. In such systems, traditional reconciliation procedures will often be carried out less frequently than would be necessary to provide timely identification of unauthorized changes, and management increasingly places reliance on data file security controls to protect the data. Buttross and Ackers (1990) argued that one of the primary weaknesses in most microcomputer systems is data security and integrity. Safeguards in these areas tend to be more time consuming than other areas and, accordingly, are often ignored (p. 32).

Organizations' data files and information should be classified according to their sensitivity and inherent value to the organization. The different levels of confidentiality and security of the organizations' data and information could be classified under one of the four categories as follows:

- Public use (unrestricted) data;
- Internal use only;
- Confidential; and
- Highly classified (or top secret) data.

2021/2022 2021/2022 2021/2022

Confidential information should not be publicly displayed on the screen. To control access to sensitive data, there should be a mapping of access requirements to the system components. Access rights should be based on job function and an appropriate segregation of duties should be existed. Temporary employees should be restricted to a specific project, activity, system, and time period (Qureshi and Siegel, 1997 and Boritz, 1999).

The importance of data controls should be clearly apparent when considering the effect that faulty, loss, damaged, destroyed, or leaked data could have on the organization's daily operations and competitive position in the market. One could imagine the

30006101601571 30006101601571 30006101601571

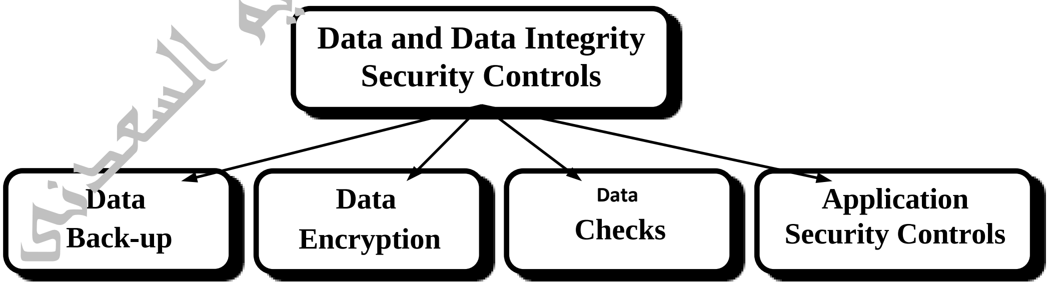
soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

loss that could occur if some important organization files were lost or destroyed, if some confidential and sensitive files of customers were altered in an unauthorized way, if some personal data of the organization's customers were illegally accessed and publicly disclosed, or some important managerial decisions were taken based on inaccurate data.

Huston and Huston (1998) suggested that data security problems could be minimized by restricting access to the system or to the data, as well as by monitoring. System access controls include restriction of physical access to the system and the use of user identifications and passwords. Data access controls include having a custodian for sensitive files, locking floppy disks in storage, encrypting data, and having read/write/execute permission identification for each user. Monitoring activities could be employed by the use of activity logs to record unauthorized attempts at system or data access.

The most important data and data integrity security controls are data backups, data encryption; data checks techniques and application security controls. We expand upon these data integrity security controls below.

2021/2022 2021/2022 2021/2022


Data and Data Integrity Security Controls
Data Back-up
Data Encryption
Data Checks
Application Security Controls

(Figure 3-6)
(Data and Data Integrity Security Controls)

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

3-4-4-1. Data Back-up

As organizations become more and more dependent on information for all aspects of their operations, not just for accounting, the importance of effective back-up and recovery procedures control cannot be overemphasized. The objective of back-up and recovery procedures is to resume processing as soon as possible after a disruption in information processing occurred, at minimum cost. This requires duplicate copies of data, software, documentation, critical supplies (such as special forms and documents) and equipment for subsequent use in the event that data, software, equipment or information processing facilities are lost due to human error, system malfunction or abuse, or disaster. Most back-up and recovery activity focuses on data and software. In some cases, particularly where processing equipment is unusual, or has a long lead-time for delivery, standby equipment might also be required. Similarly, special forms, documentation, or even specially trained personnel might also be kept on reserve or standby.

2021/2022 2021/2022 2021/2022

Dougan (1994) mentioned that, when deciding how to complete a back up schedule, the main issues that should be considered are what to back up and how often should back up occurs. The following general rules are suggested:

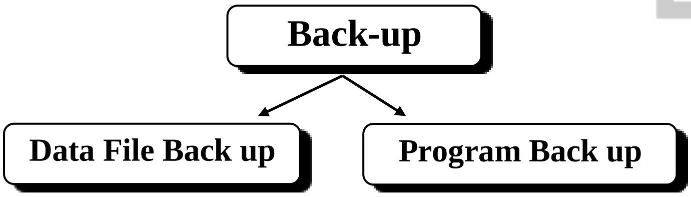
- All software programs should be backed up when purchased;
- All systems performing numerous transactions should be backed up frequently; and
- Whenever data files are significantly altered, a backup should be performed.

30006101601571 30006101601571 30006101601571

For security purposes, backup copies of data files and software should be made regularly. In this section, data file

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

backup, as an important element of security controls, will be highlighted, while program and software security controls were discussed in a previous section.



(Figure 3-7)
(Types of Back up)

Data file backup is one of the most important aspects of an ongoing information back-up and recovery system. Back-up copies of all master files should be maintained to permit reconstruction in the event that the current version is destroyed. The frequency of back-up must depend on the volume of transactions processed and their significance for an organization. Data backup should be implemented regularly in light of the increased number and significance of organization transactions.

2021/2022 2021/2022 2021/2022

Accordingly, an increased emphasis should be given to on-line disaster recovery planning, and real-time transaction-based backup. Not only is backup vital to ensure organizations' survival in the wake of catastrophic system failure, but it will also become a major marketing advantage in attracting customers. As more electronic products are introduced and as customers tie into organization databases, customers will depend on their organization's contingency plan for their survival .

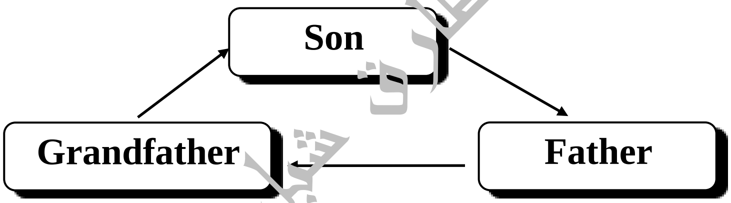
It is suggested that the minimum number of back-up copies should be two, which when added to the "in-use" copy makes for three copies. The "son-father-grandfather" concept is applied to

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

the backup cycle (figure 3-8). Periodically, say each week, the files should be Back-up

Data File Backup Program Back up rotated. The grandfather file, stored off-site, is rotated to become the operational file, after being updated for intervening changes and transactions, the father is rotated and moved off-site to become the grandfather, while the son, which was the old operational file, is rotated to become the on-site father file. Maintaining such a disciplined process might be an effective way of ensuring that critical data files are safeguarded. With the easy and reliable backup systems available today, most organizations would prefer to maintain information in electronic form and to make hard copy only when it is necessary.



2021/2022 2021/2022 2021/2022

(Figure 3-8)
(Back up Cycle)

Boritz (1999) suggested that electronic archiving is far superior to hard copy not only because access is easier and cheaper, but also because it is easier to store duplicates in alternate locations for security. Dougan (1994) argued that the most important prevention activity one can undertake is to back up data frequently. Technological advances have made back up much easier today and backup systems are far less costly. If a computer stores critical data, a tape backup or equivalent system is a must. Buttross and Ackers (1990) confirmed that off-site storage protects backups from accidental or intentional

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

destruction that might occur to the on-site components. Backups should be stored in a safe-deposit box. However, security control over sensitive data (such as payroll and customers' accounts) is another important consideration. Several steps that can be taken to block the unauthorized disclosure of such data include:

- Encryption;
- Working on sensitive data only in private offices;
- Placing sensitive data only on distinctly marked diskettes or removable hard disks;
- Removing diskette cartridges from unattended computers and storing them with a designated custodian;
- Turning off unattended microcomputers when data is removed from the system;
- Reformatting the disk or overwriting the file for destruction of sensitive data (the commands ERASE and DELETE typically do not destroy such data);
- Having microcomputer users with access to sensitive data sign binding confidentiality agreements; and
- Storing diskettes or cartridges in a secure cabinet or fire-rated safe, especially when continually updated off-site backups are not maintained.

2021/2022 2021/2022 2021/2022

Again, Buttross and Ackers (1990) argued that another area, that is often given too little attention by unsophisticated users, is the integrity of data and internally data generated programs. Control measures that enhance this integrity include validating the accuracy of customized software, dating changes to data bases, dating reports with the date of production and the date of the data base and independently validating data input. These steps should be required before decisions are made to use microcomputer results (p. 33).

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Huston and Huston (1998) argued that although backing up information is almost a foregone conclusion, the possibility of damaged or stolen backup copies is a sometimes neglected operational concern. The backup copy could be easier to steal than the main body of information because of being “out of sight, out of mind” from a protection standpoint. It is sometimes helpful to treat the backup copy as the main copy on alternate days to minimize this potential. Also, an information system is particularly prone to misuse or misappropriation during periods of transition. When a manual system is being converted to a computerized system, not only are the users careless with the new system during the learning process, but also the security system may not initially be fully operational.

3-4-4-2. Data Encryption

Encryption is the coding of text into unreadable string characters based on mathematical algorithms. It can be an effective method of preventing browsing of confidential data, since a decoding key is needed to be able to read the original message. This method might be employed when storing sensitive data or programs and when transmitting data to or receiving data from external sources. Encryption (secret coding) could be the best method of protecting data from tapping: hardware devices are used to scramble data during its transmission to and from computer terminals.

Encryption is generally used to protect data during its transmission within a LAN and from remote computers. Two types of encryption systems are available: the secret key system (which requires both parties to have the same decoding key); and the public key system (where the message is encrypted with a

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

public key and the receiver decodes the same message with a private key) (Roufail, 1990 and Henry, 1997). Boritz (1999) confirmed that encryption is an effective way of protecting data files from such exposures. While it might be an effective safeguard, encryption does have its drawbacks: storing encrypted data requires additional space and more processing time.

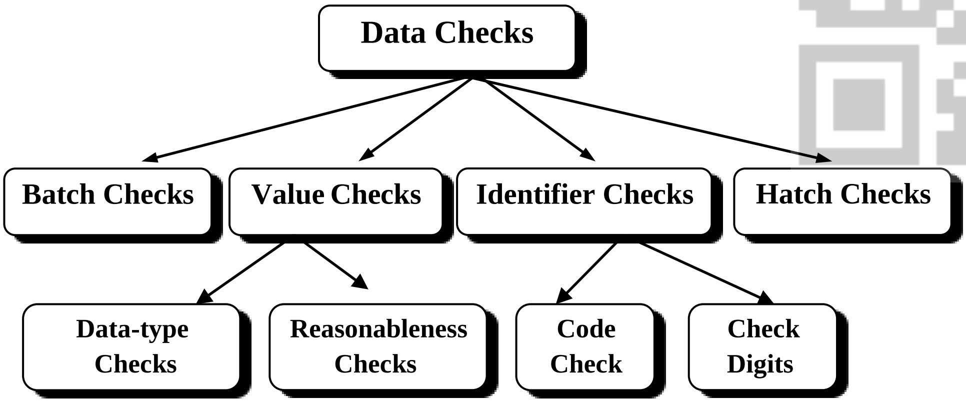
3-4-4-3. Data Checks

Financial institutions cannot survive without reliable data, therefore, audit procedures must be established to ensure the accuracy and integrity of data. In addition to strong physical and logical access security, input and processing controls which consist of value, range, consistency and reasonableness checks will improve data quality as well as processing efficiency. Program and system software control mechanisms are needed to protect the integrity of the applications, ensure valid data is entered to the system and notify the user and appropriate personnel when erroneous data has been submitted to the system. Finally, to ensure data integrity on all systems, duties should be segregated. Again, FFIEC argued that data edit procedures can significantly reduce manual entry errors during input. In addition, edits can be built into programs and applications to ensure that data being processed are valid. System software can provide a high degree of input and processing error controls (FFIEC, 1996, Ch. 14).

Various techniques could be used to check the accuracy and integrity data such as identifier checks (code checks and digit checks); value checks (data type checks and reasonableness checks); batch totals and hash totals checks. These security techniques will be briefly highlighted in the following sections.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg



(Figure 3-9)
(Data Check Components)

3-4-4-3-1. Identifier Checks

Data filters for account identifiers (such as general ledger accounts, customer accounts and inventory part numbers) are code checks and check digits. A code check compares the input of an account ID with a stored list of identifiers and rejects invalid identifiers. Usually, the ID lookup retrieves the account description and places it on the input screen next to the identifier, thereby providing visual confirmation of the account selected. Note that the code check does not assure that the input ID is correct; it assures only that a valid ID has been entered. The entry of a wrong but valid ID will be accepted. Thus, the accuracy of code checks depends heavily on a visual check (Boritz, 1999).

The check-digit system requires adding one digit to existing account identifiers. That digit is calculated from the numbers in the original identifier. Boritz (1999) mentioned that use of a common algorithm for a check digit eliminates about 95 percent of keying data errors.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Thus, if there are 5,000 entries, with an error rate of 2 percent (100 errors), only 5 errors will not be detected by such a check-digit system. Since check digits do not require any system lookups, but require only that the computer calculate the check digit, required computer resources are minimized. On the other hand, if 5,000 account identifiers must be recorded, adding a seventh (check) digit will require 5,000 additional keystrokes.

Boritz (1999) argued that code checks need screen confirmation of data entry and thus more processing time than do check digits; while check digits require additional keying time. The presence of check digits in our checking account numbers, credit card numbers and most product bar codes attests to their utility in large data processing environments.

Check digits (often associated with "head-down" data entry) use an audible sound to alert data entry personnel to errors. Code checks would seem to be preferred in low-transaction-volume environments, with the assumption that data entry personnel will "double-check" their work by reading the screen.

2021/2022 2021/2022 2021/2022

3-4-4-3-2. Value Checks

Checks to validate quantitative values (currency or physical) include two types of checks: data type checks and reasonableness checks. A data-type check ensures that all data entered are composed of a specified character set such as numbers. Such a system could ensure that entry of transaction values sales discount rates and wage rates are composed only of numbers and perhaps a decimal point. According to Boritz' survey (1999) almost all accounting software packages support such data-type checks. A reasonableness check is a useful control for some quantitative fields such as unit price and transaction

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

amounts. The simplest reasonableness limit for quantitative values entered is a minimum of zero for many fields, thereby precluding the entry of negative numbers.

For wage rates one might use both a minimum and a maximum. Great Plains Dynamics, Progression, SBT Pro, Solomon and Visual Accounting all support reasonableness limits (Boritz, 1999).

3-4-4-3-3. Batch Totals and Hash Totals Check

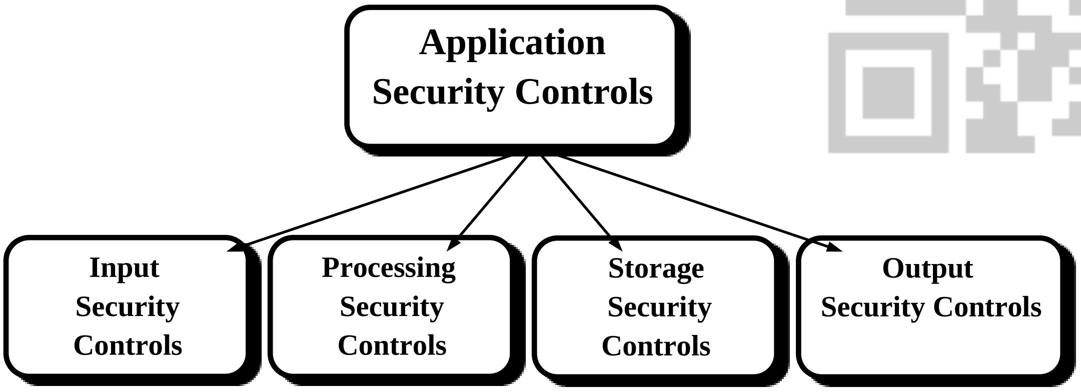
The quality of both account identifiers and value checks could be further enhanced by use of batch controls, batch totals and hash totals. Before data entry, the user can batch data that has been captured off-line and total both the account identifiers and the associated values. Identifier sums are known as hash totals and value totals are called batch totals. If the accounting software accumulates similar totals as data entry occurs or permits batch printouts with such totals, the processed data totals could be compared with the previously obtained totals. However, in evaluating the available accounting software, Boritz (1999) found that all accounting software packages (except Traverse) supported batch totals, but that none of them supported hash totals.

3-4-4-4. Application Security Controls

Application controls are built into accounting software to deter crime and minimize errors. Application controls typically include input controls, processing controls, change controls, testing controls, output controls and procedural controls (Qureshi and Siegel, 1997).

سليمان طارق شبل ابراهيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg


Application Security Controls
Input Security Controls
Processing Security Controls
Storage Security Controls
Output Security Controls

(Application Security Controls)
(Figure 3-10)

3-4-4-4-1. Input Security Controls

The purpose of input security controls is to ensure that each transaction is authorized, processed correctly and processed only once.

- An edit program verifies input by comparing fields to anticipated values and by testing
- logical relationships.
- A missing data check assures that all data fields have been used.
- A valid character check verifies that only alphabetical, numeric or other special characters are present in data fields.
- Dual read duplicates entry or key verification and verifies the accuracy of a critical field in a record by requiring that a data item be entered twice.
- A valid code check compares a classification (such as an asset account number) or transaction code (such as a credit sale entry) to a master list of accounts (master file reference) or transaction codes (Qureshi and Siegel, 1997).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شلبي ابراهيم السعدي

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

In summary, input security controls include rejecting, correcting and resubmitting data that were initially wrong or perhaps not properly authorized. Character validation tests may also be programmed to check input data fields for alpha numeric when they are supposed to have numeric.

A pre-processing edit check verifies a key entry by a second one or a visual review. There might be a limit test check of input data fields to make sure that some predetermined limit has not been exceeded (for example, employees' weekly hours should not be automatically processed if the sum of regular and overtime hours per individual exceeds 60 hours).

3-4-4-4-2. Processing Security Controls

Processing controls are used to ensure that transactions entered into the system are valid and accurate, that external data are not lost or altered, and that invalid transactions are reprocessed correctly.

2021/2022 2021/2022 2021/2022

3-4-4-4-3. Storage Security Controls

Storage security controls safeguard the integrity of information by establishing standard procedures for making modifications. For example, a log file can be maintained to document all changes. A report may be prepared showing the master file before and after each update (Qureshi and Siegel, 1997).

Boritz (1999) argued that security controls over changes to data files and accounts are vital for information. Password and input controls may be effective for transactions entered, but they do not protect non-transaction data stored in ledger master files. An effective control provides a chronological log of changes for

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

each master file. These include general ledger, receivables, payables, inventory, payroll and any other modules for which master files exist. Master file changes such as budget revisions, customer address changes and inventory supplier authorizations should be recorded in chronological logs (one for each master file) that show the changes, when they were made and who made them.

3-4-4-4-4. Output Security Controls

According to Qureshi and Siegel (1997) the purpose of output controls is to authenticate the previous controls; this is used to ensure that only authorized transactions are processed correctly. Random comparisons can be made of output to input to verify correct processing. For example, an echo check transmits data received by an output device back to its source. Output might be compared to source documents. Output controls assume data are not lost or improperly distributed. Errors by recipients of output such as customers should be investigated. Output security controls will be discussed in details in section 3-4-10.

2021/2022 2021/2022 2021/2022

3-4-5. Off-line Programs and Data Security Controls

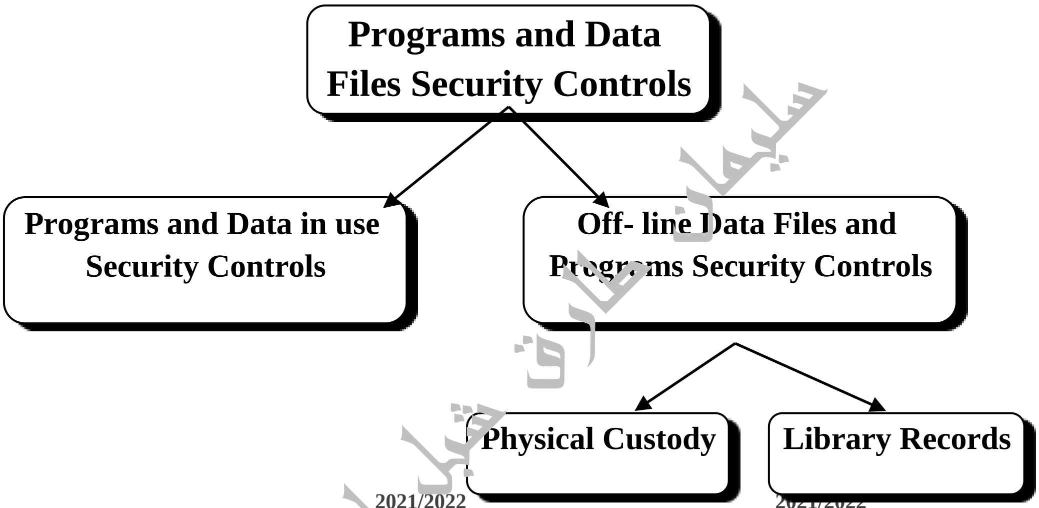
Security controls could be implemented over both in-use and off-line accounting data and programs (Figure 3-11). Programs in-use are defined as those programs which could be accessed through the system, either by operators processing jobs or through terminals. On the other hand, off–line programs are those held away from the computer when not be used, normally in a physical library.

30006101601571 30006101601571 30006101601571

According to Jenkins et al. (1992) data in use includes all data which could be accessed through the system, either by

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

operators processing jobs or through terminals. Data in use thus includes both data permanently loaded on disc storage and available for enquiry or updating as in real-time and on-line systems and tapes or discs which have been loaded for a specific processing run but are otherwise stored off-line in batch systems. On the other hand, off-line data files are those data held in a physical library.


Programs and Data Files Security Controls
Programs and Data in use Security Controls
Off- line Data Files and Programs Security Controls
Physical Custody
Library Records

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدني

(Figure 3-11)
(Programs and Data File Security Controls)

A key aspect of a sound back-up and recovery process is off-site storage. This involves keeping an extra copy of software, data and critical documentation at another location.

Jenkins et al. (1992) recommended that, where programs and data are held off-line, they should be subject to physical library controls whereby they are securely held, only issued on appropriate authority and promptly returned. With the growth in real-time and on-line systems, much of the storage of programs off-line will comprise backup copies. Both backups and program

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

documentation should be protected to avoid unauthorized personnel obtaining detailed knowledge of the contents of the programs. Backup copies of programs should be securely held in a library, or outside the installation areas, and should only be issued to the operations staff on the authority of a responsible official.

Boritz (1999) argued that many organizations fall into the trap of believing that once appropriate arrangements have been made for back up, they are protected. Many enterprises have discovered to their dismay that the arrangements fell through when they were most needed, or were not functional. One firm decided to check its off-site storage facility. It found that there was a storage room, which was locked, and inside it there was a weld mesh wire cage with a strong lock on the outside. Stored inside the secure cage sat a supply of soap and toilet paper. Stored in racks outside the cage were the company's back-up tapes. The man in charge explained that, "The toilet rolls are expensive and the cleaner keeps nicking them".

2021/2022 2021/2022 2021/2022

The two main elements of the off-line programs and data security controls are physical custody and maintaining library records. These controls will be mentioned in the following sections.

3-4-5-1. Physical Custody

In order that off-line programs and data may be secured from unauthorized access, they should be kept in a lockable area, separate from the computer room, preferably supervised by a full-time librarian responsible for the issue, receipt and security of all programs and data. Where the installation is not large enough to warrant a full-time librarian, a member of the control

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

staff should have similar duties. Access to the library should be restricted to staff authorized to obtain and deliver programs and data. Off-site storage will need to be similarly secure (Jenkins et al., 1992, p. 247).

FFICE (1996) recommended that any tape/disk and file library should be protected from physical disaster in the same manner as the computer room. Furthermore, the library should be controlled throughout all operating shifts to prevent unauthorized access to data file media. During the shifts in which the librarian is not present, alternative procedures might be implemented. All media within the library, such as magnetic tapes, disk packs and cards should be stored in a closed, dust-free, fire resistant area. Removal of these files from the library should be permitted only when needed for processing. In addition, all critical data and software on the various media should be backed up and stored off-site (ibid. Ch. 14).

All data media in the library should be externally labeled to identify their contents and to avoid their misuse. Jenkins et al. (1992) argued that wherever batch processing is carried out, there should be procedures to ensure that files are only issued for authorized processing. This means that processing schedules should be prepared to give details of the required files for processing. Schedules should be prepared for all applications and approved by a responsible official. A librarian should be instructed only to issue the appropriate files on production of an authorized processing schedule. The authority of a responsible official should be necessary for the issue of any file unsupported by a processing schedule, including transfer to off-site storage (ibid. p. 248).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Moreover, files issued for processing should not be removed from the organization's operations area. Physical control of these issued data files and programs should be the responsibility of the operation manager or chief operator. Further protection might be afforded by following up files recorded as being in issue for an unreasonable length of time.

3-4-5-2. Library Records

Each removable storage device should be allocated a unique identity number (the external label), which should be permanently recorded on the device. A record of devices should be maintained as a means of accounting for and controlling both programs and data files issued from the library and those created during processing. The record of devices and files could be maintained either electronically or manually.

3-4-6. Utility Programs Security Controls

FFIEC (1996) argued that system utility programs are valuable tools when used during program debugging, file maintenance, cataloguing, or even in daily operations of the overall computer environment. Certain programs could be used to alter storage data files and object codes, enter the supervisor state and catalogue, or to purge and rename programs. System utilities also have capabilities to alter and delete programs or data. Most computer manufactures supply these programs as part of their operating system.

According to Jenkins et al. (1992) utility programs normally leave no trace of their use in the files or programs that are amended. They must therefore be particularly tightly

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

processing failure or at any other time, does not have adverse effects on production data or programs.

These controls normally combine preventive controls, such as password restrictions on the use of utility programs or the holding of the programs off-line with specific authorization for usage, with detective controls, such as the reporting, investigation and retrospective authorization of all usage (p. 248).

According to FFIEC (1996) unauthorized use of system utility programs could be controlled in several ways. These controls, however, would not be effective if they unnecessarily impeded operations. System utilities can be controlled by:

- Installing a password system on all program libraries / directories, including the system
- utility library / directory. If password protection is used, measures must be taken to
- control access to the passwords. Passwords should be changed periodically.
- Using automated library systems. Several automated library systems that provide

program security are available from equipment manufacturers and software vendors. Such programs restrict access to the program library / directory. They can produce daily reports identifying each program that was accessed and any program changes that was made.

3-4-7. Bypassing of Normal Access Security Controls

Occasionally it might be necessary to bypass the normal security and access controls over programs and data. Examples of where this might occur are in emergency situations (such as

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل عبد الحميد السعدنى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

processing failure where data might need to be amended to correct transaction errors), or where access is given through dial-up to an external software vendor to enable him to maintain programs. In such cases there will need to be controls to ensure that such actions are authorized, that security is subsequently reinstated and unauthorized actions are prevented, or reported and investigated (Jenkins et al., 1992, p. 250; FFIEC, 1996, Ch. 14).

3-4-8. User Programming Security Controls

Recent developments in computerized systems have permitted users to use utilities or high level programming languages which give them the ability to change the data, and to write programs to generate certain reports. Such facilities enable users to access data and to create reports that satisfy their own needs. In these cases, security controls should be implemented to prevent unauthorized use of such a facility, to report and investigate unauthorized use or even attempts to use it.

2021/2022 2021/2022 2021/2022

3-4-9. Division of Duties

The effectiveness of internal controls would be influenced by whether there is adequate division of duties in the performance of accounting procedures and related internal controls. Such division of duties will consist of arrangements that reduce the risk of error and that limit the activities of individuals, to ensure that the opportunity to misappropriate assets or conceal other misrepresentations in financial statements is restricted. In general, the division of duties required is that:

30006101601571 30006101601571 30006101601571

- Those persons carrying out or checking controls should be independent of computer operations;

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Controls over standing data should be carried out or checked by individuals other than those who deal with the related transaction data;
- Separate persons should perform or check the controls relating to input and updating and those carried out on the control account;
- The reconciliation of control accounts with the subsidiary records should be performed or checked by persons other than those maintaining the control account (Jenkins et al., 1992, p. 198 and FFIEC, 1996, Ch. 14).

FFIEC (1996) mentioned that segregation of duties is critical to the accuracy and integrity of data on all types of computerized systems (mainframe, minicomputer, LAN, and PC).

Security controls measures must include the separation of duties for all computer operations. The separation of duties is used to prevent the perpetration of fraud by an individual. If duties are adequately separated, fraud can only be committed through collusion. It is also a detective safeguard, in that the more people who are involved in processing, the greater is the probability that fraud will be detected.

Qureshi and Siegel (1997) confirmed that one of the main foundations of accounting systems security is the segregation of duties. There should be segregation of duties among personnel: for example, a person should not be both programmer and operator. There should also be rotation of assignments: for example, operators work different shifts, programmers work on different applications. An activity might require more than one operator, to make it more difficult for a person to commit an

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

improper act because others are involved. Segregation should exist between developing and testing software.

Jenkins et al. (1992) suggested that an adequate division of duties within the computer installation should be implemented so that the activities of staff within each major function such as operations are restricted to that function. Having sufficient technical skills and detailed knowledge of their contents, operators could make changes to production programs. Protection against this possibility is normally provided by suitable segregation of duties, whereby the operators cannot obtain a detailed knowledge of programs.

Similarly, those responsible for the development of and maintenance of programs should not be able to gain access to the production version of a program or to the computer operation area. Where a separate program library group exists with the responsibility for cataloguing programs and maintaining program libraries, the staff in this group should not be able to access program documentation and development libraries or to access the computer operation area (p. 250).

2021/2022 2021/2022 2021/2022

3-4-10. Output Security Controls

Securing computer output against theft, unauthorized access, visibility, unauthorized printing and distribution are very important security control issues. Visual access to sensitive information, whether displayed on a terminal monitor or on a report printout, should be controlled; sensitive data should not be printed outside the data centre or central computer room and it should be printed only under precise security controls.

FFIEC (1996) stated that sensitive reports should never be left unattended by a copy or facsimile machine and on an

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

individual's disk. Classified information must be secured in a locked disk cabinet to prevent the possibility of theft, unauthorized disclosure, or modification. Procedures must be made developed for disposal of confidential data, for example, shredding machines could be made available to destroy unneeded hard copy reports. A degauser (magnet) could be used to eliminate or destroy hard and floppy disks and tapes that contain confidential information (Ch. 14).

Moreover, all computer printouts should include date/time stamps on the hard copies. The date/time stamp indicates when printing occurred and may thus suggest what data are included and who is responsible for it by reference to the user ID or terminal ID on it. Date/time stamps are economical and useful output security controls.

The following points might be useful to protect the organization's data / information output from prospective security threats:

- Input to output reconciliation should be implemented;
- Control over the distribution of output should be considered;
- Control over error and exception reports should exist;
- Appropriate security control should be implemented to protect printed data / information from theft;
- Copying of output should be restricted to authorized people;
- Security controls should be implemented over document visibility by display on monitors or as printed on paper;
- Printing and distribution of information should be done only by authorized persons;
- Prints and distributed information should be directed only to people who are entitled to receive them;

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Sensitive documents should not be handed to non-security cleared personnel for shredding.

3-4-11. Periodic Audit

Periodic audit is one of the important methods of securing an organization's information. Whether the audit is performed by external auditors or internal auditors, a regular review of internal controls and security methods should be conducted with an eye toward improving the existing system. The focus of audit and security will be on preventing internal and external fraud. Roufail (1990) suggested that computer auditing has become a high-risk environment and requires experienced personnel, extensive supervision and persuasive evidence. Above all, the auditing approach requires a heightened degree of professional skepticism in this critical audit area.

Internal audit and security should be concerned with making sure cost-effective control systems are in place and that management information systems identify problems early enough so they might be fixed before damaging organization earnings. Audit and security managers need to ask these questions: what are the organization's exposures? are systems in place to protect the bank from losses? and, are systems in place to provide correct financial data even as transactions are taking place? (Bank Management, 1990).

Therefore accounting software should be able to provide an audit trail in which a transaction could be traced from its origin to the financial statements and vice-versa. Moreover, the software should permit users to trace from the beginning balance of each account to the ending balance and vice-versa.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبايك ابراهيم السعيدي

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

According to Qureshi and Siegel (1997) the audit trail analyses transactions related to the physical custody of assets and evaluate unusual transactions. It also keeps track of the sequential numbering of negotiable computer forms. Controls should be periodically tested: for example, the audit trail requires the tracing of transactions to control totals and from the control total to supporting transactions.

Audit and information security responsibilities should also include assuring that these packages comply with regulations and meet performance and security standards. They must evaluate the controls over software packages, review bank-vendor contract, and monitor compliance with significant contract requirements (bank management, 1990).

3-5. Summary

In this chapter a general overview of the classification of information security controls has been presented and the main objectives of information security controls have been discussed. The main security controls of information have been classified under eleven security control groups. These main security control groups are: organizational security controls; hardware and physical access security controls; software and electronic access security controls; data and data integrity security controls; off-line programs and data security controls; utilities security controls; bypassing of normal access security controls; user programming security controls; division of duties; output security controls and periodic security controls. In the next chapter, alternative approaches for evaluating the security of information will be presented.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعيدي
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Questions of Chapter Three

Please select the correct answer of each of the following questions:

1. A control procedure designed so that the employee that records cash received from customers does not also have access to the cash itself is an example of a(n)
   a. preventive control.
   b. detective control.
   c. corrective control.
   d. authorization control.

2. Form design is one example of a(n)
   a. output control.
   b. processing control.
   c. input control.
   d. data entry control.

2021/2022 2021/2022 2021/2022

3. Turnaround documents are an example of a(n)
   a. data entry control.
   b. output control.
   c. processing control.
   d. input control.

4. Error logs and review are an example of
   a. data entry controls.
   b. data transmission controls.
   c. output controls.
   d. processing controls.

سليمان طارق شبل ابراهيم السعيدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

5. Which of the following data entry controls would *not* be useful if you are recording the checkout of library books by members?
   a. sequence check
   b. prompting
   c. validity check
   d. concurrent update control

6. A payroll clerk accidently entered an employee's hours worked for the week as 380 instead of 38. The data entry control that would best prevent this error would be
   a. a limit check.
   b. a check digit.
   c. batch total reconciliation.
   d. a field check.

7. The data entry control that would *best* prevent entering an invoice received from a vendor who is not on an authorized supplier list is
   a. a validity check.
   b. an authorization check.
   c. a check digit.
   d. closed-loop verification.

8. Sequentially prenumbered forms are an example of a(n)
   a. data entry control.
   b. data transmission control.
   c. processing control.
   d. input control.

سليمان طارق سليمان ابراهيم السعيدي
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

9. ________ is/are an example of a detective control.
    a. Physical access controls
    b. Encryption
    c. Emergency response teams
    d. Log analysis

10. Which of the following is an example of a corrective control?
    a. physical access controls
    b. encryption
    c. intrusion detection
    d. incident response teams

11. Which of the following is *not* a requirement of effective passwords?
    a. Passwords should be changed at regular intervals.
    b. Passwords should be no more than 8 characters in length.
    c. Passwords should contain a mixture of upper and lowercase letters, numbers and characters.
    d. Passwords should not be words found in dictionaries.

2021/2022 2021/2022 2021/2022

12. Multi-factor authentication
    a. involves the use of two or more basic authentication methods.
    b. is a table specifying which portions of the systems users are permitted to access.
    c provides weaker authentication than the use of effective passwords.
    d. requires the use of more than one effective password.

سليمان طارق عبد ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

13. If the time an attacker takes to break through the organization's preventive controls is greater than the sum of the time required to detect the attack and the time required to respond to the attack, then security is
    a. effective.
    b. ineffective.
    c. overdone.
    d. undermanaged.

14. Which of the following preventive controls are necessary to provide adequate security for social engineering threats?
    a. controlling remote access
    b. encryption
    c. host and application hardening
    d. awareness training

15. Identify the best description of an access control matrix below.
    a. does not have to be updated
    b. is used to implement authentication controls
    c. matches the user's authentication credentials to his authorization
    d. is a table specifying which portions of the system users are permitted to access

16. A validity check is an example of
    a. a data entry control.
    b. an output control.
    c. a data transmission control.
    d. an input control.

سليمان طارق عبد الرحيم السعدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

17. Parity checks are an example of a(n)
    a. data entry control.
    b. data transmission control.
    c. output control.
    d. processing control.

18. A *user review* an example of
    a. a data entry control.
    b. a data transmission control.
    c. an output control.
    d. a processing control.

19. Data matching is an example of a(n)
    a. data entry control.
    b. data transmission control.
    c. processing control.
    d. input control.

2021/2022 2021/2022 2021/2022

20. The ________ disseminates information about fraud, errors, breaches and other improper system uses and their consequences.
    a. chief information officer
    b. chief operations officer
    c. chief security officer
    d. computer emergency response team

21. The most important element of any preventive control is
    a. the people.
    b. the performance.
    c. the procedure(s).
    d. the penalty.

سليمان طارق شبل ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

22. In 2007, a major U.S. financial institution hired a security firm to attempt to compromise its computer network. A week later, the firm reported that it had successfully entered the system without apparent detection and presented an analysis of the vulnerabilities that had been found. This is an example of a
    a. preventive control.
    b. detective control.
    c. corrective control.
    d. standard control.

23. Noseybook is a social networking site that boasts over a million registered users and a quarterly membership growth rate in the double digits. As a consequence, the size of the information technology department has been growing very rapidly, with many new hires. Each employee is provided with a name badge with a photo and embedded computer chip that is used to gain entry to the facility. This is an example of a(n)
    a. authentication control.
    b. biometric device.
    c. remote access control.
    d. authorization control.

24. A *batch total* is an example of which control below?
    a. data entry control
    b. data transmission control
    c. processing control
    d. output control

2021/2022 2021/2022 2021/2022

سليمان طارق شعلان ابراهيم السعيدي

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

25. When new employees are hired by Pacific Technologies, they are assigned user names and appropriate permissions are entered into the information system's access control matrix. This is an example of a(n)
    a. authentication control.
    b. biometric device.
    c. remote access control.
    d. authorization control.

26. When new employees are hired by Pacific Technologies, they are assigned user names and passwords and provided with laptop computers that have an integrated fingerprint reader. In order to log in, the user's fingerprint must be recognized by the reader. This is an example of a(n)
    a. authorization control.
    b. biometric device.
    c. remote access control.
    d. defense in depth.

2021/2022 2021/2022 2021/2022

27. All employees of E.C. Hoxy are required to pass through a gate and present their photo identification cards to the guard before they are admitted. Entry to secure areas, such as the Information Technology Department offices, requires further procedures. This is an example of a(n)
    a. authentication control.
    b. authorization control.
    c. physical access control.
    d. hardening procedure.

سليمان طارق شبل ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

28. Cancellation and storage of documents means
    a. documents are defaced and stored.
    b. documents are defaced before being shredded.
    c. cancellation data are copied from documents before they are stored.
    d. data are copied from a document and stored, after which the document is shredded.

29. Check digit verification is an example of a(n)
    a. data transmission control.
    b. output control.
    c. processing control.
    d. input control.

30. A ________ ensures input data will fit into the assigned field.
    a. limit check
    b. size check
    c. range check
    d. validity check

2021/2022 2021/2022 2021/2022

31. This tests a numerical amount to ensure that it does not exceed a predetermined value nor fall below another predetermined value.
    a. completeness check
    b. field check
    c. limit check
    d. range check

سليمان طارق شبل ابراهيم السعدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

32. This determines if all required data items have been entered.
    a. completeness check
    b. field check
    c. limit check
    d. range check

33. This determines the correctness of the logical relationship between two data items.
    a. range check
    b. reasonableness test
    c. sign check
    d. size check

34. This determines if characters are of the proper type.
    a. field check
    b. alpha-numeric check
    c. range check
    d. reasonableness test

2021/2022 2021/2022 2021/2022

35. A computer operator accidentally used the wrong master file when updating a transaction file. As a result, the master file data is now unreadable. Which control could *best* have prevented this from happening?
    a. Internal header label
    b. validity check
    c. check digit
    d. parity check

سليمان طارق شبل ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

36. This tests a numerical amount to ensure that it does not exceed a predetermined value.
    a. completeness check
    b. limit check
    c. range check
    d. sign check

37. This batch processing data entry control sums a field that contains dollar values.
    a. record count
    b. financial total
    c. hash total
    d. sequence check

38. This batch processing data entry control sums a non-financial numeric field.
    a. record count
    b. financial total
    c. hash total
    d. sequence check

39. When I enter a correct customer number, the data entry screen displays the customer name and address. This is an example of
    a. prompting.
    b. preformatting.
    c. closed-loop verification.
    d. error checking.

سليمان طارق شبل ابراهيم السعدى

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

40. This control ensures that the correct and most current files are being updated.
    a. cross-footing balance test
    b. data matching
    c. file labels
    d. write-protect mechanism

41. This batch processing data entry control sums the number of items in a batch.
    a. financial total
    b. hash total
    c. record count
    d. sequence check

42. This data entry control compares the ID number in transaction data to a master file to verify that the ID number exists.
    a. reasonableness test
    b. user review
    c. data matching
    d. validity check

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدى

43. What control are *file labels* an example of?
    a. data entry controls
    b. output controls
    c. processing controls
    d. source data controls

44. Sonja Greer called the IT Help Desk in a bad mood. "I'm trying to open an Excel file, but I get a message that says that the file is locked for editing. Why is this happening to me?"

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

The answer is likely that

a. the file is corrupted due to a computer virus.
b. Sonja probably opened the file as read-only.
c. concurrent update controls have locked the file.
d. there is no problem. Sonja is editing the file, so it is locked.

45. This control protects records from errors that occur when two or more users attempt to update the same record simultaneously.

a. concurrent update controls
b. cross-footing balance test
c. data conversion controls
d. recalculation of batch totals

46. Modest Expectations Investment Services (MEIS) allows customers to manage their investments over the Internet. If customers attempt to sell more shares of a stock than they have in their account, an error message is displayed. This is an example of a

a. reasonableness test.
b. field check.
c. validity check.
d. limit check.

47. *Prompting* is a control that helps ensure

a. transaction data are not lost.
b. transactions data are accurate.
c. transactions data are complete.
d. transaction data are valid.

سليمان طارق شبل عبد الحليم السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

48. Modest Expectations Investment Services (MEIS) allows customers to manage their investments over the Internet. If customers attempt to spend more money than they have in their account, an error message is displayed. This is an example of a
    a. reasonableness test.
    b. field check.
    c. validity check.
    d. limit check.

49. The Spontaneous Combustion Rocket Shoppe in downtown Fargo, North Dakota, generates three quarters of its revenue from orders taken over the Internet. The revenue clearing account is debited by the total of cash and credit receipts and credited by the total of storefront and Internet sales. This is an example of a
    a. data integrity test.
    b. zero-balance test.
    c. trial balance audit.
    d. cross-footing balance test.

2021/2022 2021/2022 2021/2022

50. Which of the following is *not* a risk associated with the data input process?
    a. Data is invalid.
    b. Data is incomplete.
    c. Data is inaccurate.
    d. Data is corrupted.

سليمان طارق شبل ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

51. Which of the following is an example of a *turnaround document*?
   a. a receipt a customer must use to return the goods purchased
   b. a telephone bill the customer must return with payment
   c. a paycheck stub that must be used in the employee's tax return
   d. a customer loyalty card used every time a customer purchases goods or services

52. Which of the following is a control is an important way to prevent buffer overflow vulnerabilities?
   a. limit check
   b. size check
   c. range check
   d. field check

53. ________ copies all changes made since the last full backup.
   a. Archive
   b. Cloud computing
   c. Differential backup
   d. Incremental backup

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعيدى

54. Which of the following is *not* an objective of a disaster recovery plan?
   a. Minimize the extent of the disruption, damage or loss.
   b. Permanently establish an alternative means of processing information.
   c. Resume normal operations as soon as possible.
   d. Train employees for emergency operations.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

55. A disaster recovery plan typically does not include
    a. scheduled electronic vaulting of files.
    b. backup computer and telecommunication facilities.
    c. a system upgrade due to operating system software changes.
    d. uninterruptible power systems installed for key system components.

56. A facility that contains all the computing equipment the organization needs to perform its essential business activities is known as a
    a. cold site.
    b. hot site.
    c. remote site.
    d. subsidiary location.

57. A facility that is pre-wired for necessary telecommunications and computer equipment, but doesn't have equipment installed, is known as a
    a. cold site.
    b. hot site.
    c. remote site.
    d. subsidiary location.

58. When a computer system's files are automatically duplicated on a second data storage system as they are changed, the process is referred to as
    a. real-time mirroring.
    b. batch updating.
    c. consistency control.
    d. double-secure storage.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

59. ________ enables a system to continue functioning in the event that a particular component fails.
    a. An incremental backup procedure
    b. Fault tolerance
    c. Preventive maintenance
    d. A concurrent update control

60. A copy of a database, master file, or software that will be retained indefinitely as a historical record is known as a(n)
    a. archive.
    b. cloud computing.
    c. differential backup.
    d. incremental backup.

61. While this type of backup process takes longer than the alternative, restoration is easier and faster.
    a. archive
    b. cloud computing
    c. differential backup
    d. incremental backup

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدى

62. ________ involves copying only the data items that have changed since the last partial backup.
    a. Archive
    b. Cloud computing
    c. Differential backup
    d. Incremental backup

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

63. The maximum amount of time between backups is determined by a company's
    a. recovery time objective.
    b. recovery point objective.
    c. recovery objective.
    d. maximum time recovery objective.

64. The accounting department at Synergy Hydroelectric records an average of 12,500 transactions per hour. By cost-benefit analysis, managers have concluded that the maximum acceptable loss of data in the event of a system failure is 25,000 transactions. If the firm's recovery time objective is 120 minutes, then the worst case recovery time objective is
    a. 1 hour.
    b. 2 hours.
    c. 3 hours.
    d. 4 hours.

2021/2022 2021/2022 2021/2022

65. The accounting department at Aglaya Telecom records an average of 5,000 transactions per hour. A cost-benefit analysis leads management to conclude that the maximum acceptable amount of data loss is 20,000 transactions. If the firm's recovery time objective is 60 minutes, then the worst case recovery time objective is
    a. 1 hour.
    b. 2 hours.
    c. 3 hours.
    d. 4 hours.

سليمان طارق شبل ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

66. The accounting department at Aglaya Telecom records an average of 5,000 transactions per hour. By cost-benefit analysis, managers have concluded that the maximum acceptable loss of data in the event of a system failure is 50,000 transactions. The firm's recovery point objective is therefore
   a. 50,000 transactions.
   b. 5,000 transactions.
   c. 10 hours.
   d. 4 hours.

67. The accounting department at Aglaya Telecom records an average of 2,500 transactions per hour. Managers state that the maximum acceptable loss of data in the event of a system failure is 2,500 transactions. The firm's recovery point objective is therefore
   a. 2,500 transactions.
   b. 5,000 transactions.
   c. 1 hour.
   d. 2 hours.

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعيدى

68. Probably the *most* important change management control is
   a. monitoring user rights and privileges during the change process.
   b. testing all changes thoroughly prior to implementation on a stand-alone computer.
   c. updating all documentation to reflect changes made to the system.
   d. management's careful monitoring and review.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

69. Identify the statement below which is *true*.
    a. Cloud computing is a control technique for system availability.
    b. Cloud computing eliminates the need for backup of applications and data.
    c. Cloud computing eliminates the need for companies to own their own software and servers.
    d. Cloud computing refers to the practice of storing application files and backup data on satellites "in the clouds."

70. What is the primary objective of ensuring systems and information are available for use whenever needed?
    a. to minimize system downtime
    b. to minimize system expense
    c. to maximize system processing speed
    d. to maximize sales

2021/2022 2021/2022 2021/2022

71. Which of the following is *not* a common design feature of housing mission-critical servers and databases?
    a. adequate air conditioning systems to reduce the likelihood of damage due to overheating
    b. overhead sprinklers to provide protection from fire
    c. cables with special plugs that cannot be easily removed
    d. surge-protection devices to provide protection against temporary power fluctuations

سليمان طارق شبل ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

72. Which of the following is a key control regarding the minimization of system downtime?
    a. fault tolerance
    b. disaster recovery plans
    c. backup procedures
    d. all of the above

73. Whose responsibility is it to determine the amount of time an organization can afford to be without its information system?
    a. the board of directors
    b. senior management
    c. external auditors
    d. COBIT

74. Is it best practice for an organization to practice periodically restoring a system from its backup files?
    a. No, doing so might introduce errors into the system's data.
    b. No, doing so takes the system offline and prevents customers from being able to access the system.
    c. Yes, doing so verifies the procedure and backup media are working correctly.
    d. Yes, doing so improves the efficiency of the system.

75. The maximum acceptable down time after a computer system failure is determined by a company's
    a. recovery time objective.
    b. recovery point objective.
    c. recovery objective.
    d. maximum time recovery objective.

سليمان طارق شبل ابراهيم السعدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

76. Which of the following is incorrect with regards to a data *archive*?
    a. Archives can be a copy of a database.
    b. Archives should be stored in different locations.
    c. Archives are usually encrypted.
    d. Physical and logical controls are the primary means of protecting archive files.

77. Identify the most important component of a disaster recovery plan below.
    a. documentation
    b. operating instructions
    c. periodic testing
    d. on-site and off-site storage

78. Identify the preventive control below.
    a. reconciling the bank statement to the cash control account
    b. approving customer credit prior to approving a sales order
    c. maintaining frequent backup records to prevent loss of data
    d. counting inventory on hand and comparing counts to the perpetual inventory records

79. According to The Sarbanes-Oxley Act of 2002, the audit committee of the board of directors is directly responsible for
    a. hiring and firing the external auditors.
    b. performing tests of the company's internal control structure.
    c. certifying the accuracy of the company's financial reporting process.
    d. overseeing day-to-day operations of the internal audit

2021/2022 2021/2022 2021/2022
سليمان طارق سليمان عبد الحميد السعدى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

department.

80. Which of the following measures can protect a company from AIS threats?
    a. Take a proactive approach to eliminate threats.
    b. Detect threats that do occur.
    c. Correct and recover from threats that do occur.
    d. All of the above are proper measures for the accountant to take.

81. Internal control is often referred to as a(n) ________, because it permeates an organization's operating activities and is an integral part of management activities.
    a. event
    b. activity
    c. process
    d. system

2021/2022 2021/2022 2021/2022

82. Duplicate checking of calculations is an example of a ________ control, and procedures to resubmit rejected transactions are an example of a ________ control.
    a. corrective; detective
    b. detective; corrective
    c. preventive; corrective
    d. detective; preventive

83. Which of the following statements is *true* with regards to system availability?
    a. Human error does not threaten system availability.
    b. Threats to system availability can be completely eliminated.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

c. Proper controls can maximize the risk of threats causing significant system downtime.

d. Threats to system availability include hardware and software failures as well as natural and man-made disasters.

84. Which type of control is associated with making sure an organization's control environment is stable?

a. general

b. application

c. detective

d. preventive

85. Which type of control prevents, detects, and corrects transaction errors and fraud?

a. general

b. application

c. detective

d. preventive

86. The primary purpose of the Foreign Corrupt Practices Act of 1977 was

a. to require corporations to maintain a good system of internal control.

b. to prevent the bribery of foreign officials by American companies.

c. to require the reporting of any material fraud by a business.

d. All of the above are required by the act.

سليمان طارق شبل ابراهيم السعدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

87. Congress passed this federal law for the purpose of preventing financial statement fraud, to make financial reports more transparent and to strengthen the internal control of public companies.
    a. Foreign Corrupt Practices Act of 1977
    b. The Securities Exchange Act of 1934
    c. The Sarbanes-Oxley Act of 2002
    d. The Control Provision of 1998

88. Which of the following was *not* an important change introduced by the Sarbanes-Oxley Act of 2002?
    a. new roles for audit committees
    b. new rules for auditors and management
    c. new rules for information systems development
    d. the creation of the Public Company Accounting Oversight Board

2021/2022 2021/2022 2021/2022

89. A(n) ________ measures company progress by comparing actual performance to planned performance.
    a. boundary system
    b. diagnostic control system
    c. interactive control system
    d. internal control system

سليمان طارق شبل ابراهيم السعدي

90. A(n) ________ helps top-level managers with high-level activities that demand frequent and regular attention.
    a. boundary system
    b. diagnostic control system
    c. interactive control system
    d. internal control system

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

91. Which of the following is *not* a violation of the Sarbanes-Oxley Act (SOX)? The management at Oanez Dinnerware
    a. asked their auditors to make recommendations for the redesign of their information technology system and to aid in the implementation process.
    b. hired the manager from the external audit team as company CFO twelve months after the manager had worked on the audit.
    c. selected the company's Chief Financial Officer to chair the audit committee.
    d. did not mention to auditors that the company had experienced significant losses due to fraud during the past year.

92. The Sarbanes-Oxley Act (SOX) applies to
    a. all companies with gross annual revenues exceeding $500 million.
    b. publicly traded companies with gross annual revenues exceeding $500 million.
    c. all private and public companies incorporated in the United States.
    d. all publicly traded companies.

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدني

93. Irene Pacifica was relaxing after work with a colleague at a local watering hole. Well into her second martini, she began expressing her feelings about her company's budgeting practices. It seems that as a result of controls put in place by the company, her ability to creatively manage his department's activities have been curtailed. The level of control that the

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

company is using in this case is a(n)
   a. boundary system.
   b. diagnostic control system.
   c. interactive control system.
   d. belief system.

94. Which of the below is *not* a component of the COSO ERM?
   a. monitoring
   b. control environment
   c. risk assessment
   d. compliance with federal, state, or local laws

95. The COSO Enterprise Risk Management Integrated Framework stresses that
   a. risk management activities are an inherent part of all business operations and should be considered during strategy setting.
   b. effective risk management is comprised of just three interrelated components; internal environment, risk assessment, and control activities.
   c. risk management is the sole responsibility of top management.
   d. risk management policies, if enforced, guarantee achievement of corporate objectives.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Chapter Four
Information Security Evaluation

4-1. Introduction

In the previous chapter, the security controls of information have been discussed. In this chapter, the need as well as the importance of evaluating the security of information will be outlined. The different alternative approaches for evaluating the security of information will be considered and the main requirements for implementing an information security tool will be presented. In addition, the limitations and problems concerned with information security evaluation methods will be mentioned. Finally, the approach adopted in this study for evaluating the security of information will be highlighted.

2021/2022 2021/2022 2021/2022

4-2. Evaluating Information Security: Need and Importance

Goodhue et al. (1991) have mentioned that there are numerous methodological questions regarding how to clearly measure security concern. Although many of the previous studies have employed user perception as an empirical measure, such measures may lack theoretical clarity, because they lack a theoretical underpinning. The most commonly cited reference discipline for these measures has been job satisfaction research. However, “IS satisfaction” has not been well enough defined to clarify how it is similar to or different from “job satisfaction” (p. 15).

30006101601571 30006101601571 30006101601571

Risk analysis of the information technology environment represents another approach for evaluating information security.

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

A literature review by Eloff et al. (1993) indicated that inconsistent terminology had been used in previous studies. These differences in terminology gave rise to the need for a standard set of terms to be used for the comparison of various risk analysis methods.

As Kumar (1990) points out, evaluation in general serves to:

1. Verify that the system met requirements;
2. Provide feedback to development personnel;
3. Justify the adoption, continuation or termination of a project;
4. Clarify and set priorities for needed modifications; and
5. Transfer responsibilities from developers to users (from, Conrath et al., 1993, p. 267).

According to Symons et al. (1993), evaluation plays a crucial role at many stages of information systems development. Before introducing a new system a feasibility study should be done to appraise it and to decide whether to purchase it or not. During implementation evaluation functions as a learning and control mechanism; it is usually done informally. Post-implementation evaluation, although it is theoretically valuable, is rarely carried out by organizations.

However, all types of business systems have a need for internal controls and security safeguards. During the design, implementation, production and maintenance phases of a business life cycle, some form of documentation of the controls provided in the system is necessary as means of communicating between designers, users and auditors and for purposes of preserving information for subsequent use by users and auditors who might not have been initially involved in the system

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

development cycle (Computer Security Auditing and Controls, 1991).

Solms (1996) has noted that nowadays many business partners need to link their computer systems for business reasons, but that, they first want to receive some sort of proof that their partners have an adequate level of information security in place. He also suggested that a security evaluation and certification scheme that could instil confidence and assurance regarding information security status to external and business parties would solve a lot of problems for the commercial world. Accordingly, the objective of Solms's paper in 1996 was to prove that the commercial world needed some information security evaluation scheme: that could provide assurance to internal as well as external parties that adequate security controls were installed; and could define a set of criteria which such a security evaluation scheme must satisfy to be successful.

Evaluating the security of information is not an easy task. Reviewing the available literature in this area reveals a lot of confusion and inconsistencies since research in evaluating the security of information system is considered to be in its infancy stage. Conrath et al, (1993), in an extensive search of the information systems evaluation literature, revealed that there were no generally accepted performance measures. Since information security is an important integral part of the accounting system, so it comes under the umbrella of that result. In the following section, the researcher will briefly present the alternative approaches that could be used and implemented in evaluating the security of information.

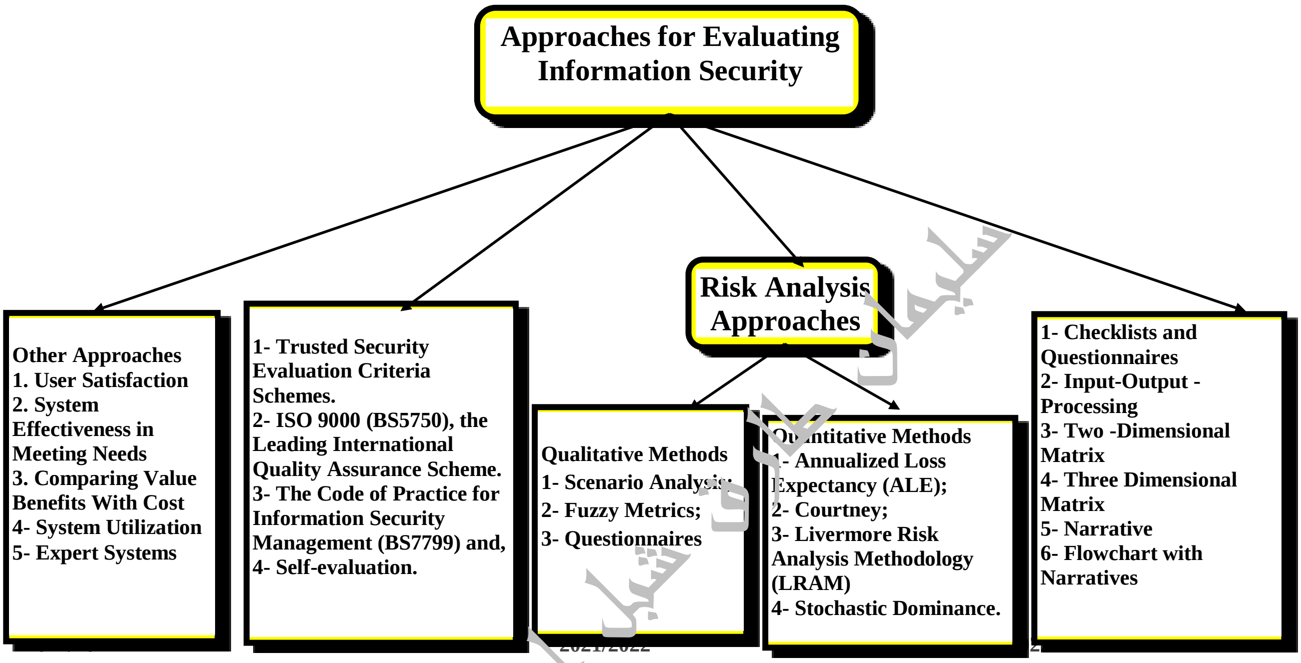
2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-3. Different Approaches for Evaluating Information Security

The different approaches and techniques for evaluating the security of information are illustrated in figure 4-1.


Approaches for Evaluating Information Security
Other Approaches
1. User Satisfaction
2. System Effectiveness in Meeting Needs
3. Comparing Value Benefits With Cost
4- System Utilization
5- Expert Systems
1- Trusted Security Evaluation Criteria Schemes.
2- ISO 9000 (BS5750), the Leading International Quality Assurance Scheme.
3- The Code of Practice for Information Security Management (BS7799) and,
4- Self-evaluation.
Risk Analysis Approaches
Qualitative Methods
1- Scenario Analysis;
2- Fuzzy Metrics;
3- Questionnaires
Quantitative Methods
1- Annualized Loss Expectancy (ALE);
2- Courtney;
3- Livermore Risk Analysis Methodology (LRAM)
4- Stochastic Dominance.
1- Checklists and Questionnaires
2- Input-Output - Processing
3- Two -Dimensional Matrix
4- Three Dimensional Matrix
5- Narrative
6- Flowchart with Narratives

(Figure 4-1)
(Different Approaches for Evaluating Information Systems Security)

According to Solms (1996) a number of evaluation and certification techniques could be linked to information security. These techniques are:

- Trusted Security Evaluation Criteria Schemes;
- ISO 9000 (BS5750), the leading international quality assurance scheme;
- The code of Practice for Information Security Management (BS7799); and
- Self-evaluation.

سليمان طارق شبل ابراهيم السعدني

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Computer Security Auditing and Controls (1991) reported that the most common approaches to documenting internal and security controls (used in evaluating the information security as well) as cited in the literature and used by various organizations are:

- Checklists and questionnaires
- Input-Output-Processing
- Two-dimensional Matrix
- Three-dimensional Matrix
- Narrative
- Flowchart with narratives.

He also presented the advantages and disadvantages of each of the above methods. Finally, he concluded that each method suffers from deficiencies that render them less than ideal if one wishes a comprehensive and effective method, in tune with the current emphasis on risk assessment concepts for control building. It was suggested that the ideal approach should first consider the security threats, the point in the system at which they can materialize, the extent or magnitude of the potential exposure that security threats would cause at that point in the system, the specific control or security objectives to be met, the "specific" control solutions and the economic incentives to invest in the controls.

2021/2022 2021/2022 2021/2022

Conrath et al. (1993) stated that the evidence from the literature leads one to conclude that, since no single measure is adequate, a combination is necessary to make up for individual limitations. Although several measures of implementation success have been identified in the information systems literature, under various names, four measures subsume most of them. These are:

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

1. Satisfaction with the system;
2. The system's effectiveness in meeting needs;
3. Cost / benefit analysis; and
4. System utilization.

From this researcher's point of view, although the previous techniques have been used in evaluating the performance of information systems in general, they could be used safely in evaluating the security specifically of information systems. A combination between checklist questionnaire and risk analysis methods has been made to avoid the deficiencies of each individual method and to enhance the potential benefits through integration of these methods. Some researchers have considered security evaluation as an integral part of the information technology risk management process. For example, Rainer et al. (1991) stated that the risk management life cycle (see figure 6-2) begins with the risk analysis process, which analyses IT assets, threats, and the vulnerabilities of those assets. Following risk analysis, several alternative security measures that address a particular risk should be presented to management for an implementation decision.

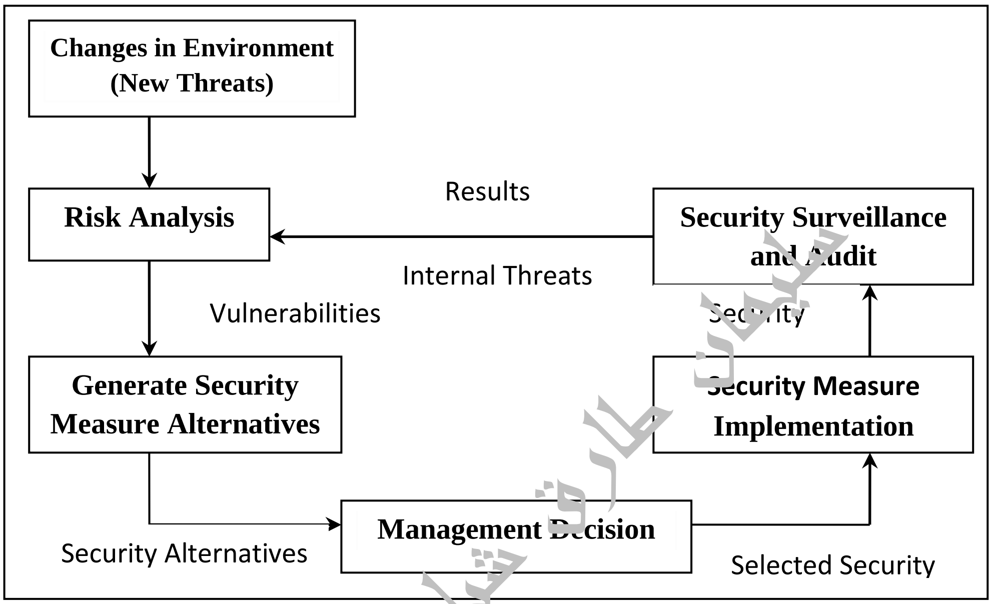
The cost of the security measures should be weighted against their effectiveness in reducing risk. Since achieving 100 percent IT security is impossible, managers must evaluate the choice of security measures. In general, the cost of security measures should not outweigh the benefits.

However, in any risk analysis approach, managers should identify the information assets, investigate the main threats facing their INFORMATION assets and the vulnerabilities of those assets to these prospected risks. They should also evaluate the expected loss resulting from the occurrence of these security

سليمان طارق شبل ابراهيم السعيدي 2021/2022 2021/2022 2021/2022 30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

threats. According to Rainer et al. (1991) there are many methods currently in use that attempt to measure the loss exposure of IT assets, which could be categorized as quantitative or qualitative risk analysis methods.



2021/2022 2021/2022 2021/2022

(Figure 2)

(The Risk Management Life Cycle)

Quantitative Risk Analysis Methodologies

Most quantitative methods are based on regarding loss exposure as a function of the vulnerability of an asset to a threat, multiplied by the probability of the threat becoming a reality. These methods are called “expected value analysis” and include four models:

- Annualized Loss Expectancy (ALE);
- Courtney;
- Livermore Risk Analysis Methodology (LRAM), and
- Stochastic Dominance (Rainer et al., 1991).

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Delphi techniques may be used in conjunction with each of the above methods to reach a consensus value of IT assets as well as the probability estimates of threat occurrence.

Qualitative Risk Analysis Methodologies

Sometimes management needs a rapid, approximate evaluation of their organization's IT risk and security situation. Management might decide in this case not to spend a lot of time and effort that might be required to perform a quantitative risk analysis. In such cases, qualitative risk analysis approaches might be used.

Qualitative methodologies attempt to express risk in terms of descriptive variables, rather than in precise monetary terms. These approaches are based on the assumption that certain threats or losses of data could not be appropriately expressed in dollars or discrete events, and that precise information might be unobtainable. These qualitative risk analysis methodologies include:

2021/2022 2021/2022 2021/2022

- Scenario Analysis;
- Fuzzy Metrics; and
- Questionnaires (Rainer et al., 1991).

Again, Delphi techniques could be used with any of the three methods mentioned above to clarify descriptive or natural language variables. In the following section, the main requirements for implementing an effective evaluation of the information security will be presented.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-4. Requirement to Implement An Information Security Evaluation Tool

According to Mathieson (1993) a researcher should ask some questions before conducting the evaluation process.

1. **Why is the evaluation being conducted?**
   This is the first and most important question since the design of evaluation sessions depends on the objectives that the researcher wishes to achieve.

2. **What is being evaluated?**
   There are three sets of issues that should be considered. First, the focus of the question being asked. Second, the specificity of the question (the level of detail) should be decided. Third, the researcher should understand when an investment in expensive but realistic security controls is justified.

2021/2022 2021/2022 2021/2022

3. **Who are the evaluators?**
   There are a number of criteria that should be used to select the evaluators of information security. First, they should know enough to be able to judge the security issues (threats, controls etc.) correctly. Second, they should be motivated to provide an evaluation. Third, they should not be biased by outcome goals before they evaluate the system.

سليمان طارق شبل ابراهيم السعيدنى

4. **How should the evaluation session be administered?**
   Since many evaluation sessions are uncontrolled, the researcher should consider the following considerations.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- The first objective is to focus the evaluators on the exact questions that they should consider;
- Second, evaluators should be given the resources they need to complete their evaluation,
- Third, the researcher should try to motivate the evaluators. People who think their decisions will have personal consequences will spend more time and effort making those decisions than would people who think otherwise.
- Fourth, the researcher should avoid introducing outcome biases. In particular, evaluators should also know that evaluations are anonymous, as far as the researcher is concerned.

In summary, the main requirements needed for implementing an effective security evaluation technique for information are:

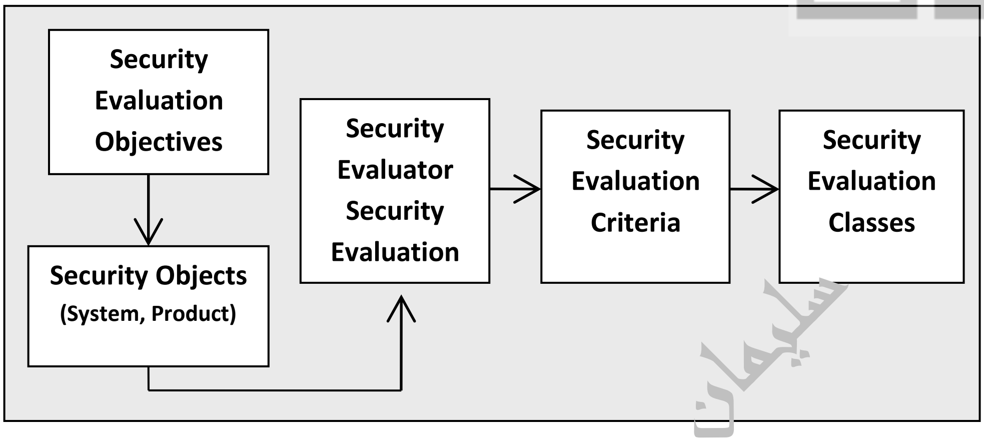
1. The objectives of the security evaluation should be well defined,
2. The security objects which represent the security of the system, subsystem, application, or product being evaluated should be specified.
3. The evaluator(s) of the security system should be determined, whether internally or externally selected (e.g., internal or external auditors, or security professionals).
4. Security classes or categories should be specified so that the objects evaluated can be precisely classified.
5. Security criteria, measures or countermeasures should be selected to evaluate the adequacy and the effectiveness of the security system.

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

These main elements for evaluating the security of information are illustrated in figure 6-3. They are briefly discussed in the following sections.


Security Evaluation Objectives
Security Objects (System, Product)
Security Evaluator Security Evaluation
Security Evaluation Criteria
Security Evaluation Classes

(Figure 6-3)
(Information Security Evaluation Elements)

4-4-1. The Evaluation Objectives

2021/2022 2021/2022 2021/2022

The main objectives of the evaluation process related to information security should be determined. The evaluation objective could be to take a decision related to purchasing a new accounting software security package; it could be that of evaluating the effectiveness of an implemented security program or security package. The objective could also be evaluation of the security of a specific application (such as payroll, or customer' loans). Finally, evaluating the security of the overall information could be the evaluation objective.

4-4-2. The Evaluation Objects

30006101601571 30006101601571 30006101601571

The evaluation object could be the information system, subsystem or IT product whose security status needs to be

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

evaluated. Alternatively, it could be the overall computerized accounting system, or some subsystems or applications (such as payroll, purchasing application, or deposit applications); it could be an IT product (a software package or a new program).

4-4-3. The Evaluator

The evaluation task could be accomplished either internally or externally. The internal evaluation of information security could be performed by computer specialists from the organization's internal departments (e.g., computer department, IT department, etc.). In other cases, this task could be carried out by the internal auditors of the organization.

Internal evaluators should have sufficient knowledge and adequate skills to accomplish this task. It is preferable if the evaluator has inside motives to be involved in the evaluation process.

On the other hand the evaluation could be done by an external evaluator. The external security evaluator should be an information security specialist who has a professional certificate. The evaluation of information security could be done by the external auditor of an organization.

2021/2022 2021/2022 2021/2022

4-4-4. Information Security Categories

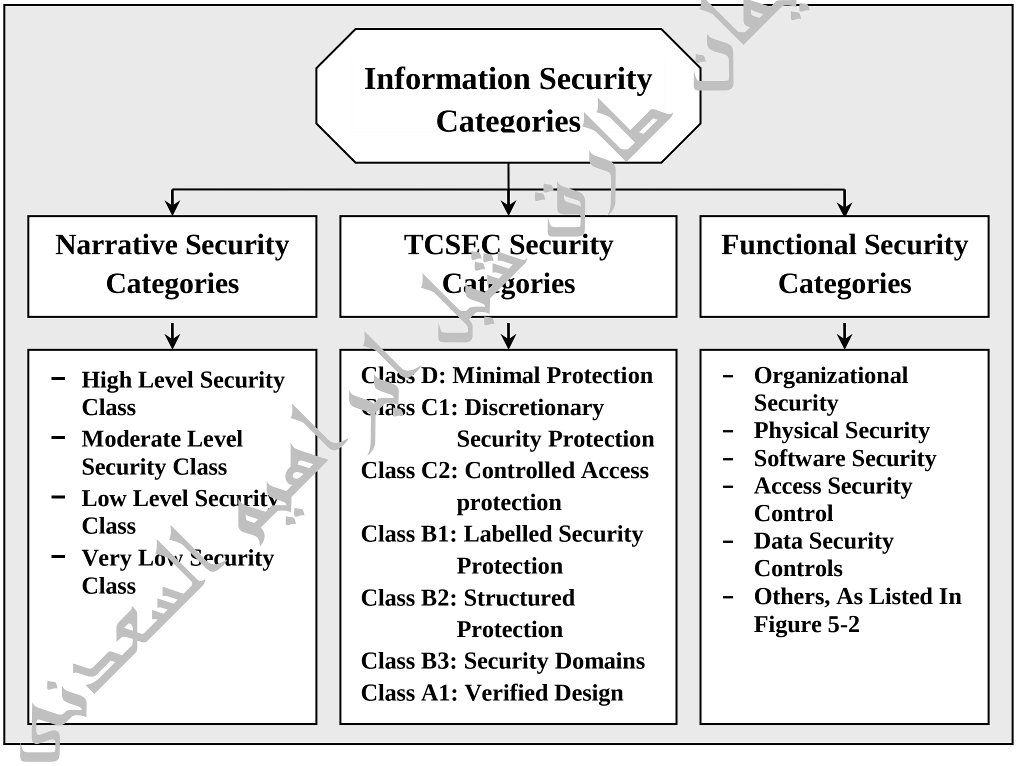
Solms (1994) comments that information security is a very broad area. It needs to be broken down into smaller chunks or categories to make it more manageable. Many authors have subdivided information security into categories and sub-categories and most such categorizations differ quite drastically (p. 148). However, several alternatives could be used to categories the information security in an organization. The status

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

of the information security could be classified in a narrative way according to its strength or weakness into “high”, “moderate”, “low” and “base” levels of system security (figure 6-4).

The security of information systems could also be categorized under functional security groups, which includes similar functions and interrelated security countermeasures. These information security groups could be classified as the following: organizational; environmental, physical (hardware), software and access control, Internet and communication security (see figure 4-4 and figure 5-2 for an expanded categorization).


Information Security Categories
Narrative Security Categories
TCSEC Security Categories
Functional Security Categories
– High Level Security Class
– Moderate Level Security Class
– Low Level Security Class
– Very Low Security Class
Class D: Minimal Protection
Class C1: Discretionary Security Protection
Class C2: Controlled Access protection
Class B1: Labelled Security Protection
Class B2: Structured Protection
Class B3: Security Domains
Class A1: Verified Design
– Organizational Security
– Physical Security
– Software Security
– Access Security Control
– Data Security Controls
– Others, As Listed In Figure 5-2

2021/2022

سليمان طارق شبل ابراهيم السعدني

(Figure 4-4)
(Information Security Categories)

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

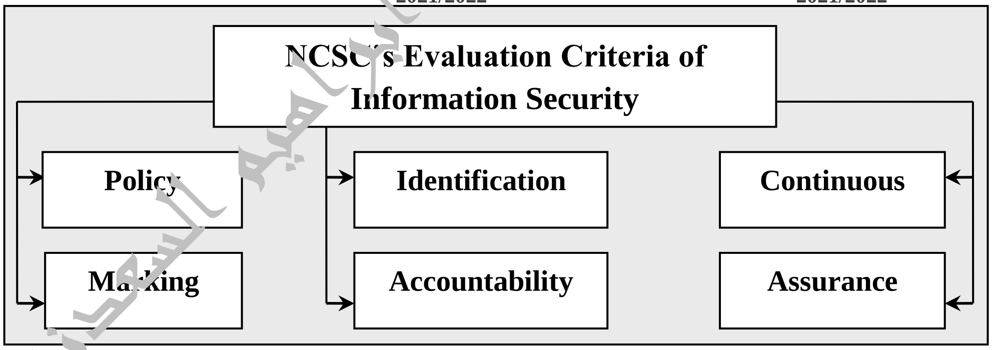
Alternatively, the Trusted Computer System Evaluation Criteria (TCSEC) determined some restrictive classes that could be used to classify or categories the information security according to its status, as follows:

Class D: Minimal Protection
Class C1: Discretionary Security Protection
Class C2: Controlled Access protection
Class B1: Labeled Security Protection
Class B2: Structured Protection
Class B3: Security Domains
Class A1: Verified Design.

4-4-5. Information Security Criteria or Measures

The National Computer Security Committee (NCSC) used a group of requirements called "Criteria" for the security classes listed above to identify various measures and requirements in the following six areas:

2021/2022 2021/2022 2021/2022



سليمان طارق قبل ابراهيم السعدى

(Figure 4-5)
(NCSC's Evaluation Criteria of Information Security)

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-4-5-1. Policy

According to the TCSEC, the first requirement is for a system-level security policy defining how instruction will be enforced. NCSC's Evaluation Criteria of Information Security Policy Marking Identification Accountability Assurance Continuous Protection

"Requirement 1 - Security Policy - There must be an explicit and well-defined security policy enforced by the system. Given identified subjects and objects, there must be rules used by the system to determine whether a given subject can be permitted to gain access to a specific object. Computer systems must enforce a security policy that can implement access rules for handling sensitive information. These rules include requirements such as: No person lacking proper authority shall obtain access to sensitive information. In addition, discretionary security controls are required to ensure that only selected users or groups of users may obtain access to data (e.g., based on a need-to-know)" (Overview of NCSC Security Evaluation, 1997).

2021/2022 2021/2022 2021/2022

4-4-5-2. Marking

The second requirement of TCSEC is marking, which essentially states that every object must be associated with a "label" that indicates the security level of that object. "Requirement 2 - Marking - Access control labels must be associated with objects. This is done to control access to information stored in a computer, and relies on a mandatory security policy that defines how to mark every object with a label that reliably identifies the object's sensitivity level and / or the modes of access accorded to subjects who may potentially access

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

the object. This can be expanded to include non-discretionary controls in higher levels of evaluation (class B and above)".

4-4-5-3. Identification

The third requirement is that every subject must be uniquely and convincingly defined. Further, all access requests must be checked against the subjects assigned permissions. "Requirement 3 - Identification - Individual subjects must be "identified". This is done so that each access to information can be mediated by who is accessing the information and what classes of information they are authorized to deal with. This identification and authorization to information must be securely maintained by the computer system and be associated with every active element that performs some security relevant to the system" (Ibid.).

4-4-5-4. Accountability

2021/2022 2021/2022 2021/2022

The fourth fundamental requirement is accountability. The system must maintain complete, secure records of actions that effect security, including users' set-up, assignment, or change of security level (privilege group) and denied access attempts. "Requirement 4 - Accountability - Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party. A trusted system must be able to record the occurrences of security-relevant events in an audit log and must have the capability to select the audit events to be recorded to minimize the auditing expense and to allow efficient analysis. Audit data must be protected from modification and authorized destruction and must permit detection for after-the-act investigation of security violations".

30006101601571 30006101601571 30006101601571

سليمان طارق شبل ابراهيم السعيدي

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-4-5-5. Assurance

The fifth requirement is for assurance, which means that the information must contain mechanisms that enforce security and it must be possible to measure the effectiveness of these mechanisms. According to TCSEC "Requirement 5 - Assurance - The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements from 1 to 4 above".

TCSEC stated that "In order to assure that the four requirements of security policy, marking, identification, and accountability are enforced by computer system, there must be an identified and unified collection of hardware and software controls performing those functions. These mechanisms are typically embedded in the operating system and designed to perform the assigned tasks in a secure manner. Then the basis for trusting the system mechanisms in their operational environment must be clearly documented and followed so that it is possible to independently examine the evidence and evaluate their sufficiency" (Overview of NCSC Security Evaluation, 1997).

2021/2022 2021/2022 2021/2022

The assurance, or confidence, based on some form of analysis, that an objective or requirement is being / will be achieved has two aspects:

- The level of confidence that a violation of information security will not occur
- The level of confidence that a violation of information security has not occurred.

Confidence that a violation will not occur is based on a belief in the effectiveness and correctness of security controls

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

and safeguards and other preventive security measures associated with information, as well as by their appropriateness to defined security objectives.

4-4-5-6. Continuous Protection

The final requirement of the TCSEC is that protection should be continuous. “Requirement 6 - Continuous Protection - The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes”. Again, TCSEC confirmed that “Computer systems cannot be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion”.

This essentially means that the hardware and software mechanism that implements security must itself be protected against unauthorized changes. Likewise, it is necessary to evaluate system reliability, right down to the level of system security, as it evolves with new versions and platform changes.

2021/2022 2021/2022 2021/2022

The most important features of these criteria are that they can be trusted by evaluators, that they are available for public inspection and that they have withstood the tests of time and logic. The NCSC thus offer what is a generally-accepted basis for evaluation. The acceptance of these criteria is growing in both the public and private sectors, analogous to the generally accepted accounting practices in the accounting realm or to generally accepted audit procedures for internal and electronic data processing auditors (Ibid.).

30006101601571 30006101601571 30006101601571

It is generally accepted that class C2 defines the baseline level of security features that should be examined and

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

implemented. This has become the minimum security rating required by many governments and offices (such as branches of the US military, federal reserve, or intelligence agencies) and by many corporations. Accordingly, class C2 is the minimum-security rating granted by the NCSC. Class B introduces a higher level of security for dedicated and non-dedicated systems that manipulate and transfer sensitive financial or proprietary data. It defines a number of additional requirements over the previous level; most notably in the areas of mandatory access control and data labeling.

This level of security is appropriate for banking and governmental agencies that deal with highly sensitive or classified data.

Solms et al. (1994) reported that very few international standards or criteria currently exist. Therefore, TCSEC and ITSEC are the most common criteria used to evaluate operating system security. They also argued that an international set of information security criteria would make it possible for an organization to compare its information security level with that of another. Such a set of security criteria could be known and recognized anywhere in the world (ibid. p.148).

سليمان طارق شبل ابراهيم السعدى
2021/2022 2021/2022 2021/2022

In the following section, the process of evaluating information security will be discussed in some detail.

4-5. The evaluation process of Information Security

Wheatman (1998) stated that to justify properly any expense in information security, organizations must perform a threat assessment. The steps of this analysis include assessing potentially threatening motives, means, and opportunities; categorizing the threats; prioritizing multiple available security

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

countermeasures; evaluating their costs; and deciding whether to implement safeguards or to accept a certain degree of risk.

Without such an assessment, certification - or any other measures - is likely to be a tactical, point solution, rather than a part of an overall risk-based security strategy. The evaluation of information security could mean:

1- An evaluation process to determine whether or not a condition of security was met; or

2- The comparison of the current controls in place against some complete set of security criteria.

Both of these security evaluation techniques will be discussed in the following sections.

4-5-1. Evaluation for a Condition

TCSEC as well as ITSEC have identified various levels or classes of security for an operating system environment. TCSEC has defined four levels of protection with subclasses: D, C1, C2, B1, B2, B3 and A1. Each of these classes represents a certain condition of information security. However, these security conditions could be met in various ways, by using different techniques and different countermeasures. Therefore, somebody must certify that the associated condition has been met. If a certain product has been certified as a B2 system, everybody should know what level of protection is associated with that specific product.

Solms et al. (1994) argued that the ideal solution to information security evaluation would be a technique of self evaluation, which can only be possible if a security condition being measured is very clearly defined and very specific guidelines are written on how the evaluation be executed. The

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

whole idea of self-evaluation seems unattainable at this stage, partly because of the lack of an international standard (p. 149).

The evaluation of information security could be done against one of the following security criteria:

- Trusted Security Evaluation Criteria.
- The ISO 9000 Series of Standards
- Code of Practice

4-5-1-1. Security Evaluation against Trusted Security Evaluation Criteria

The Trusted Computer Security Evaluation Criteria (TCSEC), first published in 1985, were the first criteria to achieve wide acceptance. The Information Technology Security Evaluation Criteria (ITSEC), published in 1990, and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), 1993, were the European and Canadian responses to TCSEC respectively.

2021/2022 2021/2022 2021/2022

The trusted computer system evaluation criteria defined in the issued documents apply primarily to trusted, commercially available, automatic data processing (ADP) systems. They are also applicable to the evaluation of existing systems and the specification of security requirement for ADP systems acquisition (Overview of NCSC Security Evaluation, 1997). Evaluation criteria refer to products (such as an operating system or systems, or a collection of products assembled to meet the specific requirements of a given application). However, not all criteria mentioned above evaluate both products and systems: for example, TCSEC only evaluate products.

30006101601571 30006101601571 30006101601571

According to Solms (1996), in all the above evaluation criteria, three aspects have been addressed: ***functionality*** (the

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

security features of a system), ***effectiveness*** (to ensure that mechanisms used are appropriate for the given security requirements) and *assurance* (the thoroughness of evaluation). TCSEC considers all three aspects simultaneously in the definition of its security classes, whereas ITSEC allows them to be considered independently.

The system or product to be evaluated against ITSEC is referred to as the target of evaluation (TOE). Each TOE needs a document called the "security target". The security target of a system contains:

- A system security policy, including the security objectives, the envisaged threats, the list of the security enforcing functions and the list of physical, personnel and procedural measures.
- A specification of the required security-enforcing functions.
- A definition of the required security mechanism (optional).
- The claimed minimum strength of mechanism rating.
- The target evaluation level (Gentile, et al., 1994).

2021/2022 2021/2022 2021/2022

4-5-1-2. The ISO 9000 Series of Standards

The ISO 9000 Series of Standards is a series of international quality assurance standards that apply to the quality management system and process used to produce a product. ISO 9000 establishes a basic set of quality system requirements necessary to ensure that the organization's process is capable of consistently producing products that meet the expectations of the customer. ISO 9000 does not address information security directly, but many security related issues are addressed by ISO 9000, for example, security policy, risk analysis and continuity

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

planning. The ISO series of standards was published in 1987, has been adopted by many countries and is rapidly replacing prior national and industry-based standards (Solms, 1996).

From Solms' (1996) point of view the ISO 9000 is a generic model for quality assurance in design / development, production, installation and servicing. The requirements of the standard have to be formally interpreted by each organization wishing to be registered as an evidence of meeting its requirements. ISO 9000 makes use of an audit-oriented evaluation method, which means that mainly documentation, procedures and processes are evaluated. Under ISO 9000 a certificate is issued following a successful evaluation. The ISO 9000 certificates are used by organizations to create confidence among their customers and clients in their ability to deliver goods and provide services that meet the clients' requirements.

4-5-1-3. Code of Practice

2021/2022 2021/2022 2021/2022

The Code of Practice for information security management is a reference document for managers and employees who are responsible for initiating, implementing, and maintaining information security within their organizations. The objectives of the Code of Practice are: firstly, to provide a common basis for organizations to develop, implement, and measure effective security management practice, and, secondly, to provide confidence in inter-company trading. The Code of Practice was published in 1993 and in 1995 a British Standard - BS7799, based on the Code of Practice was published. This British Standard was amended in 1999.

30006101601571 30006101601571 30006101601571

Solms (1996) argued that a Code of Practice intends to serve as a single reference point for identifying the range of

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

controls required from most institutions encountered in industry and commerce. Ten categories, of the entire IT- environment, in general use in most companies, are identified in the Code of Practice. Under each of these ten categories a comprehensive set of security controls are listed. Not all of these controls are applicable to every IT-environment and they should be used selectively, according to local circumstance.

Solms confirmed that no formal evaluation and certification scheme for the Code of Practice currently exists, but a certification and accreditation scheme for compliance to BS 7799 is under consideration in the United Kingdom (ibid., p. 285).

4-5-2. Evaluation through Comparison (Information Security Self-evaluation)

Since there are no international generally accepted security criteria or measures currently available, Solms et al. (1994) argued that the alternative approach of evaluating information security by comparing the security status against predefined criteria is problematic. This would be possible only if an international accepted set could be identified. Self-evaluation might then even become a possibility: because the set used in the evaluation would be internationally specified, an information security measurement level would be the same for everybody (p.149). Solms suggested that the only possibility at this stage is to use information security countermeasures as the criteria. The security evaluation would then take the form of comparing installed information security countermeasures against a complete set of predetermined security countermeasures as an evaluation criterion.

سليمان طارق سليمان ابراهيم السعيدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Again, Solms (1996) confirmed that the ideal solution would be some IT security self-evaluation scheme; where the current installed information security controls can be evaluated by the organization itself to demonstrate whether they have achieved adequate protection, or not. This will provide management with a checklist against which they can test their own current controls and approach in the area of information security. He also argued that various organizations use various techniques and approaches to evaluate their own information security status. These techniques vary from pure "gut-feel" approaches, where a very high level security screening is done, to more formal approaches where the information security status of the organization is "measured" according to a definite methodology or against a specific checklist.

However, two kinds of problems have been identified by Solms et al. (1994) regarding the self-evaluation technique. Firstly, security countermeasures might be installed in an organization, but then managed or operated ineffectively. Secondly, during the process of self-evaluation, prejudice might affect its accuracy. Solms (1996) argued that, unless the criteria to evaluate against are well defined, with strict, definite conformance testing, the results will always be treated with some suspicion and will never be accepted outside the organization. The fact is underlined by European Computer Manufacturers Association (ECMA), stating "when criteria are ill-defined and ambiguous, any evaluation process (including one by a third party) will be arbitrary … and potentially very costly". Self-evaluation could be useful, but only for internal usage.

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-6. The Limitations of Information Security Evaluation

Evaluating the security of information is a very sensitive issue and it is not an easy task to be carried out since it faces many challenges and limitations. Warigon (1998) mentioned that every time one identifies and selects cost effective measures to secure information assets against various attacks, the attackers tend to double their efforts to defeat these security attempts. Therefore the best one can do is to prevent these attacks from happening, make them difficult to carry out, or be prepared to rebound quickly when they occur. One will not be well positioned to do any of these if effectiveness is not evaluated on an ongoing basis.

According to Gentile, et al. (1994) evaluation makes sense only if it is performed considering a given security objectives and identified threats (assumed threats, in the case of product): for instance, objectives and threats must be part of the ITSEC security targets. Solms (1996) argued that neither the common criteria of TCSEC or of ITSEC would provide the ideal evaluation scheme (p. 286). Some of the limitations and criticisms related to TCSEC and ITSEC security evaluation criteria are:

2021/2022 2021/2022 2021/2022

- It can clearly be seen that security evaluation criteria, in their current form, would not be able to provide a comprehensive evaluation scheme, although it must be stressed clearly that ITSEC, TCSEC and, in the future, any other common criteria will still provide the *building blocks* to help an organization towards information security in the entire IT environment (Solms, 1996, p. 282).
- Trusted products do not provide security on their own, but they contribute to it, if the associated products are correctly

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

adopted. However, in the author's opinion, the most important elements in the security system are the individuals who implement the system and use the products

- Strous (1994) commented that security evaluation criteria are not only intended for application in the evaluation and certification of IT-products and systems, they must also contribute to an integral, consistent, analytical, pragmatic and cost effective approach to IT- security within the user environment. The focus of security evaluations currently upon IT- products and systems: these form only part of a much broader IT environment, which is what really needs to be secured.
- One of the biggest problems haunting information security efforts is the lack of an adequate infrastructure: policies, procedures, responsibility statements and related information security matters (Solms, 1996).

Menkus (1991) recommended that, regardless of the computerized environment, any effort to evaluate the effectiveness of a particular information security mechanism should recognize that:

2021/2022 2021/2022 2021/2022

- Security is always considered as an overhead expense. Ideally, it involves both risk limitation and compromise containment. In most situations, security makes no direct, demonstrable contribution to either the accomplishment of an organization's stated mission or its realization of profit.
- If an organization's senior management will not accept the operational overhead associated with the implementation of the mechanism and no meaningful penalty is imposed on the individual who attempts to violate or compromise the

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

mechanism, the security policy or mechanism is essentially worthless.

- All security mechanisms are relatively ineffective. They can be compromised, subject only to the compromiser’s time and opportunity and access to enough of the right resources. In addition, no security mechanism maintains its absolute effectiveness indefinitely. The reliability of all these mechanisms deteriorates over time.
- No security mechanism, no matter how well designed or how complex or reliable its underlying technology, will be effective if those who require its use and those who must use it do not conform to the mechanism’s operational requirements (p. 11).

Symons et al. (1993) suggested that evaluation cannot be effective unless it is interpretative; taking account of the different and sometimes conflicting perspectives of those involved in systems development. Again, Solms et al. (1994) argued that no current, internationally accepted subdivision of information security exists. The information security tool will itself have to define categories which might be used during the evaluation process. Different information security evaluation tools might thus use different categories and define subdivisions for information security differently. Further no internationally recognized and accepted set of information security criteria or standard or conditions exist to be used in the evaluation process (p. 150).

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-7. Considerations for Selecting an Effective Evaluation Security Approach

Warigon (1998) argued that all security measures involve expenses, and security expenses require justification. The selection of security measures should rely on their impact on corporate data at risk. Cost-effective security measures should be selected to safeguard the data against known vulnerabilities. Selecting cost-effective security measures is a prudent business practice. It ensures that the costs of protecting the data do not exceed the maximum monetary value that loss of the data would represent. Senior management would, for instance, deem it imprudent to commit $500,000 annually to safeguard data that has an annualized loss expectancy of only $250,000. However, the cost factor should not be the only criterion for selecting appropriate security measures. Compatibility, adaptability, and potential impact on accounting system performance should also be taken into consideration.

2021/2022 2021/2022 2021/2022

Warigon (1998) recommended that evaluations should be conducted continuously to determine whether the security measures are:

1. Small, simple, and straightforward.
2. Carefully analyzed, tested, and verified.
3. Used properly and selectively so that they do not exclude legitimate access.
4. Elastic, so that they can respond effectively to changing security requirements.
5. Reasonably efficient in terms of time, memory space, and user-centric activities, so that they do not adversely affect the protected computing resources. It is equally important to ensure that the end-users understand and embrace the

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

propriety of security measures through an effective security awareness program.

Solms (1996) defined five criteria that should be considered in the evaluating IT security:

1. Trusted IT- products and systems, as evaluated and certified according to TCSEC and ITSEC, will not ensure a secure IT-environment, but will contribute as secure building blocks.
2. An audit-oriented evaluation approach is needed to ensure that all IT security policies, procedures, functional and related issues within the IT-environment are introduced and practiced as prescribed.
3. The evaluation scheme should span an entire IT-environment and should not be restricted to isolated products and systems.
4. The evaluation scheme should make provision for more than one level of security.
5. The standards and criteria defined need to be precise enough to enable self-evaluation, for domestic use.

2021/2022 2021/2022 2021/2022

Solms (1996) summarized the previous criteria in a comprehensive definition of an IT-Evaluation Security Evaluation Scheme (IT-ESES) as follows: “An audit-oriented evaluation and certification scheme that evaluates all relevant aspects, e.g. organizational, managerial, administrative, functional, etc., in an IT-environment, that possibly utilizes trusted products and systems, and that utilizes clearly defined criteria that will enable self evaluation”.

In the next section, the researcher will briefly presents the fundamental elements of the evaluation approach adopted in evaluating the security of information.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-8. The Adopted Approach for Evaluating the Security of Information

In developing the adopted approach for evaluating the security of information, the researcher considered Mathieson's (1993) recommendations for controlling bias in user evaluations. These suggested recommendations are:

1. Decide on the objective. In particular, what tasks are of interest?
2. Decide how specific the evaluation should be. In the early stage of a project, general information is the most valuable. As the project progresses, more specific information becomes important.
3. Tell the evaluators what tasks should be addressed and how specific the evaluations should be. If there are any special issues, the evaluators must be told to consider them.
4. Choose evaluators who are familiar with the tasks to be supported, who have some IS experience, and who know the constraints under which users operate.
5. Avoid evaluators who might be affected by social adjustment goals, protective goals, or value expressive goals. If such people are used, allow for biases when interpreting their evaluation.
6. Give the evaluators the resources they need including time and test data. Be careful to choose test data that is unbiased.
7. Have evaluation sessions administered by someone who is seen as impartial. The administrator should not be a member of the development team or the evaluator's functional area. The evaluation should not be anonymous

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

to the administrator, but may need to be disguised before being sent to the sponsor.

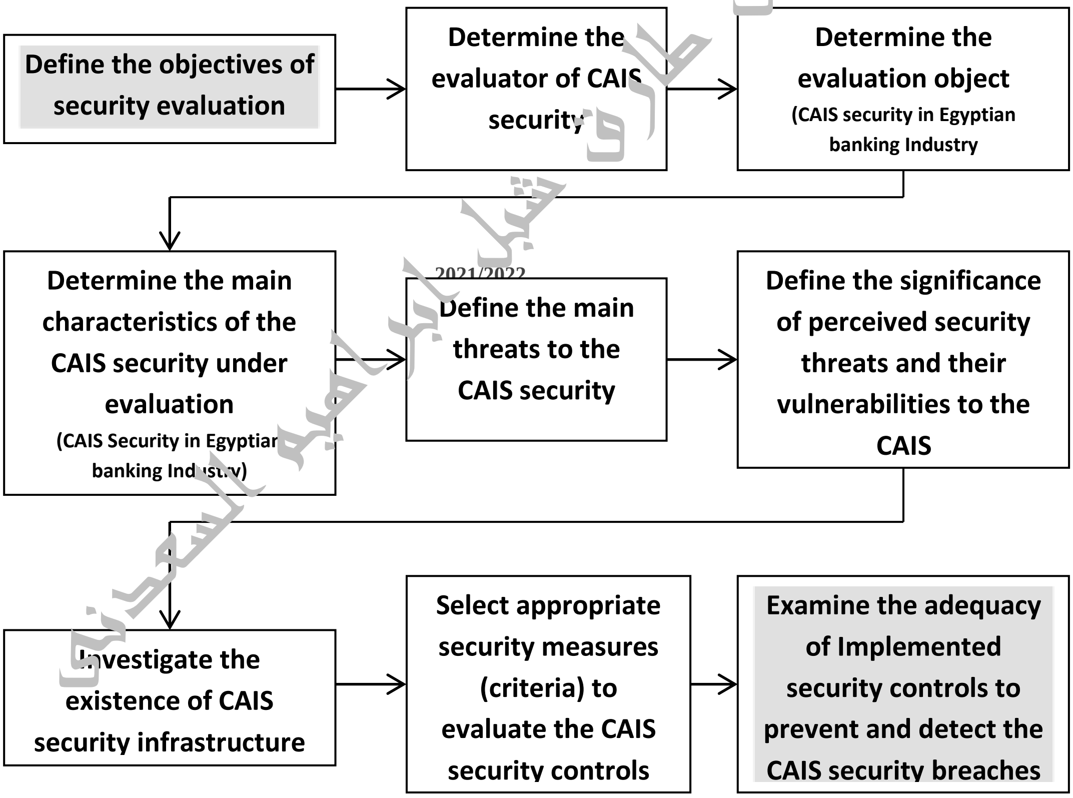
The selected evaluation approach adopted in this research is composed of nine main steps, illustrated in figure 6-6. Each of these steps will be briefly outlined in the following sections:

4-8-1. Define the Objectives of the Evaluation

The main objective is to evaluate the security of information in. Therefore, this research could be regarded as a post-implemented evaluation of information security, since it deals with the existing, implemented security programs or mechanisms.

سليمان طارق شبل ابراهيم السعدني

2021/2022


Define the objectives of security evaluation
Determine the evaluator of CAIS security
Determine the evaluation object (CAIS security in Egyptian banking Industry
Determine the main characteristics of the CAIS security under evaluation (CAIS Security in Egyptian banking Industry)
Define the main threats to the CAIS security
Define the significance of perceived security threats and their vulnerabilities to the CAIS
Investigate the existence of CAIS security infrastructure
Select appropriate security measures (criteria) to evaluate the CAIS security controls
Examine the adequacy of Implemented security controls to prevent and detect the CAIS security breaches

30006101601571 30006101601571 30006101601571

(Figure 6-6)

(The Adopted Approach for Evaluating the Security of CAIS)

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

The objectives of the information security evaluation are thus:

1. to investigate the existence and the main characteristics of information security policies, programs and infrastructure in place;
1. to explore the main perceived security threats that challenge information in place;
2. to investigate the vulnerability of the information to these threats;
3. to investigate the nature and adequacy of the implemented information security controls to reduce and eliminate the potential risks of these security threats; and
4. to enhance the awareness of the information security issues in the organizations.

4-8-2. Determine the Information Security Evaluator

The heads of internal audit departments and the heads of computer departments in the organization have been chosen as evaluator targets to evaluate the security of the information in their organizations.

2021/2022 2021/2022 2021/2022

4-8-3. Determine the Evaluation Object

The evaluation object in the current research is the security of information in the organization. The evaluation will cover information security policies, perceived security threats, and the security controls in place to eliminate these security threats or reduce harmful effects on information.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-8-4. Determine the Main Characteristics of Information under Evaluation

A number of questions were designed to collect the essential data regarding the nature and the characteristics of information implemented in the organization. This data is very important, since it gives information about the environment in which the accounting systems work.

4-8-5. Define the Significant Security Threats and Their Vulnerabilities to Information

The security threats of information should be identified. However, a list of these perceived security threats developed. After identifying the threats of information security, the next step is to determine their materiality and the vulnerabilities of information to these threats. The significance of the security threats could be investigated through their frequency of occurrence in the organization.

2021/2022 2021/2022 2021/2022

4-8-6. Investigate the Existence of Information Security Infrastructure

Investigating the existence of the information security infrastructure and its characteristics is an important element in evaluating the security of any information. The infrastructure includes the security policy or statement, procedures, responsibility statements and other related information security matters.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4-8-7. Select Appropriate Security Measures or Criteria to evaluate Information Security Controls

One of the main important steps in evaluating the security of information is selecting the appropriate security measures or criteria that could be used as a baseline to examine the implemented security controls. A comprehensive security control checklist has been developed based on the available literature in this area. The security controls checklist is a general and comprehensive medium, which could be used by any organization to conduct a self-evaluation of its information security controls. The suggested security controls checklist is presented in the appendixes of this textbook.

4-8-8. Examine the Adequacy of the Implemented Information Security Controls

The final step in evaluating the information security control is to compare the existing implemented security controls against the entire elements of the security controls checklist to investigate the adequacy of security controls in place. The results of that comparison would identify the weaknesses of security controls in banks. Accordingly, actions could be taken to correct and strengthen these information security controls in the organization.

2021/2022 2021/2022 2021/2022

4-9. Summary

In this chapter, evidence regarding the need as well as the importance of evaluating the security of information has been covered. The alternative approaches for evaluating information security used and implemented in previous literature were

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

presented. Moreover, the requirements for selecting appropriate security countermeasures as well as implementing an effective evaluation security technique have been discussed. Finally, the main steps of the approach adopted for evaluating the security of information in the organization have been highlighted and discussed.

As information becomes more readily available to all types and sizes of businesses, the need to understand and employ adequate systems security becomes an issue no business owner can ignore (Henry, 1997). The current textbook is written to enhance a body of knowledge concerned with the security of information and it tacks a substantial step in that direction.

Through theoretical conceptualizations of information and systems security, an integrated theoretical framework of information, which includes the security objectives, threats and controls, has been developed. This book has focused on evaluating the security of information, rather than of the IT products and accounting software: therefore, it contributes to filling the vacuum in this research area. This book has provided invaluable information regarding the information security policies, the significant perceived information security threats and expected inadequacies of implemented information security controls in the organization. Accordingly some actions should be taken to strengthen the security controls. From a practical standpoint, managers and practitioners alike stand to gain from the findings of this study. The textbook offers students, managers and practitioners a roadmap to champion IT development for business success.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Chapter Five
Information Security Governance

5.1 Introduction

Many organizations nowadays are facing a global revolution in governance which might directly affect their information management practices. Information security has become an integral part of daily life, and organizations need to ensure that their information is adequately secured. It is argued that the assurance of protecting information as a valuable asset should not be left to the chief information officer (CIO) of an organization, but should be treated as a governance issue. Relevant aspects of corporate information security governance (ISG) include accountability to shareholders, compliance with legal requirements, setting of well-planned security policies, spearheading security awareness and education, defining roles and responsibilities within the organizational structure, contingency planning and instituting best practice standards (Mears & Von Solms, 2005).

Information and the systems that handle it are critical to the operation of virtually all organizations. Access to reliable information has become an indispensable component of conducting business; indeed, in a growing number of organizations, information is the business.

Organizations continue to witness information-related crime and vandalism becoming the choice of a growing global criminal element. Existing institutions burdened by countless conflicting jurisdictions and inadequate resources have not been successful in reducing the amount or impact of these activities.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571
سليمان طارق شبل ابراهيم السعدى

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Therefore, a large portion of the task of protecting critical information resources falls squarely on the shoulders of executives and boards of directors.

Until recently, the focus of security had been on protecting the IT systems that process and store the vast majority of information, rather than on the information itself. However, this approach is too narrow to accomplish the level of integration, process assurance and overall protection that is now required.

As organizations strive to remain competitive in the global economy, they respond to constant pressures to cut costs through automation, which often requires deploying more information systems. Whilst managers become ever more dependent on these systems, the systems have become vulnerable to a widening array of risks that can threaten the existence of the enterprise. This combination is forcing management to face difficult decisions about how to effectively address information security. This is in addition to scores of new and existing laws and regulations that demand compliance and higher levels of accountability.

2021/2022 2021/2022 2021/2022

Information security should not be regarded as a technical issue, but a business and governance challenge that involves adequate risk management, reporting, and accountability. Therefore, information security must be addressed at the highest levels of the organization and not regarded as a technical specialty relegated to the information technology (IT) department. Effective information security requires the active involvement of executives to assess emerging threats and the organization’s response to them.

According to the IT Governance Institute (2006), organizations should consider the impact on reputation and enterprise value resulting from information security failures.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

While executive management has the responsibility to consider and respond to information security issues, boards of directors will increasingly be expected to make information security an intrinsic part of the enterprise's governance efforts, aligned with their IT governance focus and integrated with processes they have in place to govern other critical functions. The IT Governance Institute (2006) also argued that the benefits of implementing good ISG practices are not just a reduction in risk or a reduction in the impact should something go wrong. Good security can improve reputation, confidence, and trust from others with whom business is conducted, and can even improve efficiency by avoiding wasted time and effort recovering from a security incident.

Mears and Von Solms (2005) highlighted the importance of ISG for organizations, and the real need to be taken seriously not only by the IT department, but also by the board of directors and senior management, to ensure that the information asset is adequately protected. A definite responsibility and reporting structure needs to exist between the different levels of authority within the organization. Accordingly, holistic ISG should be addressed and implemented.

It is also argued that effective ISG cannot be established overnight and it requires continuous improvement. The Corporate Governance Task Force has developed some recommendations and tools that could provide a strong start to organizations seeking to improve their ISG. The Task Force calls on organizations to make ISG a priority and to use these tools to launch internal ISG processes and generate awareness of the need to treat information security as a governance issue (National Cyber Security Summit Task Force, 2004). The IT Governance

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Institute (2006) also confirmed that the requirement to improve ISG will continue into the foreseeable future. While spending on security has grown in response to increasing risk, the failure of security to deal with identity theft, fraud, wholesale loss of customer personal information and a host of other criminal and destructive uses of information systems continues unabated. Therefore, information security must be addressed as a governance level concern.

5.2 Information Security Governance: An Overview

Information security governance is an important component of the IT governance and an integral part of the enterprise governance. The International Federation of Accountants (IFAC), IT Governance Institute, and the Information Systems Audit and Control Association (ISACA) have defined the enterprise governance as "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly" (IFAC, 2004; and Allen & Westby, 2007). According to the IT Governance Institute (2003) IT governance, which could be regarded as an integral part of enterprise governance consisting of the leadership and organizational structures and processes, aims to ensure that the organization's IT sustains and extends the organization's strategies and objectives (ITGI, 2003). Robles et al., (2008) also confirmed that Information Technology Governance is "a subset discipline of corporate governance focused on information

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

technology (IT) systems and their performance and risk management”.

ISG could be regarded as implementing the governance concepts and principles on information security issues. ISG consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that information is never compromised. Therefore, the main purpose of ISG is to protect against risks that can impact the confidentiality, integrity and availability of the company’s electronic assets (data, information, software, hardware, people etc) and should be well-maintained all the times (Kritzinger & Von Solms, 2006; Von Solms & Von Solms 2006 a).

Moulton and Coles (2003) defined ISG as: “the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems.” While the IT Governance Institute (2006) defined ISG as: “a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program.”

ISG is also defined as the organization’s management responsibilities and practices that provide strategic vision, ensure objectives are achieved, manage risks appropriately, use organizational resources responsibly, and monitor the success or failure of the information security programs (IBM Global Business Services, 2006). IBM (2006) also confirmed that ISG

2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

relates to the protection of valuable assets against loss, misuse, disclosure, or damage. In this context, valuable assets are the information recorded on, processed by, stored in, shared by, transmitted from, or retrieved from an electronic medium. The information must be protected against harm from threats leading to different types of impacts such as loss, inaccessibility, alteration, or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage.

Based on the above deliberation, it can be concluded that ISG is an important integrant component of information technology governance and a subset of corporate governance. ISG can be defined as the set of responsibilities and practices exercised by the board of directors and executive management with the goal of providing information security strategic direction, ensuring that information security objectives are achieved, ascertaining that information security risks are managed appropriately, and verifying that the information security resources are used responsibly. ISG aims to establish and maintain the control environment to preserve confidentiality, integrity and availability of information and its supporting processes and systems, and to protect information against various information security threats. The next section briefly introduces the importance and expected benefits of ISG.

2021/2022 2021/2022 2021/2022

5.3 Benefits of Information Security Governance

Implementing an effective ISG can generate many direct and indirect benefits to an organization. The IT Governance Institute (2006) stated that protecting critical information must constitute one of the major risks to be considered in management strategies and should also be recognized as a crucial contributor

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

to business success. Robles et al., (2008) also confirmed that ISG has gained great attention due to failures of big companies. While, the IT Governance Institute, (2006) argued that organizations might survive the loss of other assets, including facilities, equipment and people, few could continue with the loss of their critical information (i.e., accounting and financial reporting information and operations and process knowledge and information) or customer data. The risks, benefits and opportunities these resources present have made ISG a critical facet of the overall governance.

It is also argued that as organizational assets continue to become more intangible, the requirements of paying due care in protecting such valuable information assets requires greater attention and resources. Additionally, effective ISG becomes a necessity in order to adequately address numerous legal and regulatory requirements. Organizations that fail to address information security issues will find themselves at a competitive disadvantage and fall victim to ever more technologically sophisticated criminals. Organizations will find share value increasingly tied to governance (good and bad) as the market becomes more knowledgeable of its relevance (Posthumus & Von Solms, 2004; IT Governance Institute, 2006).

Organizations should consider that failing to provide adequate protection of critical information assets is becoming more visible and less acceptable. According to the IT Governance Institute, (2006) implementing effective ISG would generate many significant benefits to an organization, including:

- An increase in share value for organizations that practice good governance;

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Increased predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable levels;
- Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care;
- The structure and framework to optimize allocation of limited security resources;
- Assurance of effective information security policy and policy compliance;
- A firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information;
- A level of assurance that critical decisions are not based on faulty information,
- Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response.

2021/2022 2021/2022 2021/2022

Moreover, ISG could add significant value to an organization by improving trust in customer relationships, protecting the organization’s reputation, decreasing likelihood of violations of privacy, providing greater confidence when interacting with trading partners, enabling new and better ways to process electronic transactions, and reducing operational costs by providing predictable outcomes, while mitigating risk factors that may interrupt the process (IT Governance Institute, 2006).

ISG would also help in ensuring that organizations are complying with all applicable laws, regulations and codes of practice. According to Swindle and Conner (2004) ensuring compliance with laws and regulations is the responsibility of

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

executive management and it should be in their best interest to fulfill this responsibility as failure in this regard could result in stringent legal action against them.

Moulton and Coles (2003) also confirmed that new legal requirements have significantly changed enterprise management's governance responsibilities and are driving changes to the ways that information security is approached. Therefore, a governance approach to information security could provide a better framework to meet new requirements and to manage risks within the enterprise. It could help to communicate more effectively within the enterprise as well as with external parties, including regulators. Furthermore, it could help to further the security profession by clearly establishing governance and protection roles and responsibilities.

Entrust (2004) stated that the benefits derived by organizations that implement the ISG framework go beyond facilitating compliance with applicable legislative, regulatory and contractual requirements. ISG and its associated information security program would result in tangible business benefits, including:

2021/2022 2021/2022 2021/2022

- Improved internal processes and controls: Authentication, authorization and auditability of the people, devices and applications on the network improves efficiency and effectiveness of business processes.
- Potential for lower audit and insurance costs: Better governance and the ability to demonstrate an auditable, complete IS.
- Market differentiation through a continuous improvement process: Industry first resisted quality-improvement processes as added cost, but soon evolved to embrace it as a method for

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

improving productivity and customer loyalty. Ultimately, quality became a market differentiator. Over time, an ISG program may also provide results that help determine a market leader.

- Self-governance as a better alternative than regulation: Implementation of an industry-led solution based on open standards and best practices will help mitigate the requirement for new governmental regulation. Should new legislation emerge, organizations that have invested in an ISG program are likely to benefit.

According to The IT Governance Institute (2006) ISG would help an organization in reducing the adverse impacts to an acceptable level of risk, and in protecting information assets against the risk of loss, operational discontinuity, misuse, unauthorized disclosure, inaccessibility and damage. It could also protect against the ever-increasing potential for civil or legal liability that organizations might face as a result of information inaccuracy and loss, or the absence of due care in its protection. Huang et al. (2006) also confirmed that in consideration of the ISG's importance, many outstanding institutes published information security guidelines and standards for protecting the confidentiality, integrity and accessibility of information. If firms follow the guidelines and standards to set up their security policy, they could own a tighter and more complete IT environment. That is, firms could safeguard their business value and benefit from IT according to well-developed information security management.

2021/2022 2021/2022 2021/2022

The IT Governance Institute (2006) also stated ISG can deliver a value to the organization, and can contribute to enhance and sustain stakeholders' value. Swindle and Conner (2004)

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

argued that if administered effectively, ISG would be of value to organizations in ways that exceed the mere observance of lawful conduct. Furthermore, ISG would be useful as a mechanism to increase overall productivity and lower costs in an organization and to produce value for all of its relevant stakeholders, including governments and other legislative authorities.

It is argued that, in this era of increased cyber attacks and information security breaches, it is essential that all organizations give information security the focus it requires. Addressing these cyber and information security concerns, the private sector will not only strengthen its own future security, but the nation's homeland security as well. The task force calls on organizations to make ISG a priority and to use the tools described in this report to develop effective ISG programs (National Cyber Security Summit Task Force, 2004).

The benefits of good information security are not just a reduction in risk or a reduction in the impact should something go wrong. Good security can improve reputation, confidence and trust from others with whom business is conducted, and can even improve efficiency by avoiding wasted time and effort recovering from a security incident.

Accordingly, implementing adequate and effective ISG could protect information recorded on, processed by, stored in, shared by, transmitted or retrieved from electronic media from loss, inaccessibility, alteration, or wrongful disclosure. It could protect information from threats of errors and omissions, fraud, accidents, and intentional damage, and achieve regulatory compliance and mandated best practices (IBM Global Business Services, 2006). The next section introduces a proposed integrated framework for ISG.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

5.4 Information Security Governance Framework

ISG has become a major issue of concern to both the private and public sectors, including governments around the world. Therefore, effective governance frameworks should exist and be effectively implemented (Corporate Governance Task Force, 2004). Entrust (2004) confirmed that the acceptance and implementation of an ISG framework is an important action for securing business information through the protection of information systems, acting in accordance with legislation, as well as improving the efficiency of business operations, amongst other things. ISG enables an organization to effectively fulfill all the internal and external requirements in terms of protecting business information assets and, therefore, covers the full scope of risks faced by an organization in this regard. These security requirements could be viewed as information risk directives that would advise executive management on what should be done in order to govern and manage information security properly. Consequently these requirements would ultimately help to guide the construction and implementation of an effective information security strategy through corporate governance. ISG would also enhance the internal security practices and controls, and the promotion of self-governance as a preference over increased legislation by governments and local authorities (Entrust, 2004; Swindle & Conner, 2004; and Posthumus & Von Solms, 2004).

ISG is a responsibility of the board of directors and senior executives, and it should be treated as an integral part of enterprise governance and be aligned with the IT governance framework. However, in order to exercise effective enterprise and information security governance, boards of directors and senior executives should have a clear understanding of what to

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

expect from their enterprise's information security program. They need to know how to direct the implementation of an information security program, how to evaluate their own status with regard to an existing information security program, and how to decide the strategy and objectives of an effective information security program (IT Governance Institute, 2006). Da Veiga and Ellof (2007) argued that in order to inculcate an acceptable level of information security culture, the organization must govern information security effectively by implementing all the required information security components.

The current study introduces an integrated ISG framework (Figure 1) that would enable organizations to better understand, analyze, implement and evaluate ISG practices to achieve businesses success. The proposed ISG framework has been developed based on the ISG conceptual framework proposed by IT Governance Institute (2006) and other ISG models and frameworks available in the literature (e.g., Hong et al., 2003; Moulton and Coles, 2003; Posthumus & Von Solms, 2004; Swindle and Conner, 2004; Saint - Gemain, 2005; Eloff and Eloff, 2005; Von Solms and Von Solms, 2006a and b; Luthy and Forcht, 2006; Huang et al., 2006; Da Veiga and Ellof, 2007; Allen & Westby, 2007; The Wolcott Group, 2007; Robles et al., 2008; and Abu-Musa, 2009a).

The information security framework generates a set of activities that supports fulfillment of achieving information security objectives. The framework also prescribed the necessary human resources needed for developing and implementing an information security strategy to be aligned with an organization's strategy and objectives. However, in order to achieve such alignment, information technology strategy should be in harmony

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

with the business strategy. It is also argued that both the business and information technology strategies provide important inputs to risk management and information security strategy development. Other inputs to the information security strategy include the business processes and risk assessments. Regulatory requirements should be also considered in developing the information security strategy.

According to Moulton and Coles (2003 implementing an effective ISG program should start with identifying the full scope and context of the real risks that the enterprise is up against, and continue with the process for managing those risks. Therefore, absolute clarity of primary and secondary risk ownership and management responsibilities are fundamental requirements. While Da Veiga and Ellot (2007) argue that the risks faced by the organization can only be addressed when a governance framework for information security is in place and equipped with specific controls that executives could use to direct employees' behavior. The governance framework should enable organizations to make provisions for human behavior in their information security initiatives, in order to cultivate an acceptable level of information security culture.

The prescribed information security strategy (Figure 1) should provide the basis for the information security action plan which is comprised of one or more security programs that should be implemented to achieve the stated security objectives. However, the information security strategy and action plans should contain provisions for monitoring as well as defined metrics to determine the level of success. Evaluating the performance of the implemented information security programs would provide a feedback to the chief information security

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

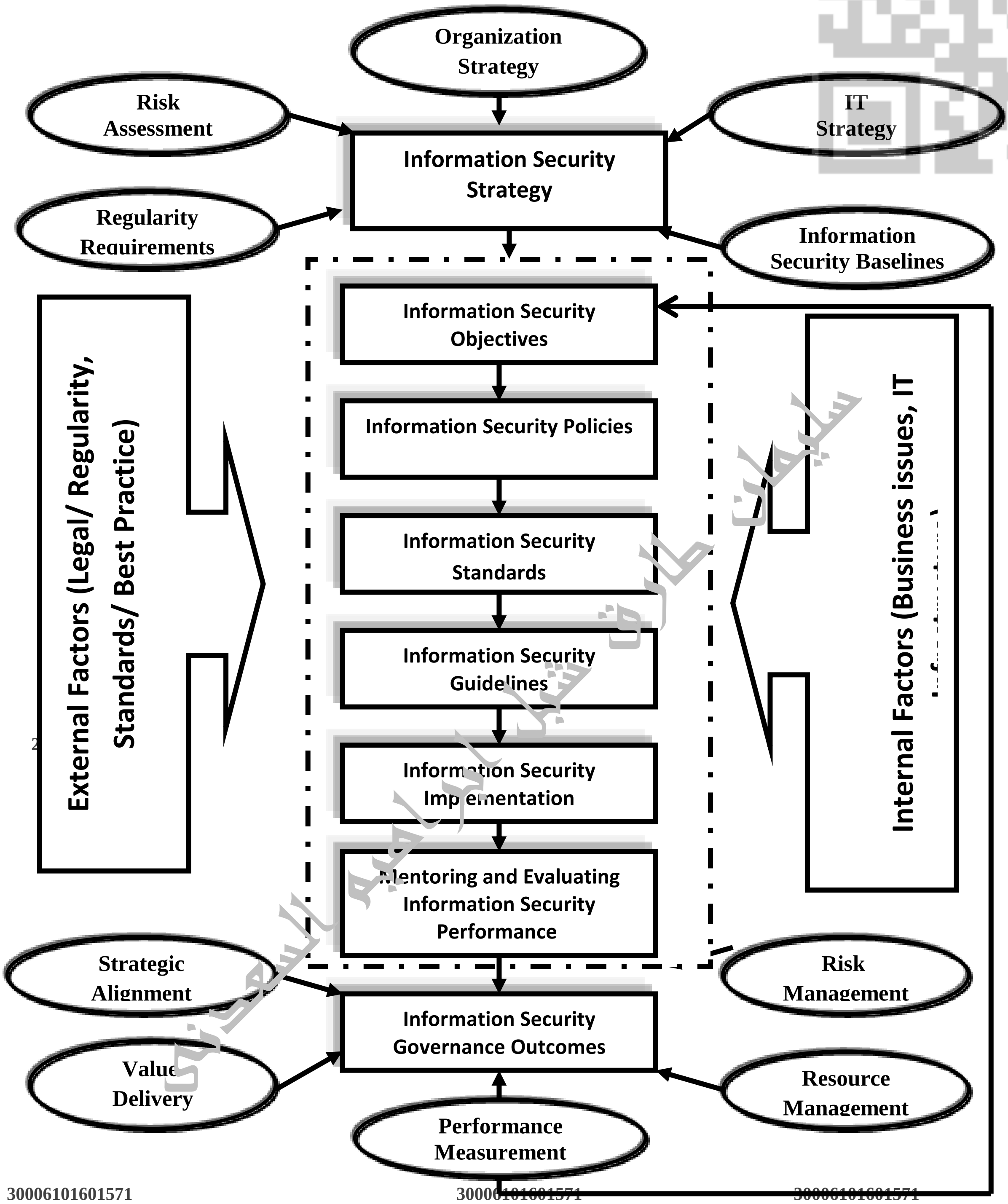
officer and steering committee to take some corrective actions, and to ensure that security initiatives are on track to achieve the defined objectives.

The objective of information security is protecting the interests of those relying on information and the information systems and communications that deliver the information from harm resulting from failures of availability, confidentiality and integrity (IFAC, 1998). The information security objectives would be achieved when information systems are available and usable when required (availability), information is disclosed only to those who have a right to know them (confidentiality), data and information are protected against unauthorized modification (integrity), and business transactions as well as information exchanges between enterprise locations or with external trading partners can be trusted (*authenticity and non-repudiation*)

Information security should not only be treated as a technical issue, but as a business and governance challenge that involves risk management, reporting, and accountability. Therefore, effective security requires an active engagement of executive management to assess emerging security threats and provide strong cyber security leadership to achieve the desired corporate governance objectives. Corporate governance consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed. ISG is a subset of an organizations' overall governance program. Risk management, reporting, and accountability are central features of these policies and internal controls (National Cyber Security Summit Task Force; 2004).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg


Organization Strategy
Risk Assessment
IT Strategy
Information Security Strategy
Regularity Requirements
Information Security Baselines
Information Security Objectives
Information Security Policies
Information Security Standards
Information Security Guidelines
Information Security Implementation
Mentoring and Evaluating Information Security Performance
External Factors (Legal/ Regularity, Standards/ Best Practice)
Internal Factors (Business issues, IT
Strategic Alignment
Risk Management
Information Security Governance Outcomes
Value Delivery
Resource Management
Performance Measurement

سليمان طارق شبل ابراهيم السعدني
30006101601571 30006101601571 30006101601571

(Figure 1: Information Security Governance Framework)

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

According to the IBM Global Business Services (2006), good ISG should have a comprehensive security program which should be linked to IT and organizational objectives; an effective security organization and structure; security policies that address strategy, control and regulation; security standards, policies and procedures; monitoring processes to ensure compliance; continual evaluation processes and updates of standards, policies and procedures; and an information security risk management methodology.

The Corporate Governance Task Force (2004) confirmed that developing and promoting a coherent governance framework would drive implementation of effective information security programs in organizations

It also argued that by implementing effective ISG framework and assessment tools, organizations could integrate information security into their corporate governance programs, thereby creating a safer business community not only for themselves, but also for those enterprises that interact with them.

It is also well recognized that the main objective of ISG is to protect the interests of those relying on information and the systems and communications that deliver the information from harm resulting from failures of availability, confidentiality and integrity. Information security helps organizations to mitigate the various risks to such information through the application of a suitable range of security controls. However, according to the IT Governance Institute (2006) the relative priority and significance of availability, confidentiality, integrity, authenticity and non-repudiation could vary according to the data within the information system and the business context in which they are used. For example, integrity is especially important relative to

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

management information due to the impact that information has on critical strategy related decisions and financial reporting. Confidentiality may be the most critical today as it relates to personal, financial or medical information, or the protection of trade secrets and other forms of intellectual property.

Based on the information resources needed and the level of protection required, information security baselines could be developed and implemented in an organization. Information security baselines are the minimum acceptable security that should be provided to protect information resources. Baselines can vary depending on the sensitivity and criticality of the asset. Baselines can be expressed as technical, procedural and personnel standards throughout the enterprise (IT Governance Institute, 2006). The National Association of Corporate Directors (NACD) (2001) also recognized the importance of information security and recommended four essential practices to enhance the ISG. These four information security practices are: to place information security on the board's agenda; to identify information security leaders, and to hold them accountable and ensure support for them; to ensure the effectiveness of the corporation's information security policy through review and approval; and to assign information security to a key committee and ensure adequate support for that committee.

However, in order to achieve effective ISG, management should establish and maintain an integrated and coherent ISG framework to guide the development, implementation, maintenance and evaluation of ISG practices in an organization (Figure 1). According to the IT Governance Institute (2006) a comprehensive ISG framework should consider and incorporate the following factors:

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- An information security risk management methodology.
- A comprehensive security strategy explicitly linked with business and IT objectives.
- An effective security organizational structure.
- A security strategy that talks about the value of information protected and delivered.
- Security policies that address each aspect of strategy, control and regulation.
- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy.
- Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk.
- A process to ensure continued evaluation and updating of security policies, standards, procedures and risks.

However, in order to provide effective governance, a set of enterprise standards for each policy must be developed to define the boundaries for acceptable processes and procedures along with assigned roles and responsibilities (Figure 1). Moreover, some organizations might also have special security requirements or objectives resulting from partnerships or customer contractual arrangements. Therefore, it is critical that management ensure that these considerations are tightly aligned with enterprise policies and procedures, and adequate resources are allocated to support the overall enterprise strategy. The IT Governance Institute (2006) stated that along with security policies, a comprehensive information security program includes:

2021/2022 2021/2022 2021/2022

- Development and maintenance of security policies.
- Assignment of roles, responsibilities, authority and accountability.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Development and maintenance of a security and control framework that consists of standards, measures, practices and procedures.
- Periodic assessments of risks and business impact analyses.
- Classification and assignment of ownership of information assets.
- Adequate, effective and tested controls for people, processes and technology.
- Integration of security into all organizational processes.
- Processes to monitor security elements.
- Information security incident management.
- Effective identity and access management processes for users and suppliers of information.
- Meaningful monitoring and metrics of security performance.
- Education of all users, managers and board members regarding information security requirements.
- Annual information security evaluations and performance reports to the board of directors.
- Plans for remedial action to address information security deficiencies.
- Training in the operation of security processes.
- Development and testing of plans for continuing the business in case of interruption or disaster.

According to the National Cyber Security Summit Task Force (2004) the board of directors / trustees or similar governance body should provide strategic oversight regarding information security, including: understanding the criticality of information and information security to the organization; reviewing investment in information security for alignment with

2021/2022 2021/2022 2021/2022
سليمان طارق شعلان ابراهيم السعدني
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

the organization strategy and risk profile; endorsing the development and implementation of a comprehensive information security program; and requiring regular reports from management on the program's adequacy and effectiveness.

The ISG framework provides organizations with an understanding of the requirements for a holistic plan for information security. It also combines technical, procedural, and people-orientated components for the purpose of cultivating an appropriate level of information security culture and minimizing risks posed to information assets (Da Veiga & Eliof, 2007; and Allen & Westby, 2007). However, ISG requires senior management commitment, a security-aware culture, promotion of good security practices and compliance with policy. The IT Governance Institute (2006) argued that it is easier to buy an information security solution than to change a culture, but even the most secured information system will not achieve a significant degree of information security if used by ill-informed, untrained, careless or indifferent personnel.

In order to ensure that all relevant elements of security are addressed in an organizational security strategy, several security standards have been developed to provide guidance and ensure comprehensiveness. A number of best practice frameworks exist to help organizations assess their security risks, implement appropriate security controls, and comply with governance requirements as well as privacy and information security regulations. Some of the most commonly used standards include Control Objectives for Information and related Technology (COBIT), ISO 17799, and others such as FIPS Publication 200 and NIST 800-53 in the US (Saint - Gemain, 2005; and IT Governance Institute, 2006).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

A comprehensive security program implements the protection of information assets through a layered series of technological and non technological safeguards and controls (i.e., safety and environmental security measures, perimeter and physical security, background checks, access control security measures, user identifiers, passwords, IT technical measures and manual and automated procedures). These safeguards and controls are necessary and should address threats and vulnerabilities in a manner that reduces their potential impact to a defined, acceptable level (IT Governance Institute, 2005).

It is also argued that different organizations have diverse needs and adapt varied approaches of ISG. Accordingly, the Task Force has identified a core set of principles to help guide organizations' efforts in this regard. It is advised that by reviewing these principles internally organizations can develop an information security program that is best tailored to their needs:

2021/2022 2021/2022 2021/2022

- CEOs should have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to the board of directors.
- Organizations should conduct periodic risk assessments of information assets as part of a risk management program.
- Organizations should implement policies and procedures based on risk assessments to secure information assets.
- Organizations should establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.
- Organizations should develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Organizations should treat information security as an integral part of the system lifecycle.
- Organizations should provide information security awareness training and education to personnel.
- Organizations should conduct periodic testing and evaluation of the effectiveness of information security policies and procedures.
- Organizations should create and execute a plan for remedial action to address any information security deficiencies.
- Organizations should develop and implement incident response procedures.
- Organizations should establish plans, procedures and tests to provide continuity of operations.
- Organizations should use security best practices guidance, such as ISO 17799, to measure information security performance (National Cyber Security Summit Task Force, 2004).

2021/2022 2021/2022 2021/2022

5.5 Information Security Governance Outcomes

ISG consists of the leadership, organizational structures and processes that safeguard information. The five basic ISG outcomes include:

1. Strategic alignment of information security with business strategy to support organizational objectives.
2. Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level.
3. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4. Performance measurement by measuring, monitoring and reporting ISG metrics to ensure that organizational objectives are achieved.
5. Value delivery by optimizing information security investments in support of organizational objectives (IT Governance Institute, 2006). The five ISG outcomes are briefly discussed below:

5.5.1. Strategic Alignment

It is often difficult to achieve the goal of strategic alignment of information security in support of organizational objectives. Security requirements should be driven by the enterprise requirements considering the following goals:

- Ensure transparency and understanding of IT security costs, benefits, strategy, policies and service levels.
- Develop a common and comprehensive set of IT security policies.
- Communicate the IT strategy, policies and control framework.
- Enforce IT security policies.
- Define security incidents in business impact terms.
- Ensure a security solutions fit for enterprise processes.
- Establish clarity on the business impact of risks to IT objectives and resources.
- Establish an IT continuity plan that supports business continuity plans.
- Ensure Investment in information security aligned with the enterprise strategy and agreed-upon risk profile (Williams, 2001, and IT Governance Institute, 2006).

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

5.5.2. Risk Management

A key goal of information security is to reduce the adverse impacts on the organization to an acceptable level of risk. Therefore, a key measure is the adverse impact of information security incidents experienced by the organization. An effective security program will show a trend of impact reduction. Quantitative measures can include trend analysis of impacts over time However, in order to manage and mitigate information security risks and reduce its potential impacts on information assets to an acceptable level, an organization should consider the following goals:

- Account for and protect all IT assets.
- Establish and reduce the likelihood and impact of IT security risks.
- Perform regular risk assessments with senior managers and key staff.
- Permit access to critical and sensitive data only to authorized users.
- Ensure critical and confidential information is withheld from those who should not have access to it.
- Identify, monitor and report security vulnerabilities and incidents.
- Develop IT continuity plans that can be executed and are tested and maintained (IT Governance Institute, 2006).

2021/2022 2021/2022 2021/2022

5.5.3. Resource Management

According IT Governance Institute (2006) Information security knowledge and infrastructure should be used efficiently

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

and effectively. Effective information resource management could be achieved through considering the following goals:

- Maintain the integrity of information and processing infrastructure.
- Account for and protect all IT assets.
- Ensure that IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.
- Ensure proper use and performance of applications and technology solutions.

5.5.4. Performance Measurement

Measuring, monitoring and reporting on information security processes ensure that organizational objectives are achieved. An organization could use the following measures to evaluate the ISG performance:

- Number of incidents damaging reputation with the public.
- Number of systems where security requirements are not met.
- Time to grant, change and remove access privileges.
- Number and type of suspected and actual access violations.
- Number and type of malicious code prevented.
- Number and type of security incidents.
- Number and type of obsolete accounts.
- Number of unauthorized IP addresses, ports and traffic types denied.
- Number of access rights authorized, revoked, reset or changed (IT Governance Institute, 2006).

سليمان طارق شعبان ابراهيم السعدني
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

5.5.5. Value Delivery

Security investments should be optimized to support organizational objectives. Security activities consume resources, and optimal investment levels occurs when strategic goals for security are achieved and an acceptable risk posture is attained by the organization at the lowest possible cost. The following information security goals should be considered:

- Ensure automated business transactions and information exchanges can be trusted.
- Make sure that IT services are available as required.
- Minimize the probability of IT service interruption.
- Minimize the impact of security vulnerabilities and incidents.
- Ensure minimum business impact in the event of an IT service disruption or change.
- Establish cost-effective action plans for critical IT risks (IT Governance Institute, 2006)

2021/2022 2021/2022 2021/2022

Self- Assessment Information Security Governance Practices	Yes	No
1. Does the organization recognize the value and importance of information security and set the appropriate tone at the top to foster a security conscious environment?		
2. Does the organization have an information security strategy?		
3. Has management issued a policy statement on information security?		
4. If it has, is the policy statement subject to review, update and approval?		
5. Has someone been appointed to be responsible for developing, implementing and managing the information security program, and is he/she held accountable?		

سليمان طارق شبل ابراهيم السعدى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Self- Assessment Information Security Governance Practices	Yes	No
6. Are information security roles and responsibilities clearly defined and communicated?		
7. Is there an effective and tested process to deal with information security incidents/emergencies?		
8. Does the risk assessment consider what information assets are subject to laws and regulations?		
9. Does risk assessment result in adequate procedures to assure compliance with these laws and regulations?		
10. Does the board understand the organization's potential liabilities in the event of regulatory non-compliance?		
11. Does the board understand the potential liability in the event sensitive information is compromised?		
12. Has the organization suffered a major security incident?		
13. Has the cost of the incident to the organization been determined?		
14. Is there a business continuity/disaster recovery plan in place?		
15. Has business continuity/disaster recovery plan been tested under live circumstances?		
16. Is business continuity/disaster recovery plan tested regularly?		
17. Does the risk assessment consider whether the entity can continue to operate if critical information is unavailable, compromised or lost?		
18. Does risk assessment cover the consequences of a security incident in terms of lost revenues, lost customers and investor confidence?		
19. Does risk assessment determine what the consequences would be if the infrastructure became inoperable?		
20. Is there a CISO or officer with sufficient authority and resources specifically charged with managing information security in the organization?		

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Self- Assessment Information Security Governance Practices	Yes	No
21. Does the CEO request an information security evaluation?		
22. Are the results of information security evaluation reviewed with staff and reported to the board of directors?		
23. Does the audit committee clearly understand its role in information security and how it will set direction with management and auditors?		
24. Are there appropriate training and awareness programs to ensure that personnel are aware of their security responsibilities?		
25. Is there an information asset classification process in place to ensure that critical assets are adequately protected?		

5.6. Evaluating the status of Information Security Governance

Boards of directors and executive management can use an information security governance maturity model to establish rankings for maturity within an organization. When IT risk is referenced, it should be considered within the context of information security. This model21 can be progressively applied as a method for:

- Self-assessment against the scales, deciding where the organization is.
- Using the results of the self-assessment to set targets for future development, based on where the organization wants to be on the scale, which is not necessarily at the top level
- Planning projects to reach the targets, based on an analysis of the gaps between those targets and the present status

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- Prioritizing project work based on project classification and an analysis of its beneficial impact against its cost

Maturity Level Description

0 Non-existent

- Risk assessment for processes and business decisions does not occur. The organization does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services
- The organization does not recognize the need for information security.
- Responsibilities and accountabilities are not assigned for ensuring security.
- Measures supporting the management of information security are not implemented. There is no information security reporting and no response process to information security breaches. There is a complete lack of a recognizable system security administration process.
- There is no understanding of the risks, vulnerabilities and threats to IT operations or the impact of loss of IT services to the business. Service continuity is not considered as needing management attention.

1 Initial/*Ad Hoc*

- The organization considers IT risks in an *ad hoc* manner, without following defined processes or policies. Informal assessments of project risk take place as determined by each project.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

- The organization recognizes the need for information security, but security awareness depends on the individual. Information security is addressed on a reactive basis and is not measured. Information security breaches invoke finger-pointing responses if detected, because responsibilities are unclear. Responses to information security breaches are unpredictable.
- Responsibilities for continuous service are informal, with limited authority.
- Management is becoming aware of the risks related to and the need for continuous service.

2 Repeatable but Intuitive

- There is an emerging understanding that IT risks are important and need to be considered. An approach to risk assessment exists, but the process is still immature and developing.
- Responsibilities and accountabilities for information security are assigned to an information security co-coordinator with no management authority. Security awareness is fragmented and limited. Information security information is generated, but not analyzed. Security tends to respond reactively to information security incidents and by adopting third-party offerings, without addressing the specific needs of the organization. Security policies are being developed, but inadequate skills and tools are still being used. Information security reporting is incomplete, misleading or not pertinent.
- Responsibility for continuous service is assigned. The approaches to continuous service are fragmented.

سليمان طارق شبل ابراهيم السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Reporting on system availability is incomplete and does not take business impact into account.

3 Defined Process

- An organization wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.
- Security awareness exists and is promoted by management. Security awareness briefings have been standardized and formalized. Information security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for information security are assigned, but are not consistently enforced. An information security plan exists, driving risk analysis and security solutions. Information security reporting is IT-focused, rather than business-focused. *Ad hoc* intrusion testing is performed.
- Management communicates consistently the need for continuous service.
- High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعيدى

4 Managed and Measurable

- The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior-level responsibility. Senior management and IT management have determined the levels

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

of risk that the organization will tolerate and have standard measures for risk/return ratios.

- Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorization are standardized. Security certification of staff is established. Intrusion testing is a standard and formalized process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilized. Information security processes are co-ordinated with the overall organization security function. Information security reporting is linked to business objectives.
- Responsibilities and standards for continuous service are enforced. System redundancy practices, including use of high-availability components, are consistently deployed.

2021/2022 2021/2022 2021/2022

5 Optimized

- Risk management has developed to the stage that a structured, organization wide process is enforced, followed regularly and managed well.
- Information security is a joint responsibility of business and IT management and is integrated with enterprise security business objectives. Information security requirements are clearly defined, optimized and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. Information security reporting provides early warning of changing and emerging risk, using

سليمان طارق شبل ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

automated active monitoring approaches for critical systems. Incidents are promptly addressed, with formalized incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk are the basis for continuous improvements. Security processes and technologies are integrated organization wide.

- Continuous service plans and business continuity plans are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers.

5.7. Summary

2021/2022 2021/2022 2021/2022

A key goal of information security is to reduce adverse impacts on the organization to an acceptable level of risk. Information security protects information assets against the risk of loss, operational discontinuity, misuse, unauthorized disclosure, inaccessibility and damage. It also protects against the ever-increasing potential for civil or legal liability that organizations face as a result of information inaccuracy and loss, or the absence of due care in its protection.

Information security covers all information processes, physical and electronic, regardless whether they involve people and technology or relationships with trading partners, customers and third parties. Information security addresses information protection, confidentiality, availability and integrity throughout

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

the life cycle of the information and its use within the organization.

Given the dramatic rise of information crimes, including phishing and other cyberattacks, few today would contend that improved security is not a requirement. With new worms/malware and the increase in reported losses of confidential customer information and intellectual property theft, senior management is left with little choice but to address these issues. Information security requires a balance between sound management and applied technology. With the widespread use of networks, individuals and organizations are concerned with other risks pertaining to privacy of personal information and the organization's need to protect the confidentiality of information, whilst encouraging electronic business.

The systems and processes that handle information have become pervasive throughout enterprises. Organizations may survive the loss of other assets, including facilities, equipment and people, but few can continue with the loss of their critical information (i.e., accounting and financial reporting information and operations and process knowledge and information) or customer data. The risks, benefits and opportunities these resources present have made information security governance a critical facet of overall governance.

Information security should be an integral part of enterprise governance, aligned with IT governance and integrated into strategy, concept, design, implementation and operation. Protecting critical information must constitute one of the major risks to be considered in management strategies and should also be recognized as a crucial contributor to success.

سليمان طارق شبل ابراهيم السعيدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Questions of Chapter Five

Please select the correct answer of each of the following questions:

1. How many principles are there in the 2013 updated COSO - Internal Control Framework?
   a. 5
   b. 8
   c. 17
   d. 21

2. Why was the original 1992 COSO - Integrated Control framework updated in 2013?
   a. Congress required COSO to modernize.
   b. U.S. stock exchanges required more disclosure.
   c. to more effectively address technological advancements
   d. to comply with International accounting standards

2021/2022 2021/2022 2021/2022

3. The COBIT5 framework primarily relates to

   a. best practices and effective governance and management of private companies.
   b. best practices and effective governance and management of public companies.
   c. best practices and effective governance and management of information technology.
   d. best practices and effective governance and management of organizational assets.

سليمان طارق شبل ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

4. Which internal control framework is widely accepted as the authority on internal controls?
   a. COBIT
   b. COSO Integrated Control
   c. COSO Enterprise Risk Management
   d. Sarbanes-Oxley Control Framework

5. Identify the statement below that is *not* true of the 2013 COSO Internal Control updated framework.
   a. It more efficiently deals with control implementation and documentation issues.
   b. It more effectively deals with control implementation and documentation issues.
   c. It provides users with more precise guidance.
   d. It adds many new examples to clarify the framework concepts.

6. Which of the following is *not* one of the five principles of COBIT5?
   a. meeting stakeholder needs
   b. covering the enterprise end-to-end
   c. enabling a holistic approach
   d. improving organization efficiency

2021/2022 2021/2022 2021/2022

7. Applying the COBIT5 framework, governance is the responsibility of
   a. internal audit.
   b. external audit.
   c. management.
   d. the board of directors.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

8. Applying the COBIT5 framework, monitoring is the responsibility of
   a. the CEO.
   b. the CFO.
   c. the board of directors.
   d. all of the above

9. Why did COSO develop the Enterprise Risk Management framework?
   a. to improve the audit process
   b. to improve the risk management process
   c. to improve the financial reporting process
   d. to improve the manufacturing process

10. Which of the following is *not* a basic principle of the COSO ERM framework?
    a. Companies are formed to create value for society.
    b. Management must decide how much uncertainty it will accept to create value.
    c. Uncertainty results in risk.
    d. Uncertainty results in opportunity.

11. The largest differences between the COSO Integrated Control (IC) framework and the COSO Enterprise Risk Management (ERM) framework is

    a. IC is controls-based, while the ERM is risk-based.
    b. IC is risk-based, while ERM is controls-based.
    c. IC is required, while ERM is optional.
    d. IC is more applicable to international accounting standards, while ERM is more applicable to generally accepted accounting principles.

سليمان طارق عبد الحميد السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

12. Personnel policies such as background checks, mandatory vacations, and rotation of duties tend to deter
    a. unintentional errors.
    b. employee fraud or embezzlement.
    c. fraud by outsiders.
    d. disgruntled employees.

13. Which type of audits can detect fraud and errors?
    a. external audits
    b. internal audits
    c. network security audits
    d. all of the above

14. The amount of risk a company is willing to accept in order to achieve its goals and objectives is
    a. inherent risk.
    b. residual risk.
    c. risk appetite.
    d. risk assessment.

2021/2022 2021/2022 2021/2022

15. The first step of the risk assessment process is generally to
    a. identify controls to reduce all risk to zero.
    b. estimate the exposure from negative events.
    c. identify the threats that the company currently faces.
    d. estimate the risk probability of negative events occurring.

16. Which type of audit assesses employee compliance with management policies and procedures?
    a. external audit
    b. internal audit
    c. network security audit
    d. all of the above

سليمان طارق شبل ابراهيم السعدنى

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

17. Independent checks on performance include all the following *except*
    a. data input validation checks.
    b. reconciling hash totals.
    c. preparing a trial balance report.
    d. supervisor review of journal entries and supporting documentation

18. One of the key objectives of segregating duties is to
    a. ensure that no collusion will occur.
    b. achieve an optimal division of labor for efficient operations.
    c. make sure that different people handle different transactions.
    d. make sure that different people handle different parts of the same transaction.

19. Which of the following is a control related to design and use of documents and records?
    a. locking blank checks in a drawer or safe
    b. sequentially prenumbering sales invoices
    c. reconciling the bank statement to the general ledger
    d. comparing physical inventory counts with perpetual inventory records

20. A store policy that allows retail clerks to process sales returns for $500 or less, with a receipt dated within the past 30 days, is an example of
    a. general authorization.
    b. specific authorization.
    c. special authorization.

سليمان طارق شعبان احمد السعدني

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

d. generic authorization.

21. An accounting policy that requires a purchasing manager to sign off on all purchases over $5,000 is an example of
    a. general authorization.
    b. specific authorization.
    c. special authorization.
    d. generic authorization.

22. The Director of Information Technology for the city of Tampa, Florida formed a company to sell computer supplies and software. All purchases made on behalf of the City were made from her company. She was later charged with fraud for overcharging the City, but was not convicted by a jury. The control issue in this case arose because the Director had both ________ and ________ duties.
    a. custody; authorization
    b. custody; recording
    c. recording; authorization
    d. management; custody

2021/2022 2021/2022 2021/2022

23. As a result of an internal risk assessment, Allstate Insurance decided it was not profitable to provide hurricane insurance in the state of Florida. Allstate apparently chose to ________ the risk of paying hurricane claims in Florida.
    a. reduce
    b. share
    c. avoid
    d. accept

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

REFERENCES

Abu-Musa Ahmad A., and Mohammad S. Khattab (2012), “The Critical Success Factors of Information Security Programs: An Empirical Study in Saudi Companies”, ***Journal of Faculty of Commerce for Scientific Research***, Alexandria University, Vol. 49, No. 1.

Abu-Musa, Ahmad A. (2011), "Exploring Information Systems / Technology Outsourcing in Saudi Organizations: An Empirical Study", ***Journal of Faculty of Commerce for Scientific Research***, Alexandria University, Vol. 48, No. 2., Part I, pp. 51- 111.

Abu-Musa, Ahmad A. and Ehssan Al-Moataz, (2011), "The Effect of Using Electronic Data Processing Systems on the Auditing Procedures and Methods: An Empirical Study on Saudi Accounting Firms", ***Journal of Faculty of Commerce for Scientific Research***, Alexandria University, Vol. 48, No. 2. Part II, pp. 31- 81.

Abu-Musa, Ahmad A. (2011), "Exploring Information Systems/Technology Outsourcing in Saudi Organizations: An Empirical Study", ***Journal of Accounting, Business & Management (JABM)***, Vol. 18 ISSUE 2, ISSN - 0216-423X,.

Abu-Musa, Ahmad A. (2010), "Information Security Governance in Saudi Organizations: An Empirical Study", ***Information Management & Computer Security***, Bradford, Vol. 18, No. 4, pp. 226-276.

Abu-Musa, Ahmad A. (2010), “Investigating Adequacy of Security Controls in Saudi Banking Sector: An Empirical Study”, ***Journal of Accounting, Business & Management (JABM),*** Vol. 17, No. 1, PP. 1- 40.

Abu-Musa, Ahmad A. (2009), “Exploring the Importance and Implementation of COBIT Processes in Developing Countries: An Empirical Study”, ***Information Management & Computer Security***, Bradford, Vol. 17, No. 2, pp. 73-95.

Abu-Musa, Ahmad A. (2009), “Exploring COBIT Processes for ITG in Saudi Organizations: An Empirical Study” ***The International Journal of Digital Accounting Research***, Vol. 9, Iss.15, pp.99-126.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Abu-Musa, Ahmad A. (2008), “Information Technology and its Implications for Internal Auditing: Empirical study on Saudi Organizations”, ***Managerial Auditing Journal,*** Vol. 23, No. 5, pp. 438- 466. **(21 Citations)**

Abu-Musa, Ahmad A. (2007), “Exploring Information Technology Governance (ITG) in Developing Countries: AN Empirical Study” ***The International Journal of Digital Accounting Research,*** Vol. 7, Iss.13-14, pp. 71- 120. **(15 Citations)**

Abu-Musa, Ahmad A. (2007), “Evaluating the Security Controls of CAIS in Developing Countries: An Examination of Current Research”, ***Information Management and Computer Security, USA,*** Vol. 15, Iss.1, pp. 46- 63**. (4 Citations)**

Abu-Musa, Ahmad A. (2007), “Evaluating the Security Controls of CAIS in Developing Countries: An Empirical Investigation”, ***Information Management and Computer Security, USA,*** Vol. 15, Iss.2, pp. 128- 148.

Abu-Musa, Ahmad A. (2006), **"**Evaluating the Security Controls of CAIS in Developing Countries: The Case of Saudi Arabia", ***The International Journal of Digital Accounting Research,*** Vol. 6, Iss.11, pp. 25- 64. **(8 Citations)**

Abu-Musa, Ahmad A. (2006), “Perceived Security Threats of Computerized Information Systems in the Egyptian Banking Industry”, ***Journal of Information Systems***, Vol. 20, Iss.1, PP. 189 -205. **(19 Citations)**

Abu-Musa, Ahmad A. (2006), **“**Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", ***Journal of King Saud University - Computer and Information Sciences***, Vol. 18, pp. 1 -30. **(9 Citations)**

Abu-Musa, Ahmad A. (2006), "Exploring Perceived Threats of CAIS in Developing Countries: The Case of Saudi Arabia", ***The Journal of Managerial Auditing, UK,*** Vol. 21, Iss.6, pp. 487- 407.

Abu-Musa, Ahmad A. (2005), "The Role of IT Governance in Improving Corporate Governance: A Proposed Model from Managerial Accounting Context" ***The Journal of Trade & Finance,*** The

سليمان طارق عبد الحميد السعدنى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Scientific Journal of the Faculty of Commerce, Tanta University, Egypt, Summer, Vol. 25, Number 2, pp. 55-118. [Arabic]

Abu-Musa, Ahmad A. (2005), “The Determinates of Selecting Accounting Software: A Proposed Model”, ***The Review of Business Information Systems, USA***, summer, Vol. 9, Number 3; PP. 85-109.

Abu-Musa, Ahmad A. (2004), “Investigating the Security Policies of Computerized Accounting Information Systems in the Banking Industry of an Emerging Economy: The Case of Egypt”, ***The Review of Business Information Systems***, summer, Vol. 8. Number 3; PP. 83-102.

Abu-Musa, Ahmad A. (2004), “Investigating the Security Controls of CAIS in an Emerging Economy: An Empirical Study on Egyptian Banking Industry”, ***The Journal of Managerial Auditing, UK,*** Vol. 19, Iss.2, pp. 272 -302. **(15 Citations)**

Abu-Musa, Ahmad A. (2004), “Important Threats to Computerized Accounting Information Systems: An empirical Study on Saudi Organizations” ***Pubic Administration***, A Professional Quarterly Journal Published by The Institute of Public Administration, Riyadh, Saudi Arabia, vol. 44, No. 3, pp. 509 – 570. [Arabic]

2021/2022 2021/2022 2021/2022

Abu-Musa, Ahmad A. (2004), “Auditing E-Business: New Challenges for External Auditors”, ***Journal of American Academy of Business, Cambridge, US***A, September Vol. 4. No.1 & 2, March, pp. 28-41.

Abu-Musa, Ahmad A. (2003), “The Perceived Threats to the Security of Computerized Accounting Information Systems”, ***The Journal of American Academy of Business, Cambridge, USA,*** Vol. 3, No.1, September, pp. 9- 20.

Abu-Musa, Ahmad A. (2002), “Computer Crimes: How Can You Protect Your Computerized Accounting Information System”, ***the Journal of American Academy of Business, Cambridge, USA***, Vol. 2. No.1 Sept., pp. 91-11.

30006101601571 30006101601571 30006101601571

Abu-Musa, Ahmad A. (2002), “Security of Computerized Accounting Information Systems: An Integrated Evaluation Approach”, ***the***

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Journal of American Academy of Business, Cambridge, USA, Vol. 2. No.1 September 2002, pp. 141-149.

Abu-Musa, Ahmad A. (2002), "Security of Computerized Accounting Information Systems: A Theoretical Framework", ***the Journal of American Academy of Business, Cambridge, USA***, Vol. 2. No.1 September, pp. 150-155.

Abu-Musa, Ahmad A. (2001), Evaluating the Security of Computerized Accounting Information Systems: An Empirical Study on the Egyptian Banking Industry, ***PhD Thesis in Accountancy***, University of Aberdeen, U.K.

Abu-Musa, Ahmad A. and Roger Buckland (2001a), "Evaluating The Security of Computerized Accounting Information Systems In Developing Countries: Evidence from Egyptian Banking Industry", ***British Accounting Association Annual Conference 2001,*** (26th -28th March), University of Nottingham, UK.

Abu-Musa, Ahmad A. and Roger Buckland (2001b), "Evaluating The Security of Computerized Accounting Information Systems In Developing Countries: An Empirical Study in Egyptian Banking Industry", ***European Accounting Association 24th Annual Congress Athens 2001,*** (18th - 20th April), Athens University of Economics and Business (AUEB), Greece.

Abu-Musa, Ahmad A. (2000a), "The Threats of Computerized Accounting Information Systems: An Empirical Study on Egyptian Banking Industry", ***Working Paper, British Accounting Association Annual Conference 2000,*** (11th - 13th April), University of Exeter, UK.

Abu-Musa, Ahmad A. (2000b), "Security of AIS", ***Working Paper, BAA-ICAEW Doctoral Colloquium,*** (18th -20th April), Manchester Business School, the University of Manchester, UK

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدنى
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Abu-Musa, Ahmad A. (2000c), "Evaluating The Security of information: An Empirical Study on Egyptian Banks", ***Working Paper, ICAS / BAA Accounting & Finance Colloquium for ScotDoc,*** (19th June), University of Glasgow, UK.

Abu-Musa, Ahmad A. (2000d), "Evaluating The Security Controls of Computerized Accounting Systems: An Empirical Study on the Egyptian Banking Industry", ***Time, Space and Power Postgraduate Conference,*** (13th-14th July), Faculty of Social Science and Law, Aberdeen University.

Abu-Musa, Ahmad A. and Roger Buckland (2000a), "Evaluating The Security of Computerized Accounting Information Systems: Threats and Controls - An Empirical Study on the Egyptian Banking Industry", ***International Accounting and Finance Special Interest Groups 2000 Conference,*** (11th September) Cardiff Business School, Cardiff University, UK.

Abu-Musa, Ahmad A. and Roger Buckland (2000b), "Evaluating The Security Controls of Computerized Accounting Systems: An Empirical Study on the Egyptian Banking Industry", ***MARG (Management Accounting Research Group) 2000 Conference,*** (11th-12th September), Aston Business School, University of Birmingham, UK.

Abu-Musa, Ahmad A. (1999a), "Evaluating the Security of Computerized Accounting Information Systems: An Empirical Study", ***Working Paper, BAICAEW Doctoral Colloquium,*** (14th-16th April), Manchester Business School, the University of Manchester, UK.

Abu-Musa, Ahmad A. (1999b), "Evaluating the Security of Computerized Accounting Information Systems: A Pilot Study on Egyptian Banking Industry", ***Working Paper, AIB (Academy of International Business), 26th Annual Conference,*** (16th-17th April) University of Stirling, UK.

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Abu-Musa, Ahmad A. (1999c), "Evaluating Accounting Information Security in Computerized Systems: An Empirical Study on Egyptian Organizations", ***Working Paper, American Accounting Association / Taiwan Accounting Association First Globalization Conference,*** (10th -15th July), Taipei, Taiwan. (Accepted Paper)

Abu-Musa, Ahmad A. (1998), "Evaluating Accounting Information Systems Security: An Empirical Study on Egyptian Organizations", ***Working Paper, ICAS / BAA Accounting & Finance Colloquium for Scots Ph.D. students,*** 24th June, Dundee University, UK.

Advisory Committee For The Co-ordination of Information Systems (ACCIS) (1992), ***Information System Security Guidelines For The United Nations Organizations,*** (United Nations, New York).

Anderson, Richard J. (1996), "From Critics To Coaches", ***Bank Management,*** (May / Jun.), pp. 26-32.

Anderson, Ross J. (1994), "Information Management & Computer Security: Whither Cryptography?", ***Information Management & Computer Security,*** (Vol. 2, No. 5), pp. 13-20.

Arab African International Bank (1997), "World Economic Analysis: Egypt", ***Euromoney,*** (September), London, p. 50.

Bandyopadhyay, Kakoli, Peter P. Mykytyn and Kathleen Mykytyn (1999), "A Framework for Integrated Risk Management in Information Technology", ***Management Decision,*** (Vol. 37, Iss. 5).

Bank Management (1990), "Assets At Risk", ***Bank Management (BAD),*** (Vol. 66, Iss. 1) pp. 44 - 48.

Baskerville, Richard (1988), ***Designing Information System Security,*** John Wiley and Sons, New York.

Bodnar, George H. (1995), "Trends In Data Security", ***Internal Auditing,*** (Summer), pp. 5 - 55.

2021/2022 2021/2022 2021/2022
سليمان طارق شعبان ابراهيم السعدني
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Boockholdt, J. L. (1989), "Implementing Security and Integrity in Macro-Mainframe Networks", ***MIS Quarterly***, (June), pp. 135 - 144.

Boritz, J. Efrim (1999), ***Computer Control and Audit Guide,*** (http:// arts.unwareloo.co/ACCA/ccag).

Bowling, Ann (1997), ***Research Methods in Health: Investigating Health and Health Services***, Open University Press, Buckingham, UK.

Buttross, Thomas E. and John C. Malley (1990), "What You Need To Know about Microcomputer Security", ***Practical Accounting,*** (Vol. 23, Iss. 6), pp. 94 -100.

Buttross, Thomas E. and Michael D. Ackers (1990), "A Time - Saving Approach To Microcomputer Security", ***Journal Of Accounting & EDP,*** (Vol. 6, Iss. 1), pp. 31 - 35.

Clay, Bruce M. (1995), "PC Security Criteria A to Z: The Why And What Of Providing PC Security", ***IS Audit and Control Journal,*** (Vol. 5), pp. 27-32.

Clayton, Michelle (1998), "FDIC addresses Internet security risks", ***America's n Community Banker,*** February, (Vol. 7, Iss. 2), p. 40.

Cloud, Avery C. (1990), "An EDP Audit with a Twist", ***Information Executive***, (Fall), pp. 14 - 15.

Collier, Paul, Rob Dixon and Claire Marston (1991), "The Role of Internal Auditor in The Prevention and Detection Of Computer Fraud", ***Public Money and Management,*** (Winter), pp. 53 - 61.

Collins, Tony (1992), "Bank Worker Guilty of ATM Fraud", ***Computer Weekly,*** March 19, p. 4.

Computer Security Auditing and Controls (1991), "Methods for Documenting Controls and Security Provisions", ***Computer Security Auditing and Controls,*** (Vol. 18, Iss. 3), pp. 1 - 14.

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Conrath David W. and Ravi S. Sharma (1993), “Evaluation Measures for Computer Based Information Systems”, ***Computers in Industry,*** (Vol. 21 Iss. 4), pp. 267 - 271.

Corbitt, Terry (1996), “Stop, Thief”, ***Accountancy Age***, (Feb), p. 20

Courtney, Harley M., Cheryl L. Prachyl and Terryann Glandon (1998), “Guide to Accounting Software: The Pluses and Minuses of Nine Leading Mid-Price-Range Products”, ***Journal of Accountancy,*** March (Vol.185, No.3), pp. 44 - 61.

Courtney, Robert H. (1987), “Contemporary Data Security : A Leadership Vacuum”, ***Computer Security Journal***, (Vol. IV, No. 2).

Crockett, Barton (1993), “Banks Are Leaders in Computer Security”, ***American Banker***, (Nov.), p. 20.

Crockford, N. (1880), ***An Introduction to Risk Management,*** Woodhead-Faulkner Limited, Cambridge, England. 359

Crossborder Monitor (1998), “Egypt: Banking on Privatization”, ***Crossborder Monitor,*** New York, (Jun 24, Vol.6, Iss. 25), p. 6.

Cushing, Romney (1994), ***Accounting information Systems,*** Sixth edition, Addison-Wesley publishing company, USA.

Davis, Charles E. (1996), “Perceived Security Threats to Today’s Accounting Information Systems: A Survey of CISAs”, ***IS Audit & Control Journal,*** (Vol. 3), pp. 38 - 41.

Davis, Charles E. (1997), “An Assessment of Accounting Information Security”, ***The CPA Journal,*** New York (Vol. 67, Iss. 3), pp. 28 - 34.

Demirsar, Metin (1998), “Banking”, ***Institutional Investor,*** New York, (Jun 24, Vol.32, Iss. 7) p. E8.

Dickinson (1990), ***Statistical Analysis in Accounting and Finance***, Philip Allan, London.

2021/2022 2021/2022 2021/2022
سليمان طارق شبل ابراهيم السعدني
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Doost, Roger K. (1990), "Accounting Irregularities And Computer Fraud", ***National Public Accountant,*** (Vol. 35 Iss. 5), pp. 36 - 39.

Dopp, Paul (1995), "Abusing the System", ***CGA Magazine***, (Jan), pp. 40 - 45.

Dorey, Paul G. (1991), "The Business of Computer Security Risk Management", ***Computer Security Guide,*** pp. 63 - 66.

Dougan, Jim (1994), "Internal Control Checklist for Hospitality Computer Systems", ***Bottom Line,*** (Vol. 9, Iss. 5), pp. 8 - 11.

EDPACS (1992), "A major International Organization Ignores Computer Security", ***EDPACS: The EDP Audit, Control, & Security Newsletter,*** (Vol. 20, Iss. 4), pp. 18-19.

Eloff, J. H. P., L. Labuschagne and K. P. Badenhorst (1993), "A Comparative Framework for Risk Analysis Methods", ***Computers & Security,*** (Vol. 12), pp. 597 - 603.

FDIC (Federal Deposit Insurance Corporation) (1999), ***Risk Assessment Tools and Practices for Information System Security,*** July 7, FDIC financial institutions letters, Washington.

Feeney, Kevin (1993), "How To Deal With Computer Fraud", ***Connecticut CPA Quarterly***, (March), pp. 10-11.

FFIEC (1996), ***IS Examination Handbook, Chapter, 14, Security-Physical And Data.*** Fink, Arlene and Jacqueline Kosecoff (1985), ***How To Conduct Surveys: A step-by-step Guide***, Sage Publication, London.

Finzel, Tobie (1993), "The IS Professional And The IS Auditor: A Partnership Formed To Achieve Common Goals", ***Computer Security Journal,*** (Fall), pp .27-35.

Fried, Louis (1994), "Information Security And New Technology", ***Information Systems Management,*** (Summer), pp. 57 - 63.

Gentile, Francesco, Luigi Giuri, Emilio Montolivo and Michele Volpe (1994), "Security Evaluation in Information Technology

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Standards”, ***Computers and Security,*** (Vol. 13, Iss. 8), pp. 79 - 89.

Gollmann, Dieter and Peer Wichmann, (1992), “PC Security Evaluation”, ***Managerial Auditing Journal,*** (Vol. 7, Iss. 6), pp. 2 -3.

Goodhue, Dale L. and Detmar W. Straub (1991), “Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security”, ***Information & Management,*** (Vol. 20), pp. 13 - 27.

Goussak, Gregory W. (1995), “Auditing The Effectiveness Of information Systems In The Hospitality Industry”, ***Bottom Line***, (Oct. / Nov.), pp. 14-16.

Granat, Burton (1998), “Up In Smoke: Security And Information Management Source”, ***Inform*** (Vol.12, Iss. 1), pp. 34.

Greengard, Sam (1998), “How Secure Is Your Data?” ***Workforce,*** May, (Vol. 77, No. 5), pp. 52-58.

Grundy, Emma, Collier, Paul and Spaul, Barry (1994), “Auditing Personnel: A Human Resource Approach to Information System Control”, ***Managerial Auditing Journal,*** (Vol. 9), pp. 10-16.

Harris, Duncan and David Sidwell (1994), “Distributed Database Security”, ***Computers & Security,*** (Vol. 17, Iss. 3), pp. 547 - 557.

Haugen Susan and J. Roger Selin (1999), “Identifying and Controlling Computer Crime and Employee Fraud”, ***Industrial Management and Data Systems,*** (Vol. 99, Iss. 8).

Henry, Laurie (1997), “A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia”, ***The Mid-Atlantic Journal of Business,*** (Vol. 33, Iss. 63), pp. 171 - 189.

Herold, Rebecca (1994), “Case Study: An Information Security Program”, ***Computer Security Journal,*** (Fall), pp.17 - 26.

سليمان طارق شبل ابراهيم السعدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Hessler, Richard, M. (1992), ***Social Research Methods,*** West Publishing Company, New York.

Hester, Edward D. and Andrew C Gross (1998), “Industry Corner: The Information Security Marketplace”, ***Business Economics,*** (Vol. 33, Iss. 2), Washington, pp. 52 - 56.

Huntington, Ian and David Davies (1994), ***Fraud Watch,*** The Institute of Chartered Accountants in England and Wales, London.

Hussin, Husnayati (1998), ***Alignment of Business Strategy and IT In Small Business***, Doctoral Thesis, Loughborough University, UK.

Huston, Terry L. and Janis L. Huston (1998), “Security in the Management of Information Systems”, ***Health Care Supervisor,*** (Jun) (Vol.16, No.4), pp. 28 - 34.

Info World Canada (1995), “Top Management Needs To Address Security: Study”, ***Info Canada,*** (Feb.), pp. IC 13- 14.

International Federation of Accountants (IFAC), Information Technology Committee, (1998), ***International Information Technology Guidelines: Managing Security of Information,*** The (January), New York.

2021/2022 2021/2022 2021/2022

Jenkins, Brian, Peter Cooke and Peter, Quest (1992), ***An Audit Approach to Computers,*** Institute of Chartered Accountants In England And Wales, London.

Journal of Accountancy (1998), “Internet Caveats”, ***Journal of Accountancy,*** (Vol. 185, Iss. 3), pp.14 - 15.

Joy, Ralph R. and Mellon Bank (1992), “A Practical Guide To Treasury Management Security” J***ournal Of Cash Management,*** (Vol. 12, Iss. 2), pp. 35 - 40.

Kay, Russell (1994), “Distributed and Secure”, ***Byte***, (June), pp. 165 - 178.

Katz, David (2000), “Elements of a Comprehensive Security Solution”, ***Health Management Technology,*** (Vol. 21, Iss. 6), pp. 12-16.

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Kirch, John F. (1998) “Virus Patrol”, ***Security Management,*** April (Vol. 42, No. 4), pp. 18-20.

KPMG (2000), ***Information Security Survey 2000, Executive Summary***, April, KPMG, London.

Kulczycki, Glory (1997), “Information Security”, ***Management Accounting;*** (Vol. 79, Iss. 6), pp. 18 - 24.

Kumar, K. (1990), “Post Implementation Evaluation of Computer-Based Information Systems: Current Practices”, ***Commun. ACM***, (Vol. 33, No. 2), pp. 217 - 226.

LaPolla, Stephanie (1992), “High Tech’s Dark Side: Fraud, Forgery, Check Swindles; Scanners, Printers are Accomplices in Crime”, ***PC Week,*** July 20, (Vol. 9, N. 29), p. 23.

Leary, John (1995), “Bench Marking Your Security Program” ***Computer Security Journal,*** (Fall), pp. 25 - 34.

Lee, Chi-Lin (1995), ***“A Study of Financial Institutions, Information Security: Factors That Influence Employees, Willingness to Adhere to Information security procedures”,*** DBA (ADAI) Dissertation, (June), pp. 1 - 153.

Leinicke, Linda Marie, W. Max Rexroad and Jon D. Ward (1990), “Computer Fraud Auditing: It Works”, ***Internal Auditor,*** (Vol. 47 Iss. 4), pp. 26 - 33.

Levi, Philip (1993), “PC security for accountants - What’s Hot And What’s New”, ***Accounting Technology,*** (Feb. / Mar.), pp. 26-30.

List, William and Robert Melville (1994), “Integrity In Information Systems – Executive Summery”, ***Computers and Security,*** (Vol. 13), pp. 295 - 301.

Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (1992), “Threats To Information Systems: Today’s Reality, Yesterday’s Understanding”, ***MIS Quarterly,*** (June), pp. 173 - 186.

Malik, Bill (1997), “Information Security: Coping With Risks”, ***Forbes;*** New York; September, 22, pp. 26-28 .

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Marro Pual E. (1995), “Overview Of Computer Crime And Security”, ***IS Audit and Control Journal,*** (Vol. 5), pp. 20 - 25.

Mathieson, Kieran (1993), “Techniques Reducing Bias In Users’ Evaluation of Information Systems”, ***Information and Management,*** (Vol. 25, Part 3), pp. 165-171.

Mau, Sonya and Jack, Catlin (1993), “Systems Security In 90’s”, ***Interpreter***, (January), pp. 8-9.

Mayu, Mishina, (1998), “Connectivity creates security headaches”, ***As/400 Systems Management,*** May (Vol. 26, No.5), pp.16 - 19.

McIntyre, Andy (1991), “Security And The Mainframe Computer”, ***Computer Security Guide***, pp. 40 - 43.

Meall, Lesley (1992), “Computer Crime: Foiling the Fraudsters”, ***Accountancy,*** (November), pp. 56-57.

Menkus, Belden (1991), “Six Key Factors In Evaluating Information Security Mechanisms”, ***EDPACS: The EDP Audit, Control, and Security Newsletter,*** (Vol. 18, Iss.10), pp. 11-13.

Miller, Delbert C. (1991), ***Handbook of Research Design and Social Measurement,*** (Fifth Edition), SAGE Publications, London..

Mitchell, Ruth C., Rita Marcella Mitchell and Graeme Baxter (1999), “Corporate Information Security Management” ***New Library World,*** (Vol. 100 Iss. 5).

Moser, G. A. and G. Kakton (1985), ***Survey Methods in Social Investigation***, Second Edition, Gower publishing company, England.

Moss, Nicholas (1996), “Banks at Mercy of Hackers”, ***The European***, October 10, N.335, p. 24.

Nachmias - Frankfort, Chava and David Nachmias (1992), ***Research Methods in The Social Science***, Fourth Edition, Edward Arnold, London.

2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

OECD (Organization for Economic Co-operation and Development) (1992), ***Guidelines for the Security of Information Systems***, The Council of the OECD, 26 November.

Parker, Donn B. (1976), ***Crime By Computer,*** Charles Scribner’s sons, New York.

Parker, Donn B., (1981), ***Computer Security Management***, Reston Publishing Company, Virginia, USA.

Parker, Donn B. (1983), ***Fighting Computer Crime,*** Charles Scribner’s sons, New York.

Peltier, Tom (1994), “How To Develop A Mission Statement”, ***Computer Security Journal,*** (Vol. 10, Iss. 2), pp. 5 - 15.

Price, R. Leon, John S. Cotner and Warren L. Dickson (1989), “Computer Fraud In Commercial Banks: Management’s Perception of Risk”, ***Journal of Systems Management,*** October, (Vol. 40, No. 10), pp. 28 - 34.

Qureshi, Anique A. and Joel G. Siegel (1997), “The Accountant And Computer Security”, ***The National Public Accountant,*** Washington, May, (Vol. 43, Iss. 3), pp. 12-15.

Rainer, Kelly Rex, Charles A. Snyder and Houston H. Carr (1991) “Risk Analysis for Information Technology”, ***Management Information Systems,*** (Vol. 8, Iss. 1), pp. 129 -

Rockwell, Robin (1990), “The Advent of Computer Related Crimes”, ***Secured Lender***, (Jul /Aug), pp. 40 - 42

Roufaiel, Nazik S. (1990), “Computer Related Crimes: An Educational And Professional Challenge”, ***Managerial Auditing Journal,*** (Vol. 5, Iss. 4), pp. 18 - 25.

Roux, Yves (1991), “Technical Criteria For Security Evaluation Of IT Products”, ***Computer Security Guide***, pp. 59 - 62.

Roy, Ashok and Seong Park (1994), “EDP Control And Security: Common Issues And Problems”, ***Internal Auditing,*** (Winter), pp. 81 - 84.

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Ryan, S. D. and B. Bordoloi (1997), “Evaluating Security Threats In Mainframe And Client / Server Environments”, ***Information & Management,*** (Vol. 32, Iss. 3), pp. 137 -

Sampson, Russell J. (1993), “Computer Security - Deficiencies In Small Business”, ***Accountants’ Journal***, (June), pp. 45 - 46

Schou, Corey D, W. Vic Machonachy, F. Lynn McNulty and Arthur Chantker (1993), “Information Security Professionalism For 1990s”, ***Computer Security Journal,*** (Spring), pp. 27 - 37

Schweitzer, James A. (1987), ***Computers, Business, And Security,*** Butterworth Publishers, London.

Sheehy, Don and Gerald Trites (1995), “Access Denied”, ***CA Management,*** (September), pp. 50 - 52.

Sherizen, Stanford (1991), “Warning: Computer Crime Is Hazardous to Computer Health”, ***Corporate Controller,*** (Nov. / Dec.), pp. 21 - 24.

Sherizen, Stanford (1992), “The Globalization of Computer Crime And Information Security”, ***Computer Security Journal,*** (Fall), pp. 13 - 19.

2021/2022 2021/2022 2021/2022

Smith, Laura B. (1995), “On The New Beat”, ***PC Week,*** (October30) (Vol. 12, No. 43), pp. E1-2.

Solms, Rossouw Von (1996), “Information Security Management: The Second Generation”, ***Computer & Security (UK)***, pp. 281 - 288.

Solms R. Von, S.H. Von Solm and W.J. Caelli (1994), “A Framework For Information Security Evaluation”, ***Information & Management,*** (Vol. 26, Iss. 3), pp. 143 - 153.

Stahl, H. Stanley (1993), “Information Security In Workstation Environments”, ***Computers and Security,*** (Vol. 12, Iss. 2), pp. 117 - 122.

30006101601571 30006101601571 30006101601571

Strous L. (1994), “Security Evaluation Criteria”, ***Computer and Security,*** (Vol. 13).

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Symons, V. J. (1993), “Evaluation And The Failure Of Control: Information Systems Development In The Processing Company”, ***Accounting Management and Information Technology,*** (Vol. 3, No. 1), pp. 51 - 76.

Thompson, Kathleen (1999), “Privacy and Huggermuggery”, ***Credit Union Magazine*** Madison, January.

Warigon, Slemo (1998), “Data Warehouse Control And Security”, ***The Internal Auditor,*** (February, Vol.55, No1), pp. 54 - 60.

Weingartner, A. and Maggie Burton (1991), “PC Security - Don’t Be Caught Out”, ***Computer Security Guide,*** pp. 33 - 35.

Weiss, Kenneth P. (1990), “Controlling the Threat to Computer Security”, ***Management Review,*** (June), (Vol. 79, No. 6), pp. 54 - 58.

West, Owen D. III and Christopher Zoladz (1993), “Microcomputer Security: Is Your Organization At Risk?” ***EDP Auditor Journal,*** (Vol. 4), pp. 44 - 49.

Wheatman, Victor S. (1998), “Risky Business Over The Net”, ***Information Week,*** May 4**,** (680), pp. 17ER - 20ER.

Williams, Paul (1995), “Safe, Secure And Up To Standard”, ***Accountancy,*** p. 60.

Wong, Ken (1993), “Securing Peace of Mind”, ***Computer Weekly***, (May), p. 38.

Wood, Charles Cresson and William W. Banks (1993), “Human Error : An Overlooked but Significant Information Security Problem”, ***Computers & Security***, (Vol. 12, Iss. 1), pp. 51 - 60

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

كراسة التقويم المستمر

مادة

امن نظم المعلومات

سليمان طارق شبل ابراهيم السعدنى

2021/2022 2021/2022 2021/2022

2022

الاسم/---

30006101601571 30006101601571 30006101601571

رقم الجلوس-------------------------------------

الفرقة الرابعة نظم معلومات الاعمال BIS

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

Please select the best answer for each of the following questions:

1. Identify the type of information below that is least likely to be considered "sensitive" by an organization.
   a. financial statements
   b. legal documents
   c. strategic plans
   d. product cost information

2. Classification of confidential information is the responsibility of whom, according to COBIT5?
   a. external auditor
   b. information owner
   c. IT security professionals
   d. management

3. Which of the following is not one of the basic actions that an organization must take to preserve the confidentiality of sensitive information?
   a. identification of information to be protected
   b. backing up the information
   c. controlling access to the information
   d. training

4. Classification of confidential information is the responsibility of whom, according to COBIT5?
   a. external auditor
   b. information owner
   c. IT security professionals
   d. management

5. Encryption is a necessary part of which information security approach?
   a. defense in depth
   b. time based defense
   c. cloud quarantine
   d. synthetic defense

سليمان طارق شبل ابراهيم السعيدى
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

6. Information rights management software can do all of the following *except*
   a. limiting access to specific files.
   b. limit action privileges to a specific time period.
   c. authenticate individuals accessing information.
   d. specify the actions individuals granted access to information can perform.

7. Identify the first step in protecting the confidentiality of intellectual property below.
   a. Identifying who has access to the intellectual property
   b. Identifying the means necessary to protect the intellectual property
   c. Identifying the weaknesses surrounding the creation of the intellectual property
   d. Identifying what controls should be placed around the intellectual property

8. What confidentiality and security risk does using VoIP present to organizations?
   a. Internet e-mail communications can be intercepted.
   b. Internet photographs can be intercepted.
   c. Internet video can be intercepted.
   d. Internet voice conversations can be intercepted.

2021/2022 2021/2022 2021/2022

سليمان طارق شبل ابراهيم السعدني

9. After the information that needs to be protected has been identified, what step should be completed next?
   a. The information needs to be placed in a secure, central area.
   b. The information needs to be encrypted.
   c. The information needs to be classified in terms of its value to the organization.
   d. The information needs to be depreciated.

30006101601571 30006101601571 30006101601571

10. Which of the following is *not* one of the 10 internationally recognized best practices for protecting the privacy of customers' personal information?
    a. Provide free credit report monitoring for customers.
    b. Inform customers of the option to opt-out of data

collection and use of their personal information.
c. Allow customers' browsers to decline to accept cookies.
d. Utilize controls to prevent unauthorized access to, and disclosure of, customers' information.

11. In developing policies related to personal information about customers, Folding Squid Technologies adhered to the Trust Services framework. The standard applicable to these policies is
a. security.
b. confidentiality.
c. privacy.
d. availability.

12. Which type of software blocks outgoing messages containing key words or phrases associated with an organization's sensitive data?
a. anti-virus software
b. data loss prevention software
c. a digital watermark
d. information rights software

سليمان طارق شبل ابراهيم السعيدي
2021/2022 2021/2022 2021/2022

13. A client approached Paxton Uffe and said, "Paxton, I need for my customers to make payments online using credit cards, but I want to make sure that the credit card data isn't intercepted. What do you suggest?" Paxton responded, "The most effective solution is to implement
a. a data masking program."
b. a virtual private network."
c. a private cloud environment."
d. an encryption system with digital signatures."

30006101601571 30006101601571 30006101601571

14. The first steps in protecting the privacy of personal information is to identify
a. what sensitive information is possessed by the organization.
b. where sensitive information is stored.
c. who has access to sensitive information.

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

d. All of the above are first steps in protecting privacy.

15.It is impossible to encrypt information

a. transmitted over the Internet.
b. stored on a hard drive.
c. printed on a report.
d. None of the above

16.Data masking is also referred to as

a. encryption.
b. tokenization.
c. captcha.
d. cookies.

17. Identify the item below that is *not* a step you could take to prevent yourself from becoming a victim of identity theft.

a. Shred all documents that contain your personal information.
b. Only print your initial and last name on your personal checks.
c. Do not place checks in your outgoing mail.
d. Refuse to disclose your social security number to anyone or any organization.

18.These are used to create digital signatures.

a. asymmetric encryption and hashing
b. hashing and packet filtering
c. packet filtering and encryption
d. symmetric encryption and hashing

19.If an organization asks you to disclose your social security number, but decides to use it for a different purpose than the one stated in the organization's privacy policies, the organization has likely violated which of the Generally Accepted Privacy Principles?

a. Collection
b. Access
c. Security

سليمان طارق شبل ابراهيم السعيدي
2021/2022 2021/2022 2021/2022
30006101601571 30006101601571 30006101601571

d. Quality

20. All of the following are associated with asymmetric encryption *except*

a. speed.
b. private keys.
c. public keys.
d. no need for key exchange.

21. If an organization asks you to disclose your date of birth and your address, but refuses to let you review or correct the information you provided, the organization has likely violated which of the Generally Accepted Privacy Principles?

a. Collection
b. Access
c. Security
d. Choice and consent

22. If an organization asks you to disclose your date of birth and your address, but fails to take any steps to protect your private information, the organization has likely violated which of the Generally Accepted Privacy Principles?

2021/2022 2021/2022 2021/2022

a. Collection
b. Access
c. Security
d. Quality

سليمان طارق شبل ابراهيم السعيدنى

23. An electronic document that certifies the identity of the owner of a particular public key.

a. asymmetric encryption
b. digital certificate
c. digital signature
d. public key

30006101601571 30006101601571 30006101601571

24. If an organization asks you to disclose your date of birth and your address, but fails to establish any procedures for responding to customer complaints, the organization has likely violated which of the Generally Accepted Privacy Principles?

soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg soliman30977675@commerce.tanta.edu.eg

a. Collection
b. Access
c. Security
d. Monitoring and enforcement

25. The system and processes used to issue and manage asymmetric keys and digital certificates are known as
a. asymmetric encryption.
b. certificate authority.
c. digital signature.
d. public key infrastructure.

سليمان طارق شبل ابراهيم السعدنى

2021/2022 2021/2022 2021/2022

30006101601571 30006101601571 30006101601571