ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

EVALUATING ISO STANDARDS APPLICATION OF SECURITY REQUIREMENTS OF E- BANKING IN SUDAN

Inshirah M. O. Elmaghrabi*, Hoida A. Abdelgadir, Wisal M. Tingari
Sudan Academy for Banking & Finance Sciences – Sudan
Sudan University for Science & Technology – Sudan
Sudan Academy for Banking & Finance Sciences - Sudan

ABSTRACT

This study aimed to measure the application of security requirements for e-banking, according to a series of ISO 27000 standards in Sudanese banks. The study is based on a set of hypotheses; planning for the creation and documentation of administrative and technical unique security requirements of the organization according to the standard documentation ISO 27001 affect the level of security and reduces risk", "implementation of administrative and technical unique security requirements of the organization according to the standard of practice ISO 27002 affect the level security and reduces risk", "setting and using measures to assess the implementation of the administrative and technical security requirements, according to the results of operations and standard measures ISO 27004 affect the level of security and reduces risk", and "setting corrective and preventive actions for the administrative and technical security requirements that are based on the results of the auditing, affect the continuous improvement of information security management system and reduces risk". Data were collected from the managers of the technical departments of the surveyed banks. They were statistically tested. The study ended with different results; most important is that the management of the administrative requirements for securing electronic systems in Sudanese banks is characterized by the following; stated according to the relative importance: security management, implementation and design, as well as risk assessment and re-assessment of awareness and responsibility. It is also proven that the management of the technical requirements for securing electronic systems in the Sudanese banks is excellent in resource security, physical security, network security and software security.

KEYWORDS e-banking, information security, security requirements.

INTRODUCTION

The world has witnessed tremendous technology advances in computer and communication technology (ICT). ICT has become the most important commodity in the information age, characterized by ease of communication and abundance of information and networks throughout the world. This affects the development of all industrial sectors including banking industry. Banking services has started by traditional means, then electronic systems were used in banking transactions, finally, they turned into what is known as Electronic banking "e-banking". E-banking has revealed many risks. It was found that information risks increase with the development of technology. This raised the importance of information security to ensure optimal use of resources and full adoption of best practices to achieve the level of security required to protect e-banking.

RESEARCH PROBLEM

Sudanese banks faced many problems when adopting the e-banking services, including the problem of risks of information security. To minimize risks banks should meet requirements needed for e-banking security in accordance with the ISO 27000 series of Standards. Thus, the research problem could be expressed by the following questions:

a) Do modern technology in banks raises risks of information security?
b) If banks did not apply the security requirements of e-banking in accordance with series standards ISO 27000, do this threaten the security of the Sudanese banks?
c) To what extent do Sudanese banks apply the requirements of e-banking security in accordance with series standards ISO 27000?

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

LITERATURE REVIEW

Below are brief definitions of the main concepts of the research

e-banking

E-banking is to provide traditional and modern banking services directly to customers who have access through online interactive communication channels [Council of Federal Financial Institutions, 2003]. This is to provide easy and convenient banking services at the least cost with the least risk. To achieve this satisfaction, necessary infrastructure for hardware, information systems, networks and fully implemented security requirements should be fulfilled.

Information Security

Procedures and preventive measures for protection against crimes and threats of using technology [National Information Center-Sudan, 2010].

Basic Security Goals

These are confidentiality, data integrity and safety, availability, optimality, lawfulness, responsibility, lack of denial and non-auditing [national information center-Sudan, 2010].

Importance of Security Assurances

This is to reduce direct or indirect losses resulting from e-banking security incidents. Security Assurances allow for quick recovery [National Information Center-Sudan, 2010].

Types of Risks

These are natural risks such as natural disasters and fire, and general risks such as power outages, internet service outages and data theft. Moreover, electronic risks such as viruses, security breach of information system and e-mail spies [Abdelgadir, 2007].

Elements of E-banking Security

These are confidentiality, reliability, content integrity, information, and service continuity [Abdelgadir, 2007].

Security Requirements

These requirements are categorized into administrative security requirements, and technical security requirements [Manual of secure networks, information systems and international business institutions, 2002].

Administrative Security Requirements

According to the manual of secure networks, information systems and international business institutions, 2002, there are 9 principles of Administrative Security Requirements, categorized as follows:

a) Basic principles:
   - awareness
   - liability
   - response

b) Social principles:
   - ethics
   - democracy.

c) Principles of security phases:
   - risk assessment
   - security design and implementation
   - security management
   - revaluation

Technical Security Requirements

Include security requirements for electronic systems and [Abdelgadir, 2007]:

a) Security of Resources
b) Physical security
c) Technical security
d) Network security and software security

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

NATIONAL CENTRE FOR INFORMATION (NCI) - SUDAN AND ISO STANDARDS SERIES IEC 27000

In 2007 NCI was established as in Sudan as a specialist unit for setting information standards. A scientific survey was carried out to set e-banking security standards [International Organization and International Electrotechnical Commission ISO 27002, 2005], and it was approved that standards for e-banking security should contain 4 documents, these are;

Preparatory Document

It is a document to define the committee setting the standards, the e-banking security standards, the purpose of the standards and how they are used and applied. It also defines standard references for e-banking security, and other related terms.

Documentation Standard for E-banking Security Management Systems

It is based on the standard ISO IEC 27001: it is concerned with the requirements of e-banking security management systems. It mainly focuses on the requirements needed to establish a system to manage e-banking security issues within organizations. It is to fix that a specialized unit should be established to deal with e-banking security

Standard for Practice of E-banking Security Management

It is based on the standard ISO IEC 27002: it sets practical guidelines for the management of e-banking security. It constitute the reference of management of e-banking security and of information resources within the organization.

Standard of Measurement of the Effectiveness of E-banking Security Management Systems

It is based on the standard ISO IEC 27004: it is a document to provide advice and guidance for setting up and using measurements and standardization of e-banking security management systems; including polices of e-banking security management system, objectives and security controls.

RESEARCH HYPOTHESES

The study seeks to answer questions relating to the problem through the following hypotheses:

a) The plan to create and document the unique requirements of technical and administrative security according to the documentation standard ISO 27001 affects the level of security and reduces risk.
b) The implementation of the unique requirements of technical and administrative security according to the documentation standard ISO 27002 affects the level of security and reduces risk.
c) Setting measures to evaluate the extent of implementing the requirements of technical and administrative security of output according the standard ISO 27004 affects the level of security and reduces risk.
d) Corrective and preventive procedures of meeting the requirements of technical and administrative security based on results of auditing positively affects the information security management system and reduces risk.

RESEARCH METHODOLOGY

The research follows a descriptive and an analytical methodology to test the hypotheses evaluating the implementation of the e-banking security requirements of e-banking in Sudan. It focuses on administrative and technical security requirements in accordance with ISO 27000 standards series.

Population & Research Sample

The population of the study is managers of the IT departments in the Sudanese banks. Population size = 36. The sample of the study was selected randomly. Sample size = 16 .

Data Collection

A questionnaire was designed to investigate implementation of the requirements of e-banking security in the Sudanese banking sector. It consists of three parts. The first part is composed of statements about demographic characteristics of the respondents. Part two consists of statements defining the requirements of administrative security. Part three consists of statements defining the requirements of technical security.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

Validity Test of the Questionnaire
The test was held to assess validity of the statements evaluating the standards of the requirements of e-banking security. It focuses on the consistency and clarity of the metrics terms.

Reliability Test of the Questionnaire
The test was performed on the demographic answers of respondents to the questionnaire. Cronbach's Alpha was applied. Table 1 illustrate the resulting values; all values exceed 60%, which indicate a very high degree of reliability for all the concerned statements; whether individually evaluated or across all demographic variables. Average %=89.7. This indicates that the standards adopted by the study are highly reliable.

Table 1: Cronbach's Alpha Coefficient of Reliability of Security Requirements

Variable		Statement #	Count of Statements	Cronbach's Alpha (%)	Total %	
First: Requirements of Administrative Security:						
1	Awareness	(1-4)	4	67.5		
2	Responsibility	(1-3)	3	66.7		
3	Response	(1-2)	2	95		
4	ethics and democracy	(1-4)	4	77.5		
5	risk assessment	(1-5)	1	82		
6	implementation and security assessment	(1-5)	5	90		
7	security management	(1-5)	5	98		
8	Reassessment	(1-3)	3	90		
Average					83.3	
Second: Requirements of Technical Security:						
1	security resources	(1-1)	1	80		
2	physical security	(1-1)	1	100		
3	technical security	(1-1)	1	100		
4	network security	(1-1)	1	100		
5	security programs	(1-1)	1	100		
Average					96.0	
Total Average						**89.7**

Testing Research Hypotheses
Table 2 illustrates the descriptive statistics of the administrative requirements [Audit tool, 2005]. Average, standard deviation and ranking of the importance of the standards were computed. The results of table 2 show that security management is highly ranked (=1). Moreover, table 1 illustrate that the value of Cronbach's Alpha =98%. This indicates high reliability of the statements about e-banking security management. On the other hand "responsibility" was the least ranked; 8, and it scored the least of Cronbach's Alpha; 66.7%.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

Table 2: Average and Standard Deviations of Administrative Requirements

Variables		Average	Standard Deviation	Interpretation	Rank
1	Awareness	1.32	0.470	Accepted	7
2	Responsibility	1.33	0.474	Accepted	8
3	Response	1.05	0.219	Accepted	2
4	ethics and democracy	1.22	0.419	Accepted	6
5	risk assessment	1.18	0.386	Accepted	5
6	implementation and security assessment	1.10	0.301	Accepted	3
7	security management	1.02	0.140	Accepted	1
8	Reassessment	1.10	0.301	Accepted	3
-	**Average**	**1.32**	**0.470**	**Accepted**	

The researchers then tested for significant differences between the "acceptance" and "not acceptance" for the variables evaluating administrative requirements of e-banking security. t-Test was used, and the results are illustrated in table 3.

Table 3: Significant Differences of Variables of Administrative Requirements

Variables		Calculated t-Test	Tabulated t-Test
1	Awareness	28.2	12.71
2	Responsibility	28.1	12.71
3	Response	47.9	12.71
4	ethics and democracy	29.1	12.71
5	risk assessment	30.5	12.71
6	implementation and security assessment	36.4	12.71
7	security management	72.4	12.71
8	Reevaluation	36.4	12.71
-	**Average**	**28.1**	**12.71**

Shown in table (3), the values of (t) calculated for significant differences among all variables of administrative requirements exceeds the values of (t) tabulated. This indicates statistically significant differences between the answers of the respondents for the benefit of the respondents accepting the administrative requirements.

Table 4 shows that all respondents agree that they have appropriate security measures for:

a) recruitment, training and retiring of staff
b) physical security to protect the building, equipment and devices and against fire disasters and outages
c) technical security to ensure safety and accuracy during input, processing, saving and retrieval
d) transmission of data is protected against fraud, theft or reliability of the content and its source
e) programmes by keeping the original version of the software.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

Table 4: Availability of security measures in banks

Statements		Percentage %	
Your bank set appropriate security measures for:		Yes	No
1	recruitment, training and retiring of staff	80	20
2	physical security to protect the building, equipment and devices and against fire disasters and outages	100	0
3	technical security to ensure safety and accuracy during input, processing, saving and retrieval	100	0
4	transmission of data is protected against fraud, theft or reliability of the content and its source	100	0
5	programmes by keeping the original version of the software.	100	0
-	Average	96	4

Table 5 shows average, standard deviation and percentage of acceptance of the importance of variables evaluating the technical requirements of e-banking security [Audit tool, 2005]. 98% of the respondents accepted the desired importance.

Table 5: Average and Standard Deviations of Technical Requirements

Variables		Average	Standard Deviation	Acceptance %
1	security of resources	1.2	0.402	80
2	physical security	1	0.000	100
3	technical security	1	0.000	100
4	network security	1	0.000	100
5	SW security	1	0.000	100
-	**Average**	**1.16**	**0.080**	**96**

The results shows that 96% of the respondents agree that technical requirements of e-banking security is fulfilled in Sudanese banks.

CONCLUSION

The study was concluded with the following results and recommendations:

Results

a) Departments of administrative requirements for the security of electronic systems in Sudanese banks are qualified by awareness, responsibility, responsiveness, ethics and democracy, risk assessment, implementation and security assessment 'security management and reassessment. The average total value of Cronbach's Alpha Coefficient of administrative requirements=83.3% as shown in table 1.

b) Departments of technical requirements for the security of electronic systems in Sudanese banks are characterized by secure resources, physical security, technical security, network security, and software security. The average total value of Cronbach's Alpha Coefficient of technical requirements=96% as shown in table 1.

Recommendations

Based on the results of the study the researchers recommend for the banks the following:

a) raising the staff awareness of the importance of information security and familiarize them with the usual methods that can be used for hacking such as email messages that contain viruses, "social engineering" scams.

b) training managers to notice behavior of staff or abnormal use of the system.

c) senior management is to support more security policies; by activating the role of different levels of management, and by delegating power to administrators to fulfill updates of the requirements of information security.

d) periodically testing the recovery plan.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

e) activating procedures that meet requests for information from government agencies or legal actions and identify those who are responsible.
f) activating a plan for risk assessment of information and communication technology (ICT).
g) setting policies to assure that information is only accessed in accordance with the principle of "knowledge as much as needed". This is to reduce the chances of bad exploitation of power.
h) setting rules to verify that the "criminal record" of candidates for employment in the information department is clear.
i) installing the Secure Socket Layer Protocol Certificate. It is used in many e-commerce transactions between businesses and customers for ease of use without the need to download additional software.

REFERENCES

1. Federal Financial Institutions Examination Council: E-Banking, IT Examination Handbook, August 2003
2. "*An Introduction to Information Security Policies and Standards*". Standards Committee of Operating Systems, Privacy and Security - Unit of Standards - Section of Quality and Development - Technical Department - 1st ed., pp. 6, 7, 49. National Centre for Information-Sudan, 2010
3. Abdelgadir, Howaida Ali. "Management Information Systems: Theory and Practice", Sudan University of Science and Technology, 1st ed., 2007
4. *"Information Security for Executive Managers. Towards Culture of Security'.* A Manual of Securing Networks & Information Systems for International Business Institutions in Accordance & The Foundation of The Organization for Economic Cooperation and Development (OECD), 2002
5. "The *Standard for Practicing Information Security Management*". Standards Committee of Operating Systems, Privacy and Security - Unit of Standards - Section of Quality and Development - Technical Department. National Centre for Information-Sudan, 2nd ed. 2005. International Organization for Standards and International Electrotechnical Commission ISO 27002, 2005 "*Information Security*". Audit tool (Questionnaire), ISO IEC 27001-2005