Webology (ISSN: 1735-188X)
Volume 19, Number 3, 2022

The Development Of The Management A Digital Risks To Face The Risk Of Using It In A Sample Of Iraqi Bank

Asst. Prof Salman Abood Zbar

Technical institute of Al-Mussaib, AL- Furat AL-Wsat Technical University (ATU),51009, Iraq
Salman Abood99@gmail.com

Abstract

This study aimed to identify the availability of information security policies and procedures in the fields of (administrative, technical and risk management) in the information system , also identify the steps creating of a digital risk management to counteract the incidental findings that a company use of information technology, applied in the Iraqi banks (the study society) on a sample of (40) individuals. A questionnaire was developed to collect the data needed to measure the variables of the study, and to test the hypotheses used descriptive statistics , the study has reached the following: The sample of the study agreed with the absence of specialized management of security and risk management in Iraqi banks, agreed with that banks implement administrative protection policies in information security system at a level higher than average, also they agreed with that banks follow many technical protection policies and procedures in their information system at a higher level ,but they agreed with the occurrence of risks in the information security system frequently due to lack of experience, awareness and training may occur more than once weekly to monthly. The study reached some of recommendations: To ensure that the activities of digital risk management are continuous and constantly evolving and linked to the Organization's strategy and to make that Organization ready for all possibilities and situations.

Keywords: information, risk, management, technology ,a digital, policy.

Introduction

This study addressed the incidental results that accompanying the use of IT. Many organizations will be develop an administrative position such as Digital Rick Manager (DRM) or its equivalent. This is due to the inability of the IT security team to manage the digital risks associated with the use of modern technologies and applications. The information technology and operational techniques, Internet stuff, and real security techniques, work according to the concept of Interrelationship and interdependence, which requires an integrated methodology based on risk management for governance and management (1)

As indicated in the survey research studies International Foundation (Gartner) that More than half of the

executive heads (CEOs) will be working to develop a managerial position (digital) in their teams by the end of 2015, by 2020, 60 percent of the digital companies will suffer from failures of comprehensive and large in the provision of services because of the inability of the information security team of risk management For modern information technology (2)

The study focused on the concepts related to digital risk management and the establishment of a system for digital risk management according to the ISO and especially the standard 27005 for 2011 which gives managers working in technology centers and departments a detailed framework for the implementation and application of an integrated approach to risk management and threats facing them Information Systems Management(3)

First Topic

Methodology of the study

This topic deals with the following:

First: Study problem:

The acceleration of technology and the feeling of many government and private agencies that they need security of data and that the converted to e-government has been increased the risk of information penetration where the gaps arise in building projects through unqualified companies and non-secure servers (Effective integration) which protects them as a group, not individuals, training the human element, classifying information by confidentiality and community awareness. All these reasons prompt organizations to establish a (Supreme Commission) that coordinates efforts, monitors outputs and intervenes in times of emergency.

Thus, the problem of the study can be summarized in numbers of questions:

1. What are the most important security challenges facing Iraqi banks that deal with information technology?
2. How can these banks protect the security and privacy of information through adherents of administrative and technical policies that prevent or limit such breaches?
3. To what extent can banks meet risks and threats by applying risk-taking policies?
4. Is it possible to rely on specialized teams in information security or establishing a specializing department in managing digital risk in an achieving integration?
5. To what extent does the creation of a specialized management of information security lead to coordination and integration of the security system and what is its responsibility?

Second: Study objectives:

The study aims to the following:

1. Identify the policies adopted by Iraqi banks that deal with information technology to reduce security breaches.

2. Know and understand the steps of establishment a specialized security management information.

Third: Importance of study:

The importance of study is as follows:

1. Availability of policies and procedures by those banks that contribute to development or reduction of risks and threats faced with it.

2. Working on the principle of Interrelationship and interdependence between units or sections of the security system when establishing the management of official risks, as well as coordination with other support organizations in the efforts to confront these risks.

3. Building organizational culture for all departments of the organization to face risks and not

   depends technicians only.

Fourth :(Hypotheses of study): The study aims to achieve the following assumptions:

The following main question must be answered and tested the following hypotheses:

Question: What are the level of policies and procedures adopted by the Iraqi banks (the society study) to reduce the breaches and security threats?

From this question, the hypotheses for the study were determined as follows:

The first hypothesis: Iraqi banks apply administrative policies to faces the using risks of IT.

The second hypothesis: Iraqi banks apply technical policies to faces the risks of the use of IT.

The third Hypothesis: Iraqi banks apply policies to reduce the recurrence of risks and threats of using IT.

Fifth: Society and study sample: The society and sample of the study is represented by the Iraqi Banks Group in the governorate of Babylon and Karbala, that deal in their transactions with electronic transactions and uses of information technology (ATM) visacard ,Electronic transfer, payment through mobile (post) surveyed through a questionnaire dedicated to this purpose

Table (1) Characteristics of the study sample according to the job status

Bank's name	Network Administrator	Technical supervisor	Maintenance Officer	Information securityy **Officer**	Infrastructure Officer	Users of Information	Other issue	NO.
Bank Baghdad branch of babe	**-**	**1**	**1**	**1**	**-**	**6**	1	10
Bank Baghdad branch of Karbala	1	1	1	1	1	**4**	1	**10**
Trade Bank of Iraq branch of Babel	1	**-**	**1**	**1**	**-**	**5**	2	**10**
Trade Bank of Iraq branch of Karbala	**1**	**1**	**1**	**1**	-	**5**	1	**10**
Total								40

Bank's name	Sex		**Age**			**Certification**					**Experience**			
	Female	**Male**	Less than30	**30-40**	more 40	Secondary	Diploma	Bachelor Deg.	Master Deg.	**PhD**	**1-5 Year**	**6-10**	**10 Above**	NO.
Bank Baghdad branch of Babel	**7**	**3**	**3**	**5**	**2**	**-**	-	**9**	**1**	-	**3**	**5**	**2**	10
Bank Baghdad branch of Karbala	5	5	2	5	3	**-**	1	**9**	**-**	-	3	3	4	10
Trade Bank of Iraq branch Babel	4	**6**	**2**	**4**	**4**	**-**	3	**7**	**-**	-	**2**	**5**	**3**	**10**
Trade Bank of Iraq branch karbala	**7**	**3**	**4**	**2**	**4**	**1**	2	**7**	**-**		**-**	**4**	**4**	**10**
Total														40

Table (2) Characteristics of the study sample according to personal data

The second topic: theoretical framework

This from second requirement: The first requirement: concepts related to digital risk management. The second requirement focused on the structure and organization of digital risk management

The first requirement: concepts related to digital risk management

2.1.1 The concept of digital risk management:

As the default approach to digital risk management, digital drivers will dramatically influence governance, control, and decision-making related to digital business.(4)

Also defined from (Forouzan) is the process of identifying vulnerabilities and threating to information resources used by the organization or the IT network to achieve commercial or other objectives, reducing and minimizing weaknesses, if any, to reduce risk to an acceptable level , Based on the value of organization information resources.(5)

This definition illustrates the following:

1. The risk management process is a repetition of ongoing processes and must be infinitely repeats because the working environment is constantly changing, and new threats and weaknesses appear every day.

2. The choice of countermeasures used to manage risk must balance productivity and cost, effectiveness of countermeasures, assets value and data protection.

The researcher defined this as the management to which all units or entities responsible for (information security, the Network of Internet, information technology, IT applications, infrastructure, etc.) are responsible for setting policies and procedures for dealing with risks and breaches of information security, and is accountable to senior management in reporting on information security and developing business methods.

1.2. The Concept of Information security.

The tools and methods are used to protect information from threats or threats by providing tools and means to protect information from internal or external risks, standards and procedures taken to prevent the access of information to unauthorized persons through communications and to ensure the authenticity and validity of communications.(6)

The Second requirement: focused on the structure and organization of digital risk management

First. Basic Function to manage digital risk:

Risk management consists of a set of basic and supportive functions that are integrating between them. They differ from one organization to another according to their needs and are as follows(7)

2.1.1. Function of information technology application: The function responsible for processing and directly related to risk management functions and performs the following functions:

- Information is processing by using various types of IT applications such as application server software,

web server software, e-commerce applications.

- Information is accessed through IT applications by users using client applications in computers, mobile devices, PDAs…etc.

- Information is stored in database, computer hardware, central data storage devices (backup copies), and mobile storage devices.

2.1.2 - function network: which is responsible for local area networks (LAN) or wide (WAN) and secure access to the information technology and the following tasks:

-Exchange of information

- Sharing software: Achieving the possibility of participating in the programs available in the information society.

- Sharing Hard ware: Utilizing network resources such as printers, cameras, fax, ... - E-Mail

- Create Work Groups: Networks allow the ability to create workgroups and allocate a portion of the storage space on the network to members of this group away from the rest of the network Central management

2.1.3 The function of IT: is the function responsible for information technology within the management of the risk and performs the following tasks:

-- Providing computer equipment and peripherals within the specifications to suit the needs of the organization. - Provide digital / personal / smart phone assist devices.

- Provision of fax and mobile phones, system servers, VoIP and voice over Internet protocol

- Maintenance of equipment and equipment.

2.1.4. The function of infrastructure: function is responsible for facilitating the interaction and interaction between the various parties involved such as customers, suppliers, partners, contractors, government agencies, and have different levels of access to information based on its role to be determined, and the most important Tasks you do:

- Construction of buildings .- Provide cables. - Provision of servers. - Configure data storage media. - Provision of equipment and infrastructure supplies. - Create a meeting room, training and demonstration facilities.

2.1.5. Information security function: The function responsible for the security aspects of the risk management environment and its various functions and functions.

- Information Security Awareness - Logical Access Management - Protection against malicious code

- Management of information security incidents - Staff security - Information security and information management - Physical and environmental security - Information security control

Third: Digital Risk Management Policies and Procedures: Policies and Procedures digital risk management

Digital Risk Management Policies: These are documented practical and technical rules to protect an entity from the information security risks that beset its business and technical infrastructure. These policy documents provide a general description of the various controls that the Organization will use to manage The risk management policy documents are a formal declaration of management intent to protect their information assets from related risks. These procedures outline the key activities required to 8)(implement these policies

Fourth: Digital Risk Management Strategy:

The digital risk management strategy is the set
of rules applied by the organization in dealing with technology and information related to access to information and work on its systems and management (9)

Strategic objectives for risk management: The goals of the digital risk management are no less important than the objectives of other sectors and departments in the organization. The organization's management means that all individuals perform their duties and determine the following strategic objectives for the management of digital risk (9)

*Identify users and administrators of their obligations and duties required to protect computer systems and networks as well as protect information in all its forms, and in the stages of input, processing ,transmission and retrieval l
. • Identify and deal with the procedures used to overcome and respond to threats and risks

The third topic: Test and analysis hypotheses of the study

This study deals with the results of the statistical analysis of a study field, which was obtained by analyzing the data which included in the questionnaire for the Iraqi banks (the study society) that dealing electronically. The sample of the study consists of 40 employees were working in the field of IT.

A five-caliber scale was used in the distribution of grades as follows:

Classification	Strongly agree	Agree	To some Extent	Disagree	StrongTy disagree
Grade	5	4	3	2	1

The closer the result of the grade (5) the greater the intensity of the approval of the expression while the intensity of the opposition increases as the result of the scale (1) ,This scales used to measure the

variables of the first and second axis of the questionnaire, the third axis measure used in the distribution of grades as follows:

Classification	At least once a day	At least once a week	At least once Month	At least once aYear	no risk at all
Grade	1	2	3	4	5

The closer the answer of the grade (5), times occur risks decrease to degree lack of risk, the risk is increased whenever the answer is (1) , but if the answer is(3), that means the average number of times the risk occurs.

First: The answers to questions about the availability of administrative protection policies in Iraqi banks.

Table (3) Results of the statistical analysis of administrative policies in Iraqi banks

	Paragraph	Mean	**Df**	**Cv%**	**Agree**
1	There is a Department for Digital Risk Management	**1.65**	**0.695**	**42.1**	**2**
2	Providing of information security and protection personnel	**4.18**	**0.873**	**20.9**	**4**
3	Availability of standard policies, standards characteristics for information security	**3.93**	**1.07**	**27.2**	**4**
4	The interest of senior management in information security is very high	**3.88**	**1.68**	**43.3**	**4**
5	employees Signing to comply with all information security policies, procedures, standards and guidelines	**4.23**	**0.768**	**18.2**	**4**
6	Staff permanently updated Operations	**4.00**	**1.07**	**29.0**	**4**
7	Organizing training periods for new employees on information security policies	**4.33**	**0.859**	**19.8**	**4**
8	Omission of the rights of the employee's use of IT resources and equipment at the end of his service	**4.15**	**0.949**	**22.9**	**4**
9	The Organization is vigilant with its attendant risks	**3.73**	**0.877**	**23.5**	**4**

10	The Organization plans to establish a digital risk management department whose work will be complemented by the units to which it is connected	**4.03**	**0.660**	**13.4**	**4**

Source: Computer-based researcher

Table (4) The Results of the statistical analysis of the availability of information assets management policy.

	Paragraph	**Mean**	**Df**	**VC%**	**Agree**
11	A party responsible for each asset shall have the right to issue a license for using	**3.93**	**1.070**	**27.2**	**4**
12	Classification of information based on sensitivity, importance, privacy , and public information	**4.00**	**0.816**	**20.4**	**4**
13	Review of the information assets periodically to ensure that they are properly classified	**4.10**	**0.841**	**20.5**	**4**
14	The trading, storage and transfer of information assets are destroyed in accordance with the rules set forth in the Information Security System	**3.68**	**1.140**	**31.0**	**4**
15	Identify individuals and groups authorized by the information owner to access sensitive information	**4.28**	**1.11**	**27.8**	**4**

Source: Computer-based researcher

Table (5) the results of the statistical analysis on the use of a set of standards and tools for information security.:

	Paragraph	**Mean**	**D f**	**VC%**	**Agree**
16	The eye network pattern is available	**3.30**	**1.40**	**42.4**	**3**
17	Fingerprint availability	**3.45**	**1.36**	**39.4**	**3**
18	Sound mode **availability**	**2.25**	**1.47**	**65.3**	**2**
19	keyboard pressure pattern availability	**4.00**	**1.11**	**27.3**	**4**

Table (6) Results of statistical analysis of the availability of the policy of using information security technology tools

	Paragraph	Mean	D f	vc%	Agree
20	Usage Smart Card	**4.28**	**0.816**	**19.1**	**4**
21	Using of control cameras	**4.43**	**0.747**	**16.9**	**4**
22	Using of alarm systems	**4.18**	**1.030**	**24.6**	**4**
23	Using of transparent glass for computer rooms	**4.38**	**0.667**	**15.2**	**4**
24	Others	**3.48**	**0.994**	**27.5**	**3**

Source: Computer-based researcher

Second : The answers to questions about the availability of a technical policies in Iraqi banks.

Table (7) Results of statistical analysis of the availability of the policy of protection programs for information security and networks

	Paragraph	mean	D f	VC%	Agree
25	Setting a password that includes letters and numbers of strength and length of safety	**4.20**	**1.11**	**26.4**	**4**
26	Changing Password Management Permanently	**4.15**	**1.00**	**24.1**	**4**
27	ti-virus software is used for genuine, licensed and continuously effective	**4.30**	**0.911**	**21.2**	**4**
28	The organization uses intrusion detection and infiltration programs	**4.03**	**1.16**	**28.8**	**4**
29	Firefighting software to protect and secure the information network and prevent access unauthorized	**4.15**	**0.921**	**22.2**	**4**
30	Availability of programs restricting the use of the wireless network and allows for specific employees	**3.93**	**0.944**	**24.0**	**4**

Source: Computer-based researcher

Table (8) Results of the statistical analysis of the availability of a policy of control and access to information

	Paragraph	Mean	D f	VC%	Agree
31	Determination the powers of authorized users of WIS	**4.28**	**0.599**	**14.0**	**4**
32	Availability of policies restricting access and browsing of specific Internet sites	**3.925**	**1.12**	**28.5**	**4**
33	Setting Access to Databases, Operating System and Application Software	**4.025**	**1.03**	**25.6**	**4**
34	All media are stored in a safe and secure environment	**4.25**	**1.01**	**23.8**	**4**

Table (9) Results of the statistical analysis of the availability of data privacy policy

	Paragraph	Mean	D f	VC%	Agree
35	Provision of information to staff according to work needs	**4.15**	**0.921**	**22.2**	**4**
36	Determination of access powers for external parties with the organization 's information security system	**3.925**	**1.16**	**29.6**	**4**
37	Immediate reporting of weaknesses in information protection	**4.25**	**0.870**	**20.5**	**4**

Source: Computer-based researcher

Table (10) Results of statistical analysis on the availability of data encryption protection policies

	Paragraph	mean	D f	CV%	Agree
38	The Organization uses encryption policy in accordance with ISO standards for coding of messages and data	**4.125**	**0.822**	**19.9**	**4**
39	Encrypt backup back up copies	**4.125**	**0.853**	**20.7**	**4**
40	Disposal procedures for various expired storage media	**3.975**	**0.947**	**23.8**	**4**

Table (11) Results of statistical analysis on the availability of technical policies to protect the access of users to information in Iraqi banks

	Paragraph	Mean	D f	Vc%	Agree
41	Provide procedures and systems to create and manage user accounts and withdraw access rights	**4.00**	**0.785**	**19.6**	**4**
42	Each user of the information system will be assigned an identity and password of	**4.35**	**1.00**	**23.0**	**4**
43	Determination of user responsibilities according to the nature of their respective work	**4.30**	**0.912**	**21.2**	**4**
44	Compel all users to read and sign the non-disclosure agreement with the Organization	**4.225**	**0.698**	**16.5**	**4**

Source: Computer-based researcher

Table (12) Results of the statistical analysis of the technical accident management policy

	Paragraph	Mean	D f	VC%	Agree
45	Requiring staff to prepare a report on security incidents of information in an administrative capacity	**4.075**	**0.615**	**15.1**	**4**
46	Create the most recent intrusion detection alert so that it can respond without delay	**4.225**	**0.891**	**21.1**	**4**
47	providing audit trail procedures to reveal the identity and activities of users connected to the network	**4.075**	**0.730**	**17.9**	**4**
48	Use of survey tools to identify protection vulnerabilities that can be exploited by outside people	**4.025**	**1.074**	**26.7**	**4**
49	Providing clear and effective policies to assess gaps and weaknesses in the information security system	**4.175**	**0.903**	**21.2**	**4**

Table (13) Results of statistical analysis of availability of e-mail policy

	Paragraph	Mean	D f	VC	Agree
50	Using the S / MIME email protocol to e-mail messages	**4.025**	**0.891**	**22.1**	**4**
51	Ensure that anti - virus programs are running for checking e - mail messages	**4.175**	**0.903**	**21.6**	**4**

Source: Computer-based researcher

Third: answers to questions about the availability of risk-response policies in the information security system.

Table (14) Results of the statistical analysis of the recurrence of risks due to lack of awareness and training in Iraqi banks

	Paragraph	At least once a day	At least once a week	At least once a month	At least once a year	No risk at all Average	**Mean**	**D f**	**Agree**
52	tampering or destruction of data by users of the information security system	**5**	**10**	**9**	**1**	**15**	**3.28**	**1.502**	Medium
53	Identity Theft of the Information Security System	**2**	**10**	**5**	**3**	**15**	**3.10**	**1.795**	Medium
54	Misuse of powers granted to users of the information security system	**2**	**12**	**6**	**7**	**13**	**3.425**	**1.02**	Medium
55	Unintentional input of erroneous data by users	**3**	**12**	**10**	**12**	**3**	**3.00**	**1.11**	Medium
56	Making unauthorized copies of important data	**1**	**10**	**6**	**8**	**15**	**3.65**	**1.29**	**High**
57	Unauthorized Access to the Information System for People from Outside of the Organization	**5**	**11**	**6**	**3**	**15**	**3.30**	**1.52**	Medium

.

Table (15) the results of the statistical analysis of the recurrence of risk due to the lack or weakness of instruments, devices and control programs in Iraqi banks

	Paragraph	at least once a day	at least once a week	at least once a month	at least once a year	no risk as all	Mean	D f	Level
58	The entry of viruses into the organization 's information security system	**11**	**6**	**6**	**9**	**8**	**2.925**	**1.53**	**Low**
59	Manipulation and deception of professional and hacking sites of the organization on the Internet	**7**	**7**	**5**	**9**	**12**	**3.30**	**1.51**	Medium
60	Wired capture, communication analysis, and network information theft	**4**	**8**	**5**	**6**	**17**	**3.60**	**1.46**	Medium
61	Dumping the system makes the information network or system permanently busy by sending email messages at once	**3**	**10**	**6**	**14**	**7**	**3.30**	**1.36**	Medium
62	E - mail fraud and information theft of users	**9**	**13**	**6**	**7**	**5**	**2.65**	**1.35**	**Low**
63	Repeated network failure	**5**	**7**	**9**	**9**	**10**	**3.30**	**1.36**	Medium
64	Wireless network penetration	**5**	**10**	**4**	**5**	**16**	**3.425**	**1.53**	Medium
65	Natural disasters such as fires, fumes and gases	**2**	**8**	**4**	**6**	**21**	**3.90**	**1.37**	**High**

Table (16) The results of the statistical analysis, (for the three axes) administrative, technical and policy of dealing with risks and threats in the information security system of Iraqi banks.

	Paragraph	Mean	D f	Agree
1	The first axis Total Management Policies (Information Assets, Metrics Used, IT Tools)	**3.831**	**0.653**	**4**
2	The second axis Total technical policies (security software,	**4.127**	**0.123**	**4**

	control and access, data privacy, data encryption, user access, incident security management, e-mail handling)			
3	**The third axis** Total risk and threat policies (risks and threats due to lack of awareness and training due to lack of or availability of instruments, equipment and control programs)	**3.296**	**0.315**	**4**
The total of the three policies		**3.751**	**0.363**	

Source: Computer-based researcher

It is clear from the following tablethat:

Iraqi banks (sample the study) followed the administrative policies, technical, and the policy of dealing with risks and threats, where are the average arithmetic (3.751), which is higher than the level of the average and standard deviation (0.363) The second axis achieved technical policies higher average arithmetic (4.127), while the third axis policy (3.296). This indicates that the technical policies adopted by Iraqi banks are high by using of a package of security programs, the development of systems to secure control and access to information, the confidentiality and strength of passwords, protect the privacy of data users and the using of anti-virus programs The SAT and control powers of the users' access.

The Iraqi banks (sample of the study) follows a stronger policy in the face of risks and threats by engaging employees in programs and training and use tools, devices and programs that limit those risks and threats.

Testing hypotheses

The first hypothesis: Iraqi banks apply administrative policies to address the risks of using information technology.

Table (17) shows the answer of the sample of the study (40) individuals on the terms composed of the first axis (administrative policies)

One - sample statistics

	N	Mean	Std. Deviation	Std. Error Mean
AXE_1	**24**	**3.8313**	**0.65329**	**0.13335**

	T	dF	Sig.(2-tailed)	Mean Difference	Lower	%95 confidence interval of the difference upper

AXE1	**28.730**	**23**	**0.000**	**3.83123**	**3.5554**	**4.1071**

The above outputs showed the answers to the terms of the administrative policies applied by the Iraqi banks. The mean (3.8313) and the standard deviation of (0.653) and the calculated value (T) (28.73) are greater than the value of the table (2.807),the hypothesis can be accepted
The second hypothesis: Iraqi banks apply technical policies to address the risks of the use of information technology.

Table (18) shows the responses of the study sample on the expressions of the second axis.

Table (18) one - sample statistics

	N	**Mean**	**Std. Deviation**	**Std. Error Mean**
AXE2	**27**	**4.127**	**0.123**	**0.0238**

one – sample statistics

	T	**d F**	**Sig.(2-tailed)**	**Mean Difference**	**Lower**	**%95 confidence interval of the difference upper**
AXE2	**172.980**	**26**	**0.000**	**4.127**	**4.0784**	**4.106**

The above outputs showed the answers to the technical statements applied by the Iraqi banks, where the mean (4.127) and the standard deviation of (0.123) and the value of (T) calculated (172.980), which is greater than the value of the table (2.779.),the hypothesis can be accepted .

The third hypothesis: Iraqi banks are implementing policies to reduce the recurrence of risks and threats to face the complexities of information technology. Table (19) shows the responses of the sample of the study to the statements of the third axis, policies for confronting risks and threats.

Table (19) one - sample statistics

	N	**Mean**	**Std. Deviation**	**Std-Error Mean**
AXE3	**14**	**3.296**	**0.135**	**0.084**

	T	**Df**	**Sig.(2-tailed)**	**Mean difference**	**Lower**	**%95 confidence interval of the difference upper**
AXE3	**39.051**	**13**	**0.000**	**3.296**	**3.114**	**3.479**

Source: Computer-based researcher

The above outputs showed the responses to the statements forming the policies for dealing with risks and threats applied by Iraqi banks. The mean is 3.296, with a standard deviation of (0.315), and the value of (t) calculated (39.051) is greater than the value of the table (3.012). Refers to the existence of risks and threats in the information security system.

The fourth topic: conclusions and recommendations

The study reached to the following conclusion

1. The sample of the study agreed that Iraqi banks implement administrative protection policies that are higher than the average, with an average of (3,831) for all paragraphs. Paragraph (7) provides for training courses for new employees at the highest level, while paragraph (1) in digital risk management), which means that there is no specialized management of security and risk management in Iraqi banks.

3. The interest of IT departments by following many administrative procedures and policies using the standards and IT tools at an average level. Paragraph (20) (smart card usage) achieved the highest level, indicating that the banks are planning to expand this service to the citizens.

4.The study sample agreed to follow several technical protection policies and procedures to secure and protect the privacy of the data for users such as the development of strong passwords to protect user accountsو the use of powerful and continuously updated anti -virus programs، management and control of users' access to the information system، Keep copies of records and all important information inside computer rooms.

5.The study sample (Table 14) agreed with the occurrence of risks in the information security system frequently due to reasons related to IT staff due to lack of experience، awareness and training. The unintentional introduction of wrong data, misuse of powers granted to users, tampering with or damaging data Users, unauthorized copying, unauthorized access to the information system of people from outside the organization are more likely to occur more than once a week to a time per month.

6. The sample (Table 15) agreed that there are some risks that may occur at least once a day, such as data tampering or destruction by users of the information security system. Unauthorized access to the information system by persons outside the organization, inadvertent input of erroneous data by Users, the entry of viruses into the information security system, e-mail fraud and the speed of information, manipulation and deception of professionals and piracy of the site of banks on the Internet.

The study recommends the following:

1. The development of digital risk management in Iraqi banks that deals electronically via the Internet to achieve integration and mutual support between all units associated with that administration. Although it has achieved successes in its policy areas (administrative and technical), it faces risks and threats in its information security system..

2. Development of programs and methods for the use of trading, storage and destruction of

information assets, avoiding identity theft and passwords, and preventing infiltration and penetration of wireless networks connected to the information system.

3. Development the program to raise awareness of security for all employees of banks at all levels.

4. To ensure that the activities of digital risk management are continuous and constantly evolving and linked to the Organization's strategy and to make that Organization ready for all possibilities and situations.

References:

1-Ait news.com/2014/07/21
2.Al-Riyadh Newspaper, Digital Risk Management The Next Shift in the World of Technology, Sunday 27 July 2014, Issue 16834, Al Yamama Health Foundation.

3.Al-Hadi, Mohamed Mohamed, 2013, Modern International Standards Concerning the Security and Privacy of Information, Egyptian Journal of Information, (Compu Net) (Issue 13).

4.Proctor, Paul, 2014, Digital Risk Management The Next Shift in Technology, Sunday 27 July 2014, Issue 16834, Al Yamama Health Foundation

5 . Forouzan , Behrouz A., 2008 , Introduction to cryptography and network security .

6-http://ar.wikipedia.org/w/index.php?title = information security 4 - & oldid=1413377"2014"

7.Saudi Communications and Information Technology Commission, 1432H2011, Guidelines for Information Security Policies and Procedures for Government Agencies, First Edition..

8.Saudi Communications and Information Technology Commission, 1432H2011, Guidelines for Information Security Policies and Procedures for Government Agencies, First Edition.pp.(21-23).

9.Al-Marri, Ayed,2014, Information Security and its elements and their strategy ,htt;//www.dralMari.com/show.asp?Fiel=res –a&id=205.