بسم الله الرحمن الرحيم

Sudan University of Science and Technology

Faculty of Graduate Studies

Deanship of Development and Quality

The Role of ISO Standard 27001:2013

In Developing Organization Performance

Case Study (ZAIN Sudan Telecommunication Company)

دور معيار أيزو 27001:2013 في تطوير أداء المؤسسة

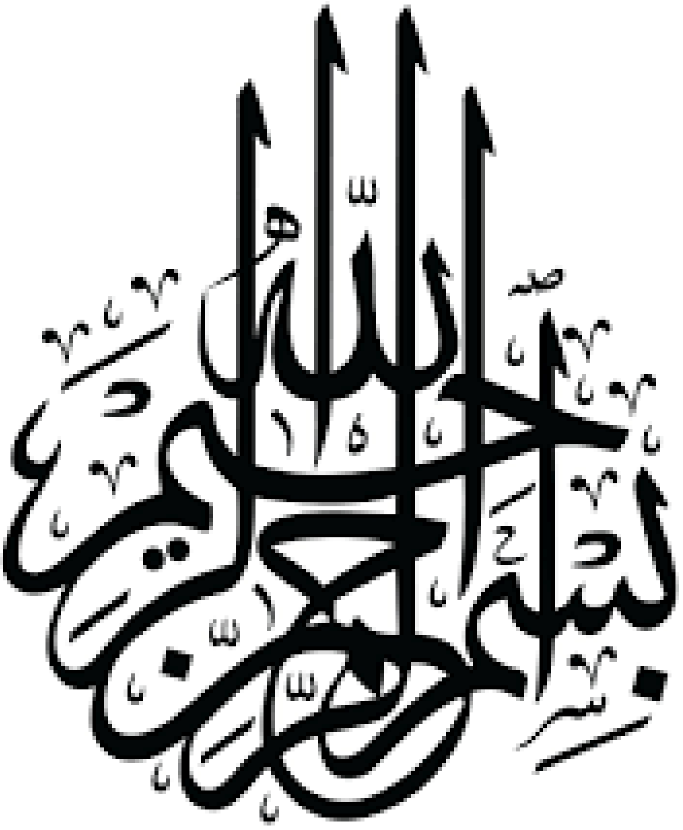
دراسة حالة (شركة زين السودان للاتصالات)

بحث تكميلي لنيل درجة الماجستير في ادارة الجودة والامتياز

Prepared by: Sakina Musa Saied Mohamed

Supervisor: Dr.Rasha Galal Eldin

July 2019


بسم الله الرحمن الرحيم

الإية الكريمة

بسم الله الرحمن الرحيم

قال تعالي :

وَمَا كَانَ لِمُؤْمِنٍ وَلَا مُؤْمِنَةٍ إِذَا قَضَى اللَّهُ وَرَسُولُهُ أَمْرًا أَن يَكُونَ لَهُمُ الْخِيَرَةُ مِنْ أَمْرِهِمْ ۗ وَمَن
يَعْصِ اللَّهَ وَرَسُولَهُ فَقَدْ ضَلَّ ضَلَالًا مُّبِينًا .

سورة الأحزاب

الآية (**36**)

الإهـــداء

إلى من لا يمكن للكلمات أن توفي حقهما

إلى من لا يمكن للأرقام أن تحصي فضائلهما

إلى والدتي العزيزة أدامها الله لنا

إلى روح والدي العزيز " موسى سيد محمد "
رحمة الله عليه

وداعا أبي للقاء إلى يوم الحـــشر ***وإن كان في قلبي عليك لظى الجمر

صبرت لأني لم أجد لي مخلصـــــــا *** وما من حيلة لي سوى الصبر

على وجهك المحزون أوسمة الطهرتراك عيني في الفراش موشحـــــا *** ...

براءة عينيك استثارت مشاعــــــري *** وفاضت بأنهار من الدمع في شعري

تعاصرني ذكراك ياساكن القـــــبر *** وتجتاح أعماقي وإن كنت في الأسر

تمنيت حتى وقفة عند نعشـــــــه *** ترد إلى نفسي الذي ضاع من صبري

تمنيت ما نالت ألوف توجهـــــــت *** إلى ربها صلت عليك مع الظهر

تمنيت كفا من تراب أحثـــــــــه *** على قبرك الميمون طيب من قبر

كأنكم اخترتم زمان رحـــــــيلكم *** بعيد صلاة الليل والخير والصبر

غسلتم بصافي الدمع صافي قلوبكم *** فشعشع فيها النور كالكوكب الدري

لقد انتهيت يا أبي من كدر هذه الدنيا ومن فتنها *** وتركتني فيها البس الحزن

إلى كل من سقط من قلمي سهوا

أهدي هذا العمل

شكر وعرفان

أشكر الله العلي القدير الذي أنعم عليّ بنعمة العقل والدين. القائل في محكم التنزيل "وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ" سورة يوسف آية 76 ....صدق الله العظيم.
وقال رسول الله (صلي الله عليه وسلم":(من صنع إليكم معروفاً فكافئوه، فإن لم تجدوا ما تكافئونه به فادعوا له حتى تروا أنكم كافأتموه) ..... "رواه أبو داوود

وأثني ثناء حسنا على...
وأيضا وفاءً وتقديراً وإعترافاً مني بالجميل أتقدم بجزيل الشكر لأولئك المخلصين الذين لم يألوا جهداً في مساعدتنا في مجال البحث العلمي ، جامعة السودان للعلوم والتكنلوجيا والشكر أجزله لأستاذة كلية الجودة والتطوير وأخص بالذكر الدكتورة الفاضلة: رشا جلال الدين على هذه الدراسة وصاحبة الفضل في توجيهي ومساعدتي في تجميع المادة البحثية، فجزاها الله كل خير.

وأخيراً لا أنسي أن أتقدم بجزيل الشكر الزميل : رامي هاشم " الذي قام بتوجيهنا طيلة إعداد هذا البحث العلمي , ومد لي يد العون والمساعدة في إخراج هذه الدراسة علي أكمل وجه.
الباحث

Abstract

This research presents a role of ISO 27001:2013 due to importance of the Information Management in any organizations such as business, records keeping, financial and so on. This role will help the organizations to fulfill the needs of the customers in managing their personal information, data . There are a few challenges faced by the organizations in managing the information so that it would fall in hand of unauthorized person or hackers.

Besides, an effective information management system can reduces the risk of crisis in the organizations. In order to know more about the importance of information security, the organizations need to overcome the challenges first. Other than that, all organizations must have their policies in secure their information so that the information can be kept safely.

المستخلص

يقدم هذا البحث دور "معيار أيزو 27001:2013 وذلك لأهمية أدارة المعلومات في كل المنظمات مثل الأعمال التجارية ، وحفظ السجلات ، والمالية ، وغيرها . كما سيساعد المؤسسات على الوفاء باحتياجات العملاء في إدارة معلوماتهم الشخصية والبيانات ومعلومات الأمان .

هناك بعض التحديات التي تواجهها المنظمات في إدارة المعلومات بحيث تقع في يد شخص غير مصرحله أو قراصنة، إلى جانب ذلك يمكن لهذا النظام الفعال إدارة أمن المعلومات بشكل يقلل من خطر حدوث أزمة في المنظمات .من أجل معرفة المزيد عن أهمية أمن المعلومات ، تحتاج المنظمات إلى التغلب على التحديات أولاً . بخلاف ذلك يجب على جميع المنظمات أن تضع سياساتها لتأمين معلوماتها بحيث يمكن حفظ المعلومات بسرية وأمان.

List of contents:

List of Tables

List of Figure

Chapter one

Overview

Chapter One

Methodology of the study

1. Introduction:

In the development of high technology nowadays in the world, all the organizations are more depends on their information systems. The public become anxious of the use of the system in saving their information, data and especially their personal information. In addition, the threat from the system hackers and identity theft has added their concern on the use of information system because nowadays there are so many hackers from all around the world.

Therefore, many organizations will identify their information as their important operation which they need to protect as their one of internal control. The scares issues about stolen or missing data are becoming a frequent in all headline news as organizations rely more and more heavily on computers to store sensitive corporate and customer information. It is necessary to be worried about information management because much of the value of a business is concentrate on the value of its information.

1.1 Definition of Information Management :

Information Management plays a key role in Service Management. It must align itself with IT Security and Business management in order to ensure that information across the organization is controlled and managed .Global Strategic Business Process Solutions, Inc. is an **ISO 27001:2013** certified company.
This certification provides enhanced ***data security and integrity*** both internally and to all of our clients. It also plays an important role in sending a valuable and important message to customers and business partners alike, both present and future, that our company does things the right way.

1.2 The Principles of ISO 27001:2013 :

a) Confidentiality :

Ensuring that information is accessible only to those authorized to have access.

b) Integrity :

Safeguarding the accuracy and completeness of information and processing methods

c) Availability:

Ensuring that authorized users have access to information and associated assets when required .

2. The Statement of the Problem and Questions of the study:

The value of information and protecting information are crucial tasks for all the modern organizations. The information were easy to value and protect but however, the organizations would be able to buy or get off-the-shelf information management solutions from other organizations or countries , but Unfortunately There are significant opportunities and areas of improvement in the development of customer services and the highest levels of satisfaction such as :

a) Improper application of quality standards in some sectors.
b) Increase the waste ratio in effort, money and time.
c) Do not protect enterprise information.

3. The Aims and the Objectives of the study :

3.1 Aims of Research:

a) Demonstrates a clear commitment to data management- including confidentiality and strict accessibility rules.
b) Provides procedures to manage risk of losing the information .
c) Keeps confidential information secure and ensures a secure exchange of information.
d) Protects the company, assets, shareholders, employees and clients.

3.2 Objectives of the study:

a) Implement the standard of ISO 27001:2013 to satisfy the customer and to obtain the confidence of stakeholders and customers that their data is protected.
b) Determining the role of implementing ISO 27001: 2013 in improving the image of the establishment and increasing its competitiveness in the market place.
c) This study helps to identify the risks and establish appropriate controls for their management or disposal.
d) Recognize the importance of information management system in increasing the control of waste of resources.
e) The importance of the role and application of the standard in reducing cases of loss of information.

4. The Study Hypotheses:

a) There is a positive relationship between the application of information management system and the development of the Organization performance.

b) The implementation of ISO 27001: 2013 helps to increase the institutional profitability of stakeholders.

c) There is a relationship between the application of ISO standard 27001:2013 and staff satisfaction.

d) There is a relationship between the use of standard and reduce of time and cost.

5. The Significance of the Study :

a) This study will provide the Sudanese Library with increasing the proportion of research related to the manage and confidentiality of information.

b) This study is a reference for researchers and institutions in the importance of implementing the information management system and determining the readiness of the organization to continue its work in the event of emergency and natural accidents that affect its performance.

c) The results of this study will help to clarify the concept of applying quality standards, which is inevitable and not an option in the light of globalization and daily competition. The development of customer services is the main pillar. The focus on customers and their requirements is the basic criterion for increasing market share.

d) This study shows that the commitment to the cafeteria indicates the interest of the organization to develop its performance and its commitment to adhere to the highest quality standards to provide the best services.

6. The Limits of the Study :

- **Site limit**: Sudan-Khartoum - ZAIN Sudan
- **Time limit**: 2017-2019.
- **Human limit**: the employee of ZAIN Sudan _ head quarter

7. Research Terminologies of the Study:

7.1 Methodology of the study:

In order to reach the goal of the research and answer the questions raised within Will be problematic to rely on descriptive analytical method in addition to the case study approach, And to strengthen various aspects of the research topic will be relying on references available both The Arabic-language or foreign languages on the subject of the search, represented in the books, Theses, forums, magazines and scientific journals, Internet web sites and library Electronic generally, in order to enrich the subject and give greater credibility.

To study the issue and verification of the problematic assumptions will be divided into **four research Classes**:

a) Role of ISO standard.
b) Best practice.
c) The concept of (ISO 27001:2013).
d) Questionnaire survey method.

As there is a lack of literature on ISO implementation progress and success factors in the information management implementation domain an exploratory research method was selected. Exploratory research is performed when few or no earlier studies are available. There are no academic studies or literature available for ISO 27001:2013 implementation progress in information management status organizations in Sudan. The focal point is to get insights and familiarity via exploratory research methods research communities.

7.2 Research Tools:

7.2.1 Questioner .
7.2.2 The information from ZAIN SUDAN (head quarter) staff .

Researcher plan in collecting data for this study depends on what set forth around this subject in literature as:

Secondary resources:

Books reference Articles Work papers and internet.

Primary resources:

a) Special meeting interview.
b) Questionnaire and document analysis

7.3 Research Structure:

The research is structure in sections according to each of objectives out lined in table of content.

Section one:

Provide the back ground, research problems, important of the topic, Objective, hypotheses, methodology and previous study.

Section two:

Provide literature review

Section three:

Present data finding and gives analyses to the data (Materials and Methods).

Section four:

Discuss the finding and gives some recommendation conclusion.

Chapter Two

Literatures Review and Previous Studies

Chapter Two

Literatures Review and Previous Studies

2.1 Section One : Information Management System :

2.1.1 Introduction:

In the development of high technology nowadays in the world, all the organizations are more depends on their information systems. The public become anxious of the use of the system in saving their information, data and especially their personal information. In addition, the threat from the system hackers and identity theft has added their concern on the use of information system because nowadays there are so many hackers from all around the world. Because of this, many organizations will identify their information as their important operation which they need to protect as their one of internal control. The scares issues about stolen or missing data are becoming a frequent in all headline news as organizations rely more and more heavily on computers to store sensitive corporate and customer information. It is necessary to be worried about information management because much of the value of a business is concentrate on the value of its information.

Organizations of all sizes will collect and store huge volumes of confidential information which may be about their employees, customers, research, products or financial operations. Most of the information is collected, processed and stored on computers and transmitted across networks from one computer to other computers. It could lead to lost business, law suits, identity theft or even bankruptcy of the business if this information fell into the wrong hands (About.com, 2014). Nowadays, information management also has evolved significantly and grown even more important in recent years. According to About.com website (2014), they stated that, some of the specialty areas or fields within information management are including network , security testing, information systems auditing, application and database management , business continuity planning and digital forensics science are also among others.

2.1.2 The Concept of information security :

According to The Open University website (2014), stated that the meaning of information is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure. Other than that, information management is also means protect the information and information systems from unauthorized access and use, disclosure of information, disruption information, modification or destruction of information in order to provide the integrity, confidentiality and also the availability if information. An integrity means protect against improper information modification or destruction which includes ensuring the information non-dissent and authenticity. While for confidentiality which means authorized restrictions which preserve on access and disclosure which includes protecting personal privacy and proprietary information and lastly, availability is to ensure the timely and reliable access to and use of information (Information Security Handbook, 2014). This definition is based on the concept which a person, business or government will suffer from harm if there is a loss of integrity, confidentiality or availability of information because that is the role of information management to minimize the possibility that such harm will occur. The terms also can change either information security, computer security or information assurances are frequently used.

2.1.3 Importance Of Information management :

Information Technology or as known as IT has become an integral part of and parcel of the organization world today, In fact it will continue becoming an ever larger factor in the future. Organizations will connect their IT systems as a result of linking to the Internet and other networking systems. All of the factors might hold an information security risk for an organization because an organization are attempt to secure their own IT environment although they have little control over the IT systems that they connect with. If the network that the organizations connect with IT environments is insecure, the information management might pose a threat to the IT systems in the host environment. This term paper talks about the importance of information system in an organization.

As people know, information management has become very important in almost organizations. This is because, the information access and use and also the resources has become easier with the emergence of information technology such as the internet and electronic commerce that is use by certain organization. So, in order to make sure that the information system is well organized, the organization need to ensure that their information is properly protected and that they maintain a high level of information security.

The information in an organization need to be protected because it has a value to the organization . The organization usually holds organization and individual records. As for example, the organization may hold sensitive information of their employees, salary information, financial statements and also the business plans for a whole year. Besides, the organization also holds trade secrets, research and other information that gives a competitive edge for their company. Other than that, for individual, the organization hold the information about their personal information that is sensitive on their home computers which typically perform online functions such as banking, shopping and social networking, sharing their sensitive information with others over the internet (MindfulSecurity.com, 2014). As more and more of this information is stored and processed electronically and transmitted across company networks or the internet, the unauthorized access risk will increases and the organization are presented with growing challenges of how best to protect it. According to MindfulSecurity.com website (2014), they told that there is a steps that must be put in order to protect the information.

The same principle can be applied by the organization as the same when people were doing when came out from the house, as for example, people will close the door, close the gate, lock the key and so on when they came out from the house. If the information is not protected, then the information can be accessed by anyone. Besides, if the information is fall on the wrong hand such as theft, hackers and identity theft, it can bring down the business and can commit harm to the whole organization. Top three (3) reasons why information management is importance based on the title, there are three top reasons why information system is importance to an organization.

The reason is as following:

1) Proving that the organization has a secure and stable network assures the customers that their information is safeguarded It is important to think of a system breach in terms of money lost in operations. The sales, customer service, staff productivity and workflow could all be affected by the downtime that will occur. Even after systems are restored many times, an additional checks need to be done to ensure that all factors of the network are clean before business can return to a normal operational state. Nowadays, if there is information breach, the average cost of a data breach is on the rise. Costs went up by over 30% between 2006 and 2007 (Slade, 2009). According to Slade (2009), in addition to these costs, the organization may also lose customers from the negative publicity and may be subject and faced to on-going seystem audits to ensure the incident does not occur again.
2) The insurance companies are increasingly interested in how companies secure their information assets nowadays, there are so many online businesses that usually in social media such as Facebook and Instagram and blogs. Since customers are beginning to do more of their business online, this is one

factor that will begin to influence with all companies either small or large company or the trend will only continue to grow with various kind of online business either in healthy products or cosmetics products. Because of this, the insurance companies are beginning to believe that the businesses will protect the customer's privacy. The insurance company will become more and more common for them to ask for proof that sensitive information is secure and network management software is up-to-date (Slade, 2009). If people maintain confidential client information on the network such as social security numbers, credit card numbers, and other financial data, they should has asked for help and talked to IT consultant about assessing the strength of the firewall in the computer to prevent from information breach. A firewall can be described as a gatekeeper to allow network actions from trusted parties and keep out unauthorized users and harmful viruses. There are also several ways a firewall can be configured and there are pluses and minuses to each (Slade, 2009). To avoid from unwanted issues, the computer must be best protected with integrated firewall to cover the software, hardware and intranet. Besides, it might be best to install a several independent mechanisms with custom levels of protection.

3) Having consistent system practices and IT maintenance procedures ensures Smooth road for business operations the organization must make sure that the computer network in the organization is securely configured and actively prevent from unknown threats. A new methods to protects from unknown threats are emerging every day to protect from malware programs that can be unintentionally installed on customer's or employee's machine, which an attempt to phishing that deceive them into giving up confidential information, to viruses, worms, and strategic identity theft attempts. One of the benefits of having a consistent technology expert on the organization roster is that the expert can offer a fast reaction time and be proactive in safeguarding organization IT system when new warnings first emerge.

   The IT network professional can also help the organization to maintain a secure virtual environment by reviewing all computer assets and determining a plan for preventive maintenance. This also includes routinely cleaning up unnecessary or unsafe programs and software, applying security patches and performing routine scans to check for intrusions. Besides, it is also crucial for the IT professional in organization to change the password of their employee's personal computer frequently, so that the information can be secure properly.

2.1.4 Information management Policies :

The written policies about information management essential to a secure organization . Everyone in a company needs to understand the importance of the role they play in maintaining security. The way to accomplish the importance of information management in an organization is by publishing reasonable company policies. These policies are documents that everyone in the organization should read, sign and compulsory to be followed when they come on board. In the case of existing employees, the policies should be distributed, explained and after adequate time, need for questions and discussions. One key to create effective policies is to make sure that they are clear, and as easy to comply with as possible. Policies that are overly complicated only encourage people to bypass the system. In order to implement this, there a few policies that needs to be followed by the employees.

2.1.4.1 Internet usage:

According to About.com website (2014), stated that the internet contain all information that employees need. It is very important to the organization to collect and gained the information from the internet. However, the internet can also bring dangers to them. As for example, the internet access which includes the downloading of malicious software such as malwares, viruses and Trojans can affect the information system . An internet usage policy should be pressed whether or not the employees are allowed to use the computers at the company for personal uses. Other than that, the policy also must make sure that only the system administrator can downloaded the software in company's computer. The internet usage policy also need to consider whether the employees can use media social using the company's computers or during company time.

2.1.4.2 Email or social networking:

As people know, nowadays, there are so many social networking that can be found on the internet such as Facebook, Instagram, Twitter and Linked. These social networking is being used to connect the people either there are near or far away from each other. Other than that, the email also a way people use to send the data or information to other people. These technologies make it very simple to disseminate information. But, these types of information must be distinguished between the personal or organizations. Once the information is leaves from the building, it can rarely be recalled. So, the employees must and should address appropriate content for company emails and social media pages. Employees must always think that not all private information can stay be private on the internet. They must use a proper way by following the policy to make sure that the company's image will stay clean and confidential information stay be kept.

2.1.4.3Visitor Management:

The visitor is mean that the people other than the employees of an organization. The visitor management must be managing properly so that An unauthorized or unescorted visitor do not intrude in the organization. This is because an unauthorized or unescorted visitor can be a physical threat and can also steal sensitive information. Before a visitor can enter into the organization, all the information about the visitor must be check. If there is problem, the information management guard must take an action. Based on the policy, the visitor might be escorted at all times especially in confidential areas. The visitors are required to wear a badge and should sign in and sign out if necessary. If the policy is being used, the organization will feel more secured and protect the importance information.

2.1.4.4 Key Control:

Unlike an electronic access device, mechanical keys can be duplicated and used without leaving a trail. The organization key control policy should include a means to track who is currently holding mechanical keys and who has permission to duplicate those keys. Besides, all the keys that has been duplicated must be placed on a secure place such as in security room. Employees must write their name on the book to make sure that when the key is lost, the last name of the employees that use the key can be track down. Other than that, the organization must make a policy to use the smart card reader other than using the mechanical keys. The authorized person such as the employees only should have the smart card to be used to scan when entering the places which contain importance information.

2.1.5 Challenges Of Information management In Organization:

In implementing the information management in organization several issues and challenges about this has been found. This issues and challenges have resulted the information management that will be implemented delayed. There are several issues or challenges that have been found in implementing the information system in the organization.

2.1.5.1 Failure to understand about Information management :

In order to handle the importance information in organization, the employees must have the understanding about the information management in their organization. As the employees need to the level of manage education and knowledge within their organizations, the employees must know what is the policies that they need to follow, the types of information’s they control, how to find the services the customers need and so on. The ultimate objective is to let the business units share in information system risk management.

The information management intelligence is a function of visibility in the organization. But nowadays, not so many people concern about the information system . They deliberately post about the fake information about the organization on their social media which can lead to the damages of the organization. They do not think about the effect of such posting on the internet. Part of raising awareness involves personalizing risks for managers, showing them how vulnerabilities could affect them as individuals and also organizations (Johnson & Goetz, 2007).

2.1.5.2 Mobile Workforce and Wireless Computing:

One of the most frequently challenges was the mobile workforce and wireless computing. Nowadays, there are so many types of smart phones located in the market. These smart phones provide the wireless connection to the internet. The arrival of mobile computing devices had made a significant impact on people's everyday life. Wireless communications release the employees and consumers from relying on phone lines to communicate. With the convergence of these devices, the information on them need to be protected because it may be contain the confidential information about the organizations as employees use it to perform the business activities on their mobile devices. A long time ago, all the organizations work was being done using the company's computers and only can be used on the company. But nowadays, all the works can be done using the mobile device. The information such as name, address, phone numbers and all other personal data can be trace by other people easily just by using the mobile devices. The employees must know that the company's computer has been provided with the anti-viruses that they cannot get it for their mobile devices. So, the organizations must take a serious way and careful considerations when handling with the wireless devices.

2.1.5.3 Shortage of Information Security Staff:

Finding a qualified information security staff is a difficult task, which will likely continue to be the case in the near future. The organization has not had the time to grow the staff necessary for these roles. In addition, the information security challenges keep growing at a rapid pace, constantly expanding the list of technology to be deployed, and the information security staff cannot keep up with the emergence of information technology. The organizations need more time and money to get the staff trained on commercially available products. Other than that, the most and greatest challenge in this area is finding a leader who has a broad background in the field and who can pull together an effective information management team in the organizations. The team cannot be operating properly if the leader is also does expert in managing the information system .

2.1.5.4 Information Attacks:

Security incidents that are related to malicious code such as worms, viruses, and Trojans have grown from slightly to significantly damaging to business operations. A computer virus is a piece of malicious code that attaches to or infects executable programs such as software in the computers. Unlike worms, viruses rely on users to execute or launch an infected program to replicate or deliver their payloads. A virus can delete data or damage system files. This challenge is the commonly happen in any organizations.

2.1.6 The Concept of ISO?

International Standardization Organization Was founded in 1946 (Geneva, Switzerland)Has members representing most countries, both developed and developing Mission is to promote trade by developing international voluntary consensus standards ISO Standard-Setting Process Work is performed through Technical Committees Member countries send delegates to TC proceedings Specific operating rules for standard development and adoption Member countries vote on Committee Draft (CD), Draft International Standards (DIS), and Final Standards (FIS).

2.1.6.1 ISO Standard-Setting Process:

Standards are reviewed / revised every five years Efforts are made to coordinate standards in different fields (e.g. ISO 9000, ISO 14001 and OHSAS 18001, ISO 27001) Purposes of Management Standards Set benchmarks for pro-active management practices Improve performance using voluntary mechanisms Allow for verification to stakeholders Decrease opportunities to “cover-up”

2.1.7 The Concept of ISO 27001?

2.1.7.1Definition:

ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISM is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information management system."

2.1.7.2 The specification defines a six-part planning process:

1) Define a security policy.
2) Define the scope of the ISMS.
3) Conduct a risk assessment.
4) Manage identified risks.
5) Select control objectives and controls to be implemented.
6) Prepare a statement of applicability.

The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organization.

The 27001 standard does not mandate specific information controls, but it provides a checklist of controls that should be considered in the accompanying code of practice, ISO/IEC 27002:2005. This second standard describes a comprehensive set of information control objectives and a set of generally accepted good practice controls .

2.1.7.3 ISO 27002 contains 12 main sections:

1) Risk assessment.
2) Security policy.
3) Organization of information management .
4) Asset management.
5) Human resources security.
6) Physical and environmental management .
7) Communications and operations management.
8) Access control.
9) Information systems acquisition, development and maintenance.
10) Information incident management.
11) Business continuity management.
12) Compliance.

Organizations are required to apply these controls appropriately in line with their specific risks. Third-party accredited certification is recommended for ISO 27001 conformances.

2.1.7.4Other standards being developed in the 27000 family are:

1) 27003 – Implementation guidance.
2) 27004 - An information management measurement standard suggesting metrics to help improve the effectiveness of ISMS.
3) 27005 – An information security risk management standard. (Published in 2008)
4) 27006 - A guide to the certification or registration process for accredited ISMS certification or registration bodies. (Published in 2007)
5) 27007 – ISMS auditing guideline.
6) 27001:2013- ISO/IEC Information technology - Security techniques -I27001:2013- ISO/IEC Information technology - Security techniques -Information security management systems – Requirements
7) Information security management systems –Requirements

2.1.8 The Concept of ISO 27001:2013:

ISO 27001 is a widely used international standard that specifies requirements for information management systems. Based on periodic risk evaluation, this standard provides a method for assessing systems that manage company and customer information.

2.1.8.1Contents of ISO 27001-2013:

2.1.8.1 Foreword:

ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2. The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote. Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent righties/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques. This second edition cancels and replaces the first edition (ISO/IEC 27001:2005), which has been Technically revised. **The clauses of ISO /IEC 27001:2013 are:**

0. Introduction

0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information management system. The adoption of an information management system is a strategic decision for an organization. The establishment and implementation of an organization's information management system is influenced by the organization's needs and objectives, system requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time. The information management system preserves the confidentiality, integrity and availability of information by applying a management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information management system is part of an integrated with the organization's processes and overall management structure and that information management is considered in the design of processes, information systems, and controls. It is expected that an information management system implementation will be scaled in accordance with the needs of the organization. This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information management requirements. The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only. ISO/IEC 27000 describes the overview and the vocabulary of information management systems, referencing the information management system family of standards (including ISO/IEC 27003.

ISO/IEC 27004and ISO/IEC 27005), with related terms and definitions.

0.2 Compatibility with other management system standards:

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO

Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for t hose organizations that choose to operate a single management system that meet the requirements of two or more management system standards . Information technology — Security techniques —

0.3 Information management systems — Requirements:

1. Scope :

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information management risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4to 10is not acceptable when an organization claims conformity to this International Standard .

2. Normative references :

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced\ document (including any amendments) applies.

3. Terms and definitions :

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4. Context of the organization :

4.1. Understanding the organization and its context :

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information management system.

NOTE: Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009

4.2. Understanding the needs and expectations of interested parties:

The organization shall determine:

a) Interested parties that are relevant to the information management system; and
b) The requirements of these interested parties relevant to information system.

NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3. Determining the scope of the information management system:

The organization shall determine the boundaries and applicability of the information management system to establish its scope.

When determining this scope, the organization shall consider:

a) The external and internal issues referred to in 4.1;
b) The requirements referred to in 4.2; and
c) Interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

4.4. Information management system:

The organization shall establish, implement, maintain and continually improve an information management system, in accordance with the requirements of this International Standard.

5. Leadership :

5.1. Leadership and commitment :

Top management shall demonstrate leadership and commitment with respect to the information management system by:

a) Ensuring the information management policy and the information management objectives are established and are compatible with the strategic direction of the organization;
b) ensuring the integration of the information management system requirements into the organization’s processes;
c) ensuring that the resources needed for the information management system are available;

d) communicating the importance of effective information management and of conforming to the information management system requirements;

e) ensuring that the information management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information management system;

g) promoting continual improvement; and

h) Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2. Policy:

Top management shall establish an information policy that:

a) is appropriate to the purpose of the organization;

b) includes information management objectives (see 6.2) or provides the framework for setting information objectives;

c) includes a commitment to satisfy applicable requirements related to information management ; and

d) Includes a commitment to continual improvement of the information management system.

The information management policy shall:

e) be available as documented information;

f) be communicated within the organization; and

g) Be available to interested parties, as appropriate.

5.3. Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information management are assigned and communicated.

Top management shall assign the responsibility and authority for:

a) ensuring that the information management system conforms to the requirements of this International Standard; and

b) Reporting on the performance of the information management system to top management.

NOTE: Top management may also assign responsibilities and authorities for reporting performance of the information management system within the organization.

6. Planning:

6.1. Actions to address risks and opportunities

6.1.1. General

When planning for the information management system, the organization shall consider the issues referred to in 4.1and the requirement s referred to in 4.2and determine the risks and opportunities that need to be addressed to:

a) ensure the information management system can achieve its intended outcome(s);
b) prevent, or reduce, undesired effects; and
c) Achieve continual improvement.

The organization shall plan:

d) Actions to address these risks and opportunities; and
e) How to
1) integrate and implement the actions into its information management system processes; and
2) Evaluate the effectiveness of these actions.

6.1.2. Information risk assessment:

The organization shall define and apply an information risk assessment process that:

a) establishes and maintains information risk criteria that include:
1) the risk acceptance criteria; and
2) criteria for performing information risk assessments;
b) ensures that repeated information risk assessments produce consistent, valid and comparable results;
c) identifies the information management risks:
1) apply the information risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information management system; and
2) identify the risk owners;
d) Analyses the information risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2c) 1) were to materialize;
2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2c) 1); and
3) determine the levels of risk;

e) Evaluates the information risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2a); and
2) Prioritize the analyzed risks for risk treatment.

The organization shall retain documented information about the information risk assessment process.

6.1.3. Information risk treatment

The organization shall define and apply an information risk treatment process to:

a) select appropriate information risk treatment options, taking account of the risk assessment results;
b) determine all controls that are necessary to implement the information risk treatment option(s) chosen;

NOTE: Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 1: Annex Contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.

NOTE 2: Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex Aare not exhaustive and additional control objectives and controls may be needed.

d) Produce a Statement of Applicability that contains the necessary controls (see 6.1.3b and c) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
e) formulate an information security treatment plan; and
f) Obtain risk owners' approval of the information risk treatment plan and acceptance of the residual information risks.

The organization shall retain documented information about the information risk treatment process.

NOTE: The information risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000.

6.2. Information management objectives and planning to achieve them:

The organization shall establish information management objectives at relevant functions and levels.

The information management objectives shall:

a) consistent with the information management policy;
b) be measurable (if practicable);
c) take into account applicable information system requirements, and results from risk assessment and risk treatment;
d) be communicated; and
e) Be updated as appropriate.

The organization shall retain documented information on the information management objectives. When planning how to achieve its information objectives, the organization shall determine:

f) What will be done;
g) What resources will be required;
h) Who will be responsible;
i) When it will be completed; and
j) How the results will be evaluated.

7. Support:

7.1. Resources:

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information management system.

7.2. Competence:

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information system performance;
b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
d) Retain appropriate documented information as evidence of competence.

NOTE Applicable actions may include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.

7.3. Awareness:

Persons doing work under the organization's control shall be aware of:

a) the information management policy;
b) their contribution to the effectiveness of the information management system, including the benefits of improved information performance; and
c) The implications of not conforming to the information management system requirements.

7.4. Communication:

The organization shall determine the need for internal and external communications relevant to the information management system including:

a) on what to communicate;
b) when to communicate;
c) with whom to communicate;
d) who shall communicate; and
e) The processes by which communication shall be effected.

7.5. Documented information:

7.5.1. General :

The organization's information management system shall include:

a) Documented information required by this International Standard; and
b) Documented information determined by the organization as being necessary for the effectiveness of the information management system.

NOTE: The extent of documented information for an information management system can differ from one organization to another due to:

1) the size of organization and its type of activities, processes, products and services;
2) the complexity of processes and their interactions; and

3) The competence of persons.

7.5.2. Creating and updating:

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);
b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
c) Review and approval for suitability and adequacy.

7.5.3. Control of documented information:

Documented information required by the information management system and by this International Standard shall be controlled to ensure:

a) It is available and suitable for use, where and when it is needed; and
b) It is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and
f) retention and disposition

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information management system, shall be identified as appropriate, and controlled.

NOTE: Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8. Operation:

8.1. Operational planning and control:

The organization shall plan, implement and control the processes needed to meet information requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information objectives determined in **8.2** The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

8.2. Information risk assessment:

The organization shall perform information risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2a).

The organization shall retain documented information of the results of the information risk assessments.

8.3. Information risk treatment:

The organization shall implement the information risk treatment plan.

The organization shall retain documented information of the results of the information risk treatment.

9. Performance evaluation:

9.1. Monitoring, measurement, analysis and evaluation:

The organization shall evaluate the information performance and the effectiveness of the information management system.

The organization shall determine:

a) what needs to be monitored and measured, including information processes and controls;
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE: The methods selected should produce comparable and reproducible results to be considered valid.

a) When the monitoring and measuring shall be performed;
b) Who shall monitor and measure;
c) When the results from monitoring and measurement shall be analyzed and evaluated; and

d) Who shall analyze and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9.2. Internal audit:

The organization shall conduct internal audits at planned intervals to provide information on whether the information management system:

a) conforms to
    1) the organization's own requirements for its information management system; and
    2) the requirements of this International Standard;

b) Is effectively implemented and maintained.

The organization shall:

a) Plan, establish, implement and maintain an audit programmer(s), including the frequency, methods, and responsibilities, planning requirements and reporting. The audit programmer (s) shall take into consideration the importance of the processes concerned and the results of previous audits;

b) define the audit criteria and scope for each audit;

c) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

d) ensure that the results of the audits are reported to relevant management; and

e) Retain documented information as evidence of the audit programmer(s) and the audit results.

9.3 Management review:

Top management shall review the organization's information management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information management system;

c) feedback on the information performance, including trends in:
    1- nonconformities and corrective actions;
    2- monitoring and measurement results;

    3- audit results; and
    4- fulfillment of information management objectives;

d) feedback from interested parties;
e) results of risk assessment and status of risk treatment plan; and
f) Opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information management system.

The organization shall retain documented information as evidence of the results of management reviews.

10 Improvements:

10.1 Nonconformity and corrective action

When nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:
    1- take action to control and correct it; and
    2- deal with the consequences;

b) Evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
    1- reviewing the nonconformity;
    2- determining the causes of the nonconformity; and
    3- determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;
d) review the effectiveness of any corrective action taken; and
e) Make changes to the information management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

f) The nature of the nonconformities and any subsequent actions taken, and
g) The results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information management system.

2.2 Section Two : Organizational Performance :

2.2.1 Introduction :

Management books are full of phrases such as organizational effectiveness, organizational efficiency, organizational alignment, and numerous others. So when we speak of ‘organizational performance’, what is it that we are speaking about? First, we’ll refer to the Oxford dictionary which defines ‘organization’ as “an organized group of people with a particular purpose”. ‘Performance’ is defined to include “the action or process of performing a task or function seen in terms of how successfully it is performed”. When these definitions are put together, we can say organization performance relates to how successfully an organized group of people with a particular purpose perform a function. Essentially, this is what we are speaking about when we refer to organizational performance and achievement of successful outcomes.

We now have a definition but what does it really mean? High organizational performance is when all the parts of an organization work together to achieve great results with results being measured in terms of the value we deliver to customers. These parts are:

1) Strategic objectives – provide the direction in which everyone within the organization should head. They provide focus and ensure we are all working towards the same end.
2) Organizational structure – this represents the form in which the organization will deliver its services. The structure must support the strategy just as the strategy must have regard to the structure. For instance, an on-line delivery strategy will not be successfully executed unless the organization has on-line capabilities.
3) Business performance measures – represent the measures by which each area of the organization will be assessed. There is no single set of measures that may be applied across all organizations. In order to be relevant and of use to the organization, the measures must be determined in light of the organization’s goals and the strategies put in place to achieve those goals. It is this measurement process that will direct behavior more than any other system that may be put in place. Further, the information must be easily obtainable - in a timely manner. This requires the management information systems to be developed to collect the right data in an efficient way.

4) Allocation of resources and processes – relates to the decision making approach that takes place within the organization. It is how the organization goes about deciding where to apply its scarce resources – including money, time and effort - in order to achieve its objectives.
5) Values, culture and guiding principles – this part is unique to the organization. If the organization was human, this would be its DNA. The culture must support the achievement of the strategic objectives in order to draw out the "best" of people. The values and guiding principles must support the purpose (remembering from our earlier definition that an organization is an organized group of people with a particular purpose) for achievement of desired outcomes.
6) Reward structures – must reinforce the culture and direct efforts to support the achievement of strategic objectives. Reward structures may include various forms – monetary (for example, bonus on achievement of short term goals), promotion (recognition of having acquired certain skills), celebration event (recognizing and congratulating team efforts), leave of absence / day off (recognition and 'thank you' for a job well done), and so on.

All these parts are inter-related and a change to one will impact one or more of the others. Similarly, one poor performing part will potentially negatively impact the others and lead to less than successful results. So, what is organizational performance? It's getting all of these parts to work in harmony in order to achieve great results.

2.3Section Three : Previous Studies

1) Does ISO 27001 implementation satisfy EU GDPR requirements:

European General Data Protection Regulation

ISO 27001 is a framework for information protection. According to GDPR, personal data is critical information that all organizations need to protect. Of course, there are some EU GDPR requirements that are not directly covered in ISO 27001, such as supporting the rights of personal data subjects: the right to be informed, the right to have their data deleted, and data portability. But, if the implementation of ISO 27001 identifies personal data as an information system asset, most of the EU GDPR requirements will be covered.

In addition to the adopted technical controls, structured documentation, monitoring, and continuous improvement, the implementation of ISO 27001 promotes a culture and awareness of management incidents in organizations. The employees of these organizations are more aware and have more knowledge to be able to detect and report security incidents. Information management is not only about technology; it’s also about people and processes.

The ISO 27001 standard is an excellent framework for compliance with the EU GDPR. If the organization has already implemented the standard, it is at least halfway toward ensuring the protection of personal data and minimizing the risk of a leak, from which the financial impact and visibility could be catastrophic for the organization. The first thing an organization should do is conduct an EU GDPR GAP Analysis to determine what remains to be done to meet the EU GDPR requirements, and then these requirements can be easily added through the Information Management System that is already set by ISO 27001. **(Bouca Carla, 2016)**

2) Information management and Organizational:

This study was conducted to analyze the effect of information management activities on organizational performance. With this in mind and with the aim of resolving transaction stability in the securities industry, using an organization’s management activities as a tool for carrying out information activities, the effect of activities on organizational performance was analyzed. Under the assumption that the effectiveness of information activity scan be bolstered to enhance organizational performance, such effects were analyzed based on Herzberg’s motivation theory, which is one of the motivation theories that may influence information protection activities. To measure the actual attributes of the theoretical model, an empirical survey of the securities industry was conducted. In this explorative study, the proposed model was verified using partial least squares as a structural equation model consisting of IT service, information management , information sharing, transaction stability, and organizational performance.

(Korean Securities Industry, 2013)

3) Evaluating the effectiveness of ISO 27001:2013 based on Annex A:

The part of the management system of an organization dealing with information system is called Information Management System . The most adopted ISO standard 27001:2005. The 2005 version of the standard has been updated in 2013 to provide more clarity and more freedom in implementation, based on practical experiences. This paper compares ISO 27001:2005 and the updated 2013 standard based on Annex A controls. We classify the controls into five categories of data, hardware, software, people and network. All of the controls defined in Annex A, regardless of their objectives, can easily be allocated to at least one of these categories. Classifying the controls to known categories offers an integrated view of the updated standard and presents a suitable guide for evaluating the performance and efficiency of the updated standard.

(**Saberi Iman , 2014)**

4) Implementation of Information Management Systems based on the ISO/IEC 27001 Standard in different cultures:

In this thesis, we investigate the potential relationship between national cultural, political and economic characteristics regarding the adoption of ISO 27001, in terms of the average number of certificates issued (2006{2014). ISO 27001 is the most adopted international ISMS (Information Management System) standard, which provides IT governance by protecting sensitive data in a structured way. Although ISO 27001 is a generic standard for all organizations and countries, some countries have yet to adopt ISO 27001 extensively. The relationship between culture (mind-set and behavior) and the adoption of an ISMS standard such as ISO 27001 has not been investigated yet. Based on our qualitative analysis, we observe a relationship between national cultural characteristics of a country and the number of issued ISO 27001 certificates. In our quantitative analysis, we separate countries into two groups based on the average number of the total ISO 27001 certificates that were issued worldwide (2006{2014). A common comparison approach may not be helpful for investigating the relationship between the adoption of ISO 27001 and the national cultural, political and economic characteristics of several countries from different continents. For countries with more than the average number of the ISO 27001 certificates issued worldwide (2006{2014), we observe a relationship between the regulation density (regulation of credit, labor, and business), GDP (Gross Domestic Product; a monetary measure of a country's economy and economic performance that equalizes the purchasing power of different currencies divided by population), and the average degree of comfortableness with uncertainty of people in a country on one side, and the adoption of ISO 27001 on the other side. For countries with less than the average number of the ISO 27001 certificates issued worldwide (2006{2014), we observe a relationship between the average degree of individualism of people in a country, the GDP, and the relation to authority and the expected level of hierarchical order of people in a country on one side, and the adoption of ISO 27001 on the other side. The correlation does not imply causality in this thesis.(**Shojaie Bahareh , 2018)**

5) ISO27001:2013 one year on – What has changed? Part two:

Certainly for most organizations that already had an established corporate risk regime, the requirement for a detailed asset-based information risk assessment was not compatible and there would be little or no appetite to work through a much more resource intensive methodology purely for a single discipline such as information system . Similarly, for those organizations that had not been convinced of the need for a corporate risk management process, any case for a resource intensive asset-based method was likely to fail from the outset unless there was a truly impelling case for certification, and then it would be a case of identifying the least amount of work required to scrape the certification bar.

The 2013 requirements are much less prescriptive and thus lend themselves to integration with a corporate regime much more easily. Meeting these requirements can also be much less resource-demanding than satisfying the 2005 criteria for those adopting an information management risk method as their first foray into risk management. Using this flexibility to align the '2013-compliant' risk method with the wider corporate risk assessment enables the organization to keep information management risks – and the resources required to deliver it – in perspective when compared to other business disciplines. Yes, there are certain schemes that require an asset-based approach and personally I still see it as the gold standard for information management risk assessments, but the flexibility offered in ISO 27001:2013 means that a blended mix of an alternative, corporate-savvy approach together with an asset-based method targeted to certain systems and activities is acceptable.

(Watkins Steve , 2014)

6) Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing:

Cloud Computing provides a scalable, high availability and low cost services over the Internet. The advent of newer technologies introduces new risks and threats as well. Although the cloud has a very advanced structures and expansion of services, but security and privacy concerns have been creating obstacles for the enterprise to entirely shift to the cloud. Therefore, both service providers and clients should build an information management system and trust relationship with each other. In this research paper, we analyzed most widely used international and industry standard (ISO/IEC 27001:2013) for information management to know its effectiveness for Cloud Organizations, each control importance factor for on-premises, IaaS, PaaS and SaaS, and identify the most suitable controls for the development of SLA based Information management Metrics for each Cloud Service Model. We generically evaluated ibid standards control objectives without considering Cloud organization size, nature of work, enterprise size. To know effectiveness, relevance to Cloud Computing, factor of standard control objectives for the in-house or in a public cloud, we defined a quantitative metric. We come to the conclusion that ISO / IEC 27001:2013 compliance improves service providers and customer's information management system and build a trust relationship but not fulfill all requirements and cover all relevant issues.**(Conference at Roma ICISSP, 2016)**

7) Role of standards 27001-2013 :

Risk management in international standards ISO/IEC 27000 series update Information management requirements:

Information management requirements It is essential that an organization identifies its management requirements. There are three main sources of system requirements:

a) Assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;
b) legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;

set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations. It is essential that an organization identifies its security requirements.

(Naganuma **Miho, 2017)**

8) Investigating Roles of Information management Strategy:

A fundamental understanding of the complexities comprising an information management

Strategy IMS in an organization is lacking. Most IMS implementations in government

Organizations equate anti-virus or installing a firewall to that of an IMS. While use of hardware and software forms a good defense; neither comprises the essence of an IMS. The IMS best integrates with business and information system strategies from the start, forming and shaping the direction of overall strategy synergistically within large government organizations. The researcher used grounded theory and investigated what a large government organization's choices was with the differing roles an information management professional (IMP) chooses to operate with and to develop an information management program. Analysis of the data collected from interviewing 32 chief information management officers (CISOs) revealed how CISOs viewed their programs, aligned their goals in the organization, and selected role(s) to execute strategy.

Use of grounded theory coding practices of the interviews showed a deficit in complexities of an IMS and a lack of an IMS in the majority of organizations. The participants came from multiple organizations in the National Capital Region on the east coast of the United States. This study advances the body of knowledge in a qualitative understanding of actions taken by CISOs to select a direction towards IMS implementation, role selection, and development of information management programs. It provides a theory for further testing of strategy development and role maturity.**(Nova Southeastern University,2015)**

9) **(James Louise , 2012)**

We advanced a contract-based argument to understand how firms can efficiently relate to external actors. Stakeholder contracting helps firms overcome market failures and information disclosure problems. It is the stakeholder conjoint effect that matters, and developing the right combination of stakeholder contracts can be a source of sustainable competitive advantage among domestic firms in emerging economies.

We learn from our Brazilian data that firm contracts with at least both government and community showed a positive impact on firm performance. Powerful external factors, such as the government, may provide protection and privileged information. Along with investments in community contracts, firms may benefit from superior access to both public and private financing, a crucial variable for firm performance in hostile emerging market environments.

Our study also informs managerial practice. Managers should consider that any decision of investing in stakeholder relationships need to take into account how different combinations of 'firm stakeholder contracts' impact firm performance. Strategy research would benefit from focusing on resource acquisition issues and how stakeholders can serve as valuable suppliers. We hope future research may benefit from these insights in search for a better understanding of the strategy phenomena and firm performance in emerging economies.

10) **(Thomason Marcus and Wallin Johanna , 2013)**

According to Sörqvist (2001) there is a correlation between quality and profitability where high quality results in better profitability‹by increasing the product quality in a company, the revenue can increase due to that a higher price can be charged for the products (Sörqvist , 2001). Further, thecosts will decrease through reduction of waste in the production, the re-work and scrap is reduced since the products are flawless directly (Ehresman, 1997). Or, as stated by Deming (2000), the product is produced correctly the first time. Moreover, the capital tied up in assets decrease not only because of less need ofbuffers between work centers and spare parts, but also through higher utilization of facilities due to less re-work and decreased need of control (Sörqvist, 2001). Bergman and Klefsjö (2010) also emphasizes that decreased capital tied up in assets result in increased profitability, but further sees two other positive outcomes; larger profit margins for the company and increased market shares and thereby the profitability in a long-term perspective (Sumanth& Arora,1992).

Feigenbaum (1991) adds the positive cash flow as a consequence of improved quality for the company, while Harrington (1987) discusses the relationship between quality and profitability, emphasizing that in order to increase a profit of a company it is better to improve the quality than increasing the sales. The reason is that increased sales require more resources such as more equipment, more materials, more floor space and more support employees, which detracts from the earned money. Instead, savings through quality improvements are often directly connected with increased profit creating possibility to continue investing in improved quality and better products (Harrington, 1987).

Further, Merino (1988) states that improved quality results in better communication in the organization together with improved communication with its customer. Juran was in year 1951 the first to discuss costs associated with poor quality and how it affects the company, while Feigenbaum five years later was the first to classify these costs into categories (Tsai, 1998). Over the years, many different expressions have been used such as poor-quality cost and quality costs, but as explained by Bergman and Klefsjö (2010) these are not good terms giving the impression that high quality costs, while it in fact is lack of poor quality that costs. Bergman and Klefsjö (2010) therefore advice to use the term Cost of Poor Quality(CoPQ) that will be used throughout this master thesis as a generic name for all costs associated with poor quality. Sörqvist (2001, p31) defines CoPQ as "the total losses caused by the products and processes of a company not being perfect". Harrington (1987, p 5) on the other hand defines CoPQ as "all the cost incurred to help the employee do the job right every time and cost of determining if the output is acceptable, plus any cost incurred by the company and the customer because the output did not meet specifications and/or customer expectations".

Failure costs are costs connected to the consequence of failure of meeting the requirement in the company and with the customer. The failure costs are divided into internal failure costs and external failure costs (Campanella, 1990). The internal and external failure costs are similar but differ in terms of that the internal failure costs include poor quality inside the company while the external failure costs include poor quality outside the company (Gryna,1999). Further, the internal failure cost will only affect the company's organization while external failure costs cause problems for the customer in terms of inadequate products or services (Harrington, 1987).

Explained by Hwang and Aspinwall (1996) the PAF-model can further be divided into a macro and micro model. The macro model is based on the external customer and supplier relationship of an organization (Hwang & Aspinwall, 1996), while the micro model focuses on the internal customer and supplier within a department or process. The micro model is similar to the macro model with the distinction that the whole organization is broken down in departments and section previous application (Winchell & Bolton, 1987).

Furthermore, the classification of CoPQ by Juranand De Feo (2010) is based on the PAF-model but with an important difference; the prevention and appraisal costs are excluded and appraisal and inspection costs are added, see figure 3.5.

The appraisal and inspection costs refer to what Feigenbaum (1991) classified as appraisal costs, since inspection costs are included in the category. Further, Juran and De Feo (2010) exclude prevention costs in the classification but do not further elaborate on why. However, Sörqvist(2001) excludes the prevention costs since these costs are not considered to be a cost due too poor quality but an investment for good quality.

Figure 3.5 - The classification of Co PQ according to Juran and De Feo (2010) Gryna (1999) expands the original view of internal and external failure costs by dividing the internal failure costs into internal failure to meet customer requirements and costs of inefficient processes, whereas the external failure costs are divided into external failure to meet customer requirements and lost CoPQ Appraisal and inspection costs Internal failure costs External failure costs 20 opportunity costs. However, it is not clarified why internal and external failure costs are divided into subcategories, see figure **3.6.**

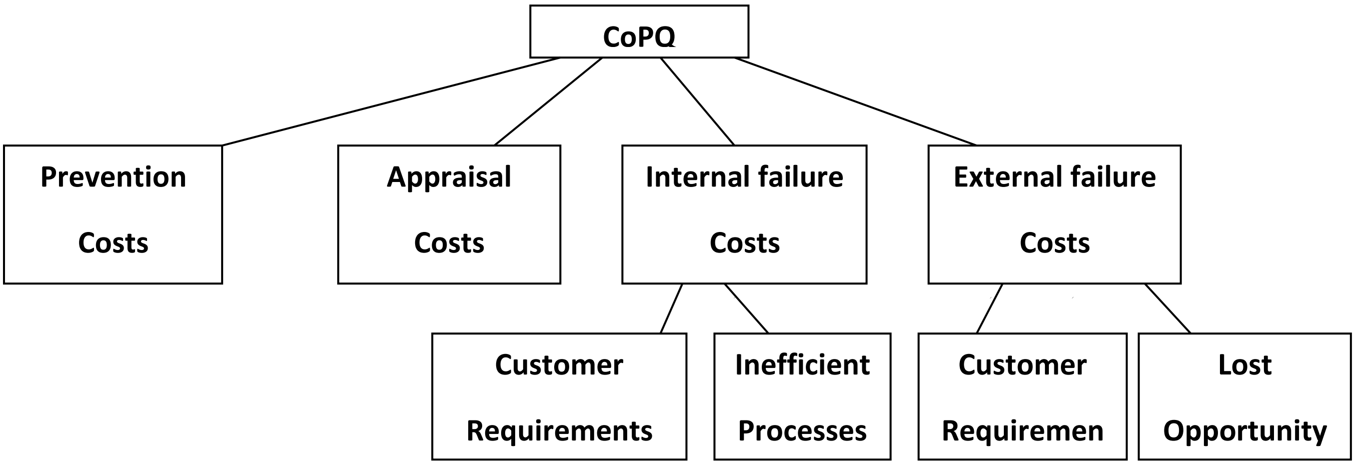


Figure (3.6) the classification of Co PQ according to Gryna (1999)

The similarities and differences between previous and current studies:

The previous study shows the paucity or scarcity of local studies related to the role of the information management system in the development of the performance of the institution , the researcher found through the search for previous studies that the researchers focused on the implementation of the standard ISO 27001:2013 that's talking about the information management system, but there is still a gap between implementation of the standard and the development of institutional performance .

The current study discussed the dimensions of the information management system through the application of the standard and its direct impact on the progress or deterioration of companies, so when managed effectively, it allows companies to work with the confidence of stakeholders and customers in that their data is well protected, The enterprise further growth and renewal and expand customer base.

From previous studies, some important points can be noted about the information management system and should be taken into account such as:

1. All previous studies are consistent with the application of the standard ISO 27001:2013 but not effectively. Evidence of this is that there is no significant improvement in performance, which helps to continuously improve institutions in terms of risk perception before they occur.
2. The researcher found that the application of the standard in some previous studies did not lead to increasing the institutional profitability of the stakeholders, which leads to the failure to comply with their requirements and get their satisfaction.
3. Previous studies have differed in their ability to avoid financial losses and reduce waste time in spite of their application to the information security management system. This may be due to the different environment and field of previous studies.
4. Based on the above, we note that the previous studies differed in addressing their topics at the Arab and foreign levels, and we find that this study is complementary to those studies in terms of clarifying the positive relationship between the application of the information management system and its ability to develop the performance of the institution and increase the institutional awareness of all employees on different Administrative and executive levels of the importance of the role of information management and what are the negative consequences of not complying with this.

Chapter Three

Case study and Methodology

Chapter Three

Case Study and Analyses

3.1Section one: Case study

3.1.1 ZAIN Sudan Telecommunications (HQ)

Kuwait City, 15 January 2008. ZAIN Group, the leading mobile telecoms operator across the Middle East and Africa with operations in 22 countries, has announced that they have signed a 3-year 'framework' agreement with DNV (Det Norske Veritas) that will help ensure that Zain's operations in the Middle East and sub-Saharan Africa are fully compliant with the rigorous international ISO standards.

Haitham Al Khaled, Zain's Chief Strategy Officer commented: "ZAIN Group vision is to be a global top ten mobile telecommunications operator by 2011. To be a global leader we have to operate to the highest possible international standards and this agreement sets a global benchmark for our core business processes. Our customers will also benefit from high integrity systems and processes where their financial data is secured to the highest international standards."

He further added "Excellence in all of our operations and functions is fundamental because it not only means that our customers enjoy an unparalleled experience but it also ensures that we will be operating at optimum levels across the entire group of companies. We are delighted to be working with one of the leading accreditation bodies in this field and I am sure that DNV will add immense value to our operations and the service experience of our customers."

ZAIN assessed six world-leading organizations as candidates for the task of helping ensure that their processes and procedures for the 22 ZAIN operations in the Middle East and Africa would effectively gain certification across all critical business areas and functions. There are four certifications that all ZAIN operators will seek to achieve;

- ISO 9001 Quality with TL9000 Telecommunications Leadership
- ISO 14001 Environmental Management System
- ISO 27001 Information Security Management System
- BS 25999 Business Continuity Management

At a signing ceremony held in Kuwait City, representatives from ZAIN and DNV formalized the framework agreement that will prepare ZAIN for ISO certification at each operation.

ZAIN operations in several countries are already ISO certified in a number of areas, but this agreement with DNV provides for a common approach to process and standards assessment, giving high level management visibility across all ZAIN operations in the Middle East and those Group companies in Africa which currently operate under the Celtel brand.

New ZAIN operations such as that in Saudi Arabia which will commence operations this year are already being structured with the certification requirements at the core of the business model and the role of DNV is to ensure compliance with the exacting and stringent requirements of the ISO and Telco Industry recognized standards.

Signing the agreement on behalf of DNV Mr. Torger Baardseth, VP and Middle East Regional Manager said: "This is an important agreement for DNV as ICT and Telecom is one of our main focus areas. DNV will, through this agreement, help ZAIN demonstrate sustainable performance. We look forward to working with ZAIN, a dynamic and fast growing organization, to guarantee quality, success and safety each step of the way".

3.1.2 About ZAIN Sudan:

The country's leading operator was established in 1997 and today serves 12.5 million customers as of 30 December 2016, reflecting a market share of 46%. Possessing the country's most advanced voice and data network, the operator's network extends to an impressive 90% of the population through a total number of 2,465 network sites. Through constant development of the telecommunications infrastructure and proactive marketing initiatives, ZAIN remains committed to offering customers in Sudan the most dynamic products and services. The foundation of ZAIN Sudan's achievements lies in the company's ability to inspire its employees to deliver the best and most imaginative services at every level. With an energetic and inspired predominantly Sudan workforce, the company is committed to employing high caliber people as well as nurturing the finest Sudan talent. With a strong human resources and training program that develops and nurtures leaders in the workplace, the company has consistently opened new doors for its dedicated staff. For more on ZAIN Sudan please visit **(www.sd.zain.com)**

What you will be Accountable to the Technology Risk and Quality team leader Responsible for Apply risks, quality, security standards, processes and procedures and monitor adherence to standards across technology functions in coordination with ZAIN Group and ZAIN Sudan teams.

How you will be required to have:

3.1.3 Technology Risk, Quality & Security:

- Implementation and automation of technology related risk mitigation policies, procedures and processes (incl. Business Continuity & Disaster Recovery), in alignment with corporate risk policies and procedures
- Handle Audit operations to ensure risk framework is applied, correctly and comprehensively
- Awareness for risk mitigation policies, procedures and processes
- Implementation and automation of quality related standards, policies, procedures and processes (e.g. health checks), in alignment with corporate quality functions, according to Group guidelines and best practices (e.g. e TOM, ITIL, etc.)
- Act as the custodian for developed technology quality standards and processes, maintain and improve them
- Audit technology activities so that all relevant procedural/legislative requirements are fulfilled
- Develop templates for tech domains to report on compliance to Quality standards
- Sign off quality check reports
- Apply information technology management related standards, policies, procedures and processes, in alignment with other corporate security functions (e.g. IT security monitoring procedures, ISO 27001, e TOM)
- Responsible of Evaluating RFPs to ensure system requirements are met by vendors
- Audit tech developments projects and operations and ensure compliance with system standards from design to testing Develop templates for technology domains to report on compliance to standards and sign off on system check reports

3.1.4 Knowledge Management (KM):

1) Develop policies and guidelines for knowledge management
2) Support technology teams’ knowledge base section by enabling collection, structuring, sharing, and maintaining know-how, expertise and best practices.
3) Define the information / knowledge hierarchy and collect knowledge requirements from different technology domains.
4) Apply KM solution, identifying requirements for its development and align directly with Enterprise Enabling Applications Development.

5) Create awareness and drive adoption of KM in the technology department (e.g. with incentive structures, inclusion on performance appraisals, or gamification).

6) Support technology Risk and quality team leader on the implementation of strategic vision for the Department.

7) Ensure compliance with all applicable policies & regulatory requirements on Information management .

3.2 Section two: Research Methodology

3.2.1 Introduction:

This chapter extends the theoretical perspective of the three research constructs presented in chapter two, encompassed resource based perspective, and Information management system with organization devolving, competitive advantage relationship is discussed. The conceptual model and the hypothesis concerning the relationships among the constructs are presented. Also describes the methods and procedures used to collect and analyze data include the study design, population, sample size and sampling procedures, data collection and procedures for analysis and presentation.

3.2.2 Population of study

The population was all project teams which consist of Zain company ; (14 Managers , and 28 employees), the number of target population was 42. Sample size calculations were carried out using following formula:

Cranach's alpha method: -

Where reliability was calculated using Cranach's alpha equation shown below:

Reliability coefficient $=\frac{\mathrm{n}}{\mathrm{N}-1} * \frac{1-\text{Total variations questions}}{\text{variation college grades}}$

$$\text{Validity} = \sqrt{\frac{\mathrm{n}}{\mathrm{N}-1} * \frac{1-\text{Total variations questions}}{\text{variation college grades}}}$$

Cranach alpha coefficient = (0.87), a reliability coefficient is high and it indicates the stability of the scale and the validity of the study

Validity coefficient is the square of the islands so reliability coefficient is (0.93), and this shows that there is a high sincerity of the scale and that the benefit of the study.

3.2.3 Sample of study

Approval of the research sample organization was initiated after a meeting with Project Manager. At the meeting we presented our research topic and its purpose and the Project Manager gave feedback and ideas for what they would be interested in finding out through our thesis, his approval was subjected to precede all information as highly confidential and company name must be hidden for published information.

3.2.4 Data collection

To ensure that meaningful data was collected and analyzed, a mixed methodology involving both quantitative and qualitative methods was adapted to this study. As noted from the research approach, aforesaid methods will be used for collection and analyzes the study data. For the phase of initial quantitative instrument, a survey methodology with survey tool of Questionnaire was regarded as appropriate to answer the "What?" , while ISMS assessment Checklist was used to assess the major gaps for the ISMS implementation using certain indicators. The indicator status of the organization was described by compare it to the standard.

Chapter Four

Data Analysis and Discussion

Chapter Four

Data analysis and discussion

4.1 Section one: Data analysis:

4.1.1 Introduction:

In this chapter we show the data analysis for Questionnaires of Managers and employees and discussion of results.

4.1.2 Data analysis for managers

The first topic Field study procedures

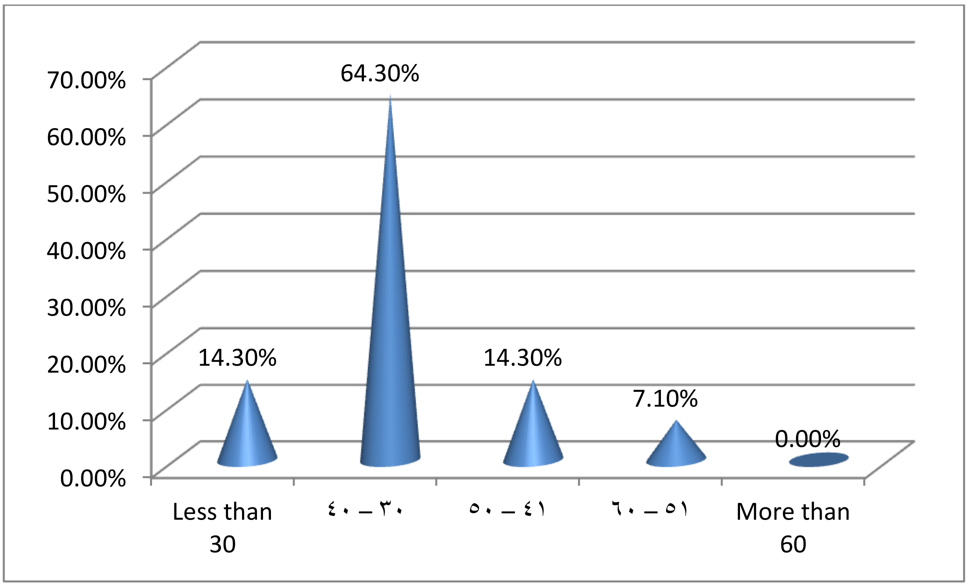
This course deals with the field study procedures under the following sections
First: population and sample of the study

Table (4.1) illustrates the frequency and percentage for Number of age

Value	Frequencies	Percentage
Less than 30	2	14.3%
30 – 40	9	64.3%
41 – 50	2	14.3%
51 – 60	1	7.1%
More than 60	0	0.0%
Total	14	100.0%

Source: IPM SPSS 24 package

Figure (4.1) illustrates the frequency and percentage for Number of age



Source: excel 2016

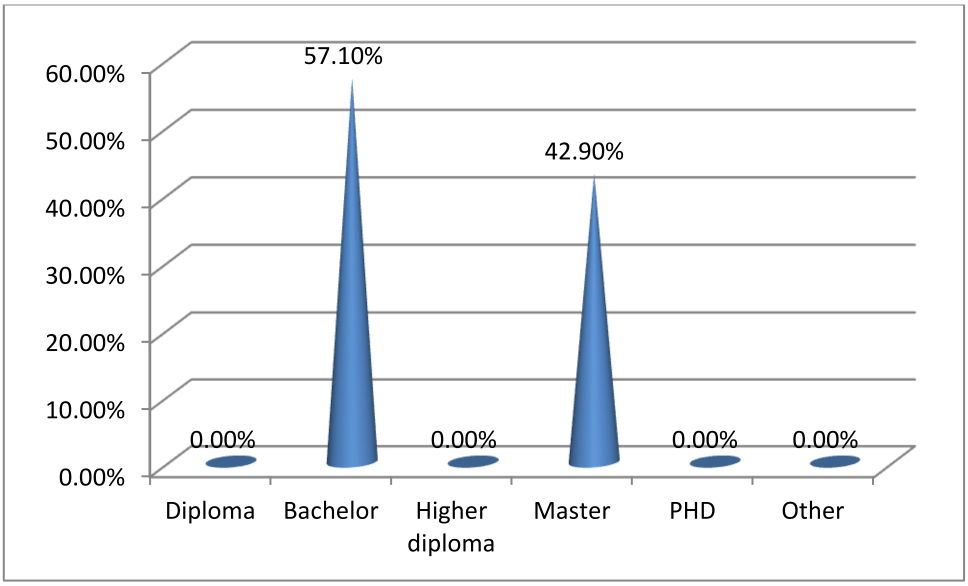
Table (4.1) illustrates the views of the distribution of the age sample by less than 30 years by (%14.3) and 30-40 years by (%64.3) and 41-50 years by (%14.3) and 51 – 60 by (%7.1) and More than 60 by (%0.0).

Table (4.2) illustrates the frequency and percentage for the Qualification

Qualification	Frequencies	Percentage
Diploma	0	0.0%
Bachelor	8	57.1%
Higher diploma	0	0.0%
Master	6	42.9%
PHD	0	0.0%
Other	0	0.0%
Total	14	100.0 %

Source: IPM SPSS 24 package

Figure (4.2) illustrates the frequency and percentage for the Qualification



Source: excel 2016

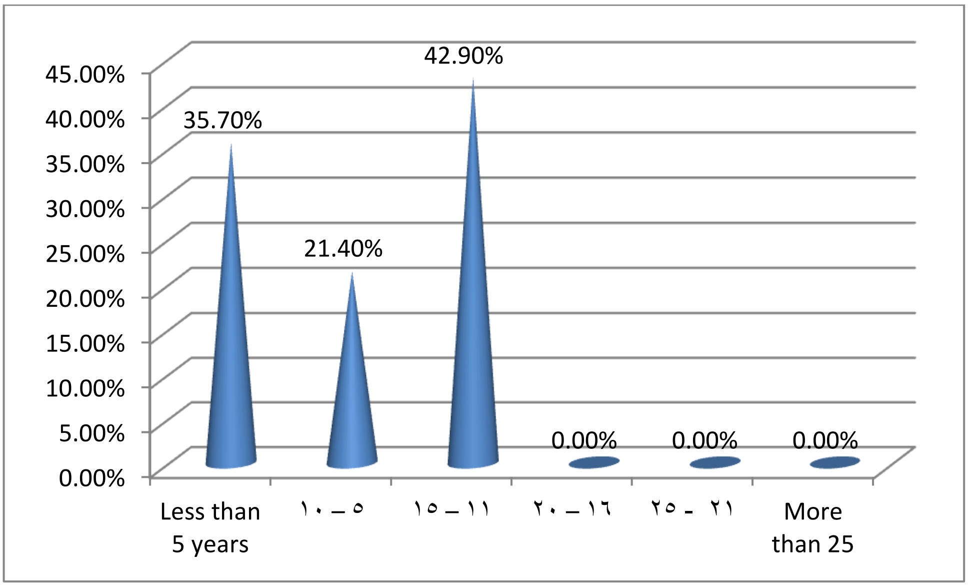
Table (4.2) illustrates the views of the distribution of the Qualification Diploma by (%0.0) and Bachelor by (%57.1) and higher diploma by (%0.0) and Master by (%42.9) and PhD by (%0.0) and other by (%0.0).

Table (4.3) illustrates the frequency and percentage for the How long have you had your current position

work	Frequencies	Percentage
Less than 5 years	5	35.7%
5 – 10	3	21.4%
11 – 15	6	42.9%
16 – 20	0	0.0%
21 - 25	0	0.0%
More than 25	0	0.0%
Total	14	100.0%

Source: IPM SPSS 24 package

Figure (4.3) illustrates the frequency and percentage for the How long have you had your current position



Source: excel 2016

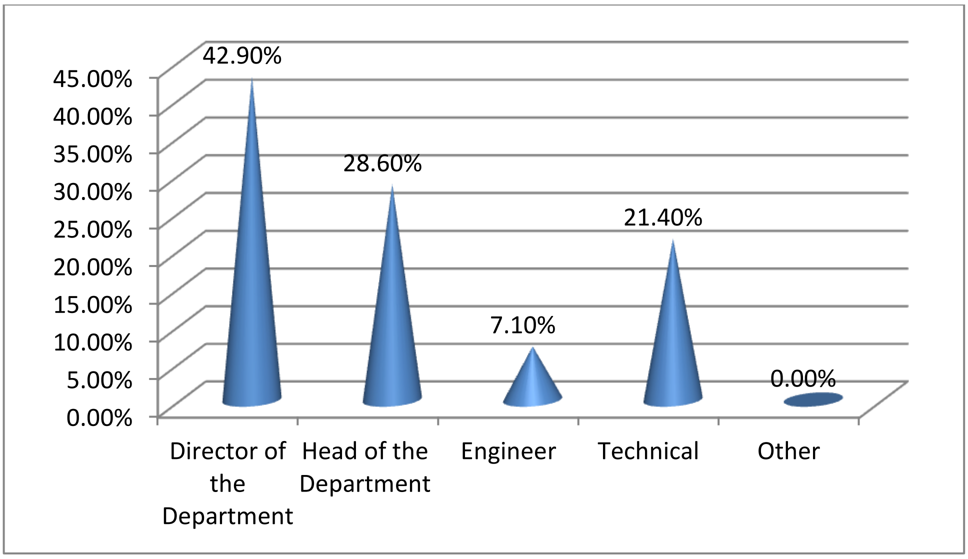
Table (4.3) illustrates the views of the distribution of the How long have you had your current position Less than 5 years by (%35.7) and 5-10 by (%21.4) and 11-15 by (%42.9) and 16-20 by (%0.0) and 21-25 by (%0.0) and More than 25 by (%0.0).

Table (4.4) illustrates the frequency and percentage for what is your position?

Value	Frequencies	Percentage
Director of the Department	6	42.9%
Head of the Department	4	28.6%
Engineer	1	7.1%
Technical	3	21.4%
Other	0	0.0%
Total	14	100.0%

Source: IPM SPSS 24 package

Figure (4.4) illustrates the frequency and percentage for what is your position?



Source: excel 2016

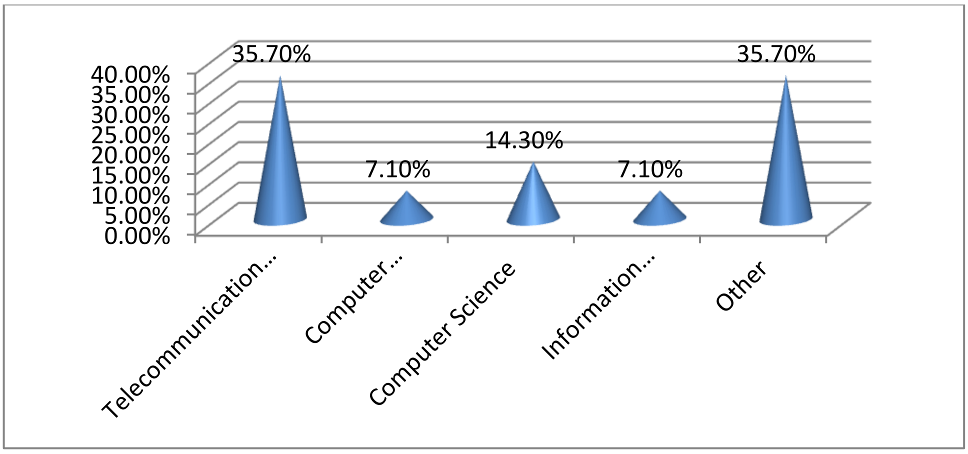
Table (4.4) illustrates the views of the distribution of what is your position Director of the Department by (%42.9) and Head of the Department by (%28.6) and Engineer by (%7.1) and Technical by (%21.4) and other by (%0.0).

Table (4.5) illustrates the frequency and percentage for the Scientific Specialization

Value	Frequencies	Percentage
Telecommunication Engineering	5	35.7%
Computer Engineering	1	7.1%
Computer Science	2	14.3%
Information Technology	1	7.1%
Other	5	35.7%
Total	14	100.0%

Source: IPM SPSS 24 package

Figure (4.5) illustrates the frequency and percentage for the Scientific Specialization



Source: excel 2016

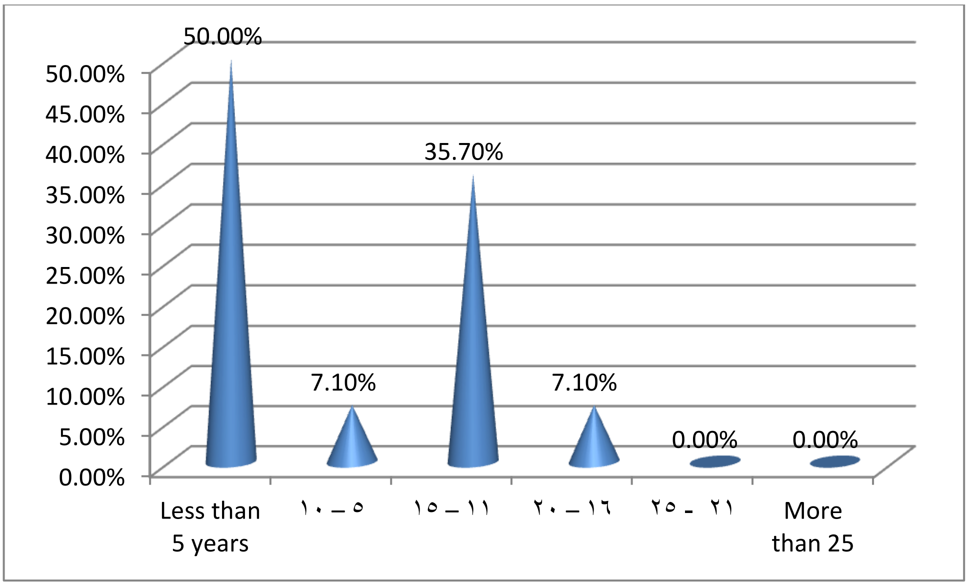
Table (4.5) illustrates the views of the distribution of the Scientific Specialization Telecommunication Engineering by (%35.7) and Computer Engineering by (%7.1) and Computer Science by (%14.3) and Information Technology by (%7.1) and other by (%35.7).

Table (4.6) illustrates the frequency and percentage for the How long have you worked in this organization?

work	Frequencies	Percentage
Less than 5 years	7	50.0%
5 – 10	1	7.1%
11 – 15	5	35.7%
16 – 20	1	7.1%
21 - 25	0	%0.0
More than 25	0	%0.0
Total	14	100.0%

Source: IPM SPSS 24 package

Figure (4.6) illustrates the frequency and percentage for the How long have you worked in this organization?



Source: excel 2016

Table (4.6) illustrates the views of the distribution of the How long have you worked in this organization Less than 5 years by (%50.0) and 5-10 by (%7.1) and 11-15 by (%35.7) and 16-20 by (%7.1) and 21-25 by (%0.0) and More than 25 by (%0.0).

Second: reliability and validity

Cranach's alpha method: -

Where reliability was calculated using Cranach's alpha equation shown below:

$$\text{Reliability coefficient} = \frac{\mathrm{n}}{\mathrm{N-1}} * \frac{1 - \text{Total variations questions}}{\text{variation college grades}}$$

$$\text{Validity} = \sqrt{\frac{\mathrm{n}}{\mathrm{N-1}} * \frac{1 - \text{Total variations questions}}{\text{variation college grades}}}$$

Cranach alpha coefficient = (0.87), a reliability coefficient is high and it indicates the stability of the scale and the validity of the study

Validity coefficient is the square of the islands so reliability coefficient is (0.93), and this shows that there is a high sincerity of the scale and that the benefit of the study.

(4.7) Cranach's alpha method

No	Value	reliability	Validity
1	The organization's leadership commitment to the ISO 27001:2013 demonstrated by	0.91	0.95
2	Roles , responsibilities and authorities	0.92	0.96
3	Access control	0.89	0.94
4	General Questions	0.90	0.95
5	Supplier relationship	0.91	0.95
6	Complains	0.91	0.95
7	Management responsibilities to employment	0.92	0.96
8	Human resources management	0.93	0.96
9	ISO resources , competence Awareness and communication	0.89	0.94
10	Risks and opportunities of ISMS implementation , assessment and treatment of information risk management	0.91	0.95
Total		0.91	0.95

Source: IPM SPSS 24 package

The second subject View and analyze data

Table (4.8) illustrates the frequency and percentage for the organization’s leadership commitment to the ISO 27001:2013 demonstrated b

No	**Items**	**Yes**	**No**	**Other**
1	Do Information Security policy exist	14	0	0
		100.0	0.0	0.0
2	Are all policies approved by management	14	0	0
		100.0	0.0	0.0
3	Are policies properly communicated to employees	13	1	0
		92.9	7.1	0.0
4	Is there establishing the information policy and objectives, in consideration of the strategic direction of the organization, and in promotion of continual improvement	14	0	0
		100.0	0.0	0.0
5	Have measurable ISO objectives and targets been established, documented and communicated throughout the organization	12	2	0
		85.7	14.3	0.0
6	Ensuring resources are available for the ISO , and directing and supporting individuals, including management, who contribute to its effectiveness	14	0	0
		100.0	0.0	0.0
7	Communicating the importance of effective information management and conformance to ISO requirements	13	1	0
		92.9	7.1	0.0
8	Are security policies subject to review	14	0	0
		100.0	0.0	0.0
9	Are the reviews conducted at regular intervals	13	1	0
		92.9	7.1	0.0

Source: IPM SPSS 24 package

From the above table result shows:

Do Information management policy exist by the (14) by (%100.0) answered yes، and(0) by (%0.0) answered no, and (0) by (%0.0) answered other.

Are all policies approved by management by the (14) by (%100.0) answered yes، and(0) by (%0.0) answered no, and (0) by (%0.0) answered other

Are policies properly communicated to employees by the (13) by (%92.9) answered yes، and (1) by (%7.1) answered no, and (0) by (%0.0) answered other

Is there Establishing the information management policy and objectives, in consideration of the strategic direction of the organization, and in promotion of continual improvement by the (14) by (%100.0) answered yes، and (0) by (%0.0) answered no, and (0) by (%0.0) answered other

Have measurable ISO objectives and targets been established, documented and communicated throughout the organization by the (12) by (%85.7) answered yes، and (2) by (%14.3) answered no, and (0) by (%0.0) answered other

Ensuring resources are available for the ISO , and directing and supporting individuals, including management, who contribute to its effectiveness by the (14) by (%100.0) answered yes، and (0) by (%0.0) answered no, and (0) by (%0.0) answered other.

Communicating the importance of effective information management and conformance to ISMS requirements by the (13) by (%92.9) answered yes، and (1) by (%7.1) answered no, and (0) by (%0.0) answered other.

Are management policies subject to review by the (14) by (%100.0) answered yes، and (0) by (%0.0) answered no, and (0) by (%0.0) answered other.

Are the reviews conducted at regular intervals by the (13) by (%92.9) answered yes، and (1) by (%7.1) answered no, and (0) by (%0.0) answered other.

Table (4.9) illustrates chi-square teat results for the organization's leadership commitment to the ISO standard demonstrated b

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Do Information Security policy exist	10.28	1	0.000	3.00	Yes
2	Are all policies approved by management	7.14	1	0.000	3.00	Yes
3	Are policies properly communicated to employees	10.28	1	0.000	3.00	Yes
4	Is there Establishing the information management policy and objectives, in consideration of the strategic direction of the organization, and in promotion of continual improvement	10.28	1	0.000	3.00	Yes
5	Have measurable ISO objectives and targets been established, documented and communicated throughout the organization	7.14	1	0.000	3.00	Yes
6	Ensuring resources are available for the ISO standard , and directing and supporting individuals, including management, who contribute to its effectiveness	13.00	2	0.000	3.00	Yes
7	Communicating the importance of effective information management and conformance to ISO requirements	10.28	1	0.000	3.00	Yes
8	Are system policies subject to review	10.28	1	0.000	3.00	Yes
9	Are the reviews conducted at regular intervals	17.28	2	0.000	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.9) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Do Information management policy exist was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Are all policies approved by management was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Are policies properly communicated to employees was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
4. The value of chi – square calculated to signify the differences between the Is there Establishing the information management policy and objectives, in consideration of the strategic direction of the organization, and in promotion of continual improvement was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
5. The value of chi – square calculated to signify the differences between the Have measurable ISO standard objectives and targets been established, documented and communicated throughout the organization was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
6. The value of chi – square calculated to signify the differences between the Ensuring resources are available for the ISO , and directing and supporting individuals, including management, who contribute to its effectiveness was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
7. The value of chi – square calculated to signify the differences between the Communicating the importance of effective information management and conformance to ISO requirements was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
8. The value of chi – square calculated to signify the differences between the Are System policies subject to review was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
9. The value of chi – square calculated to signify the differences between the Are the reviews conducted at regular intervals was (17.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
10.

Table (4.10) illustrates the frequency and percentage for Roles, responsibilities and authorities

No	**Items**	**Yes**	**No**	**Other**
1	Are the roles within the ISO standard clearly defined and communicated	12	2	0
		85.7	14.3	0.0
2	Are the responsibilities and authorities for conformance and reporting on ISO standard performance assigned	11	2	1
		78.6	14.3	7.1

Source: IPM SPSS 24 package

From the above table result shows:

Are the roles within the ISO standard clearly defined and by the (12) by (%85.7) answered yes، and (2) by (%14.3) answered no, and (0) by (%0.0) answered other.

Are the responsibilities and authorities for conformance and reporting on ISO standard performance assigned by the (11) by (%78.6) answered yes، and (2) by (%14.3) answered no, and (1) by (%7.1) answered other.

Table (4.11) illustrates chi-square teat results for Roles, responsibilities and authorities

No	**Phrases**	**Chi-square value**	**df**	**Sig.**	**Median**	**Interpretation**
1	Are the roles within the ISO standard clearly defined and communicated	7.14	1	0.000	3.00	Yes
2	Are the responsibilities and authorities for conformance and reporting on ISO standard performance assigned	13.00	2	0.000	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.11) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Are the roles within the ISMS clearly defined and communicated was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Are the responsibilities and authorities for conformance and reporting on ISO standard performance assigned was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.12) illustrates the frequency and percentage for Access control

No	**Items**	**Yes**	**No**	**Other**
1	Is there a documented access control policy	13	1	0
		92.9	7.1	0.0
2	Is there a formal user access registration process in place	14	0	0
		100.0	0.0	0.0
3	Is there a formal management process in place to control allocation of secret authentication Information	13	1	0
		92.9	7.1	0.0
4	Is media in transport protected against un authorized access, misuse or corruption	12	1	1
		85.7	7.1	7.1
5	Are complex passwords required	13	1	0
		92.9	7.1	0.0

Source: IPM SPSS 24 package

From the above table result shows:

Is there a documented access control policy by the (13) by (%92.9) answered yes، and(1) by (%7.1) answered no, and (0) by (%0.0) answered other

Is there a formal user access registration process in place by the (14) by (%100.0) answered yes، and (0) by (%0.0) answered no, and (0) by (%0.0) answered other.

Is there a formal management process in place to control allocation of secret authentication Information by the (13) by (%92.9) answered yes، and (1) by (%7.1) answered no, and (0) by (%0.0) answered other.

Is media in transport protected against un authorized access, misuse or corruption by the (13) by (%92.9) answered yes، and (1) by (%7.1) answered no, and (0) by (%0.0) answered other.

Are complex passwords required by the (13) by (92.9%) answered yes، and (1) by (7.1%) answered no, and (0) by (0.0%) answered other.

Table (4.13) illustrates chi-square teat results for Access control

No	**Phrases**	**Chi-square value**	**df**	**Sig.**	**Median**	**Interpretation**
1	Is there a documented access control policy	10.28	1	0.000	3.00	Yes
2	Is there a formal user access registration process in place	1.00	1	0.000	3.00	Yes
3	Is there a formal management process in place to control allocation of secret authentication Information	10.28	1	0.000	3.00	Yes
4	Is media in transport protected against un authorized access, misuse or corruption	17.28	2	0.000	3.00	Yes
5	Are complex passwords required	10.28	1	0.000	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.13) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Is there a documented access control policy was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Is there a formal user access registration process in place was (1.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Is there a formal management process in place to control allocation of secret authentication Information was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
4. The value of chi – square calculated to signify the differences between the Is media in transport protected against un authorized access, misuse or corruption was (17.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
5. The value of chi – square calculated to signify the differences between the Are complex passwords required was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.14) illustrates the frequency and percentage for General Questions

No	**Items**	**Yes**	**No**	**Other**
1	Have the internal and external issues that are relevant to the ISO standard , and that impact on the achievement of its expected outcome of the organization , and been determined	10	1	3
		71.4	7.1	21.4
2	Has the organization determined the interested parties that are relevant to the ISO standard	12	2	0
		85.7	14.3	0.0
3	Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements	12	2	0
		85.7	14.3	0.0
4	Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made	11	1	2
		78.6	7.1	14.3
5	Is there a process which details how and when contact is required	11	1	2
		78.6	7.1	14.3
6	Do all projects go through some form of information management assessment	9	1	4
		64.3	7.1	28.6

Source: IPM SPSS 24 package

From the above table result shows:

Have the internal and external issues that are relevant to the ISO standard , and that impact on the achievement of its expected outcome of the organization, and been determined by the (10) by (%71.4) answered yes، and (1) by (%7.1) answered no, and (3) by (%21.4) answered other.

Has the organization determined the interested parties that are relevant to the ISO standard by the (12) by (%85.7) answered yes، and (2) by (%14.3) answered no, and (0) by (%0.0) answered other.

Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements by the (12) by (%85.7) answered yes، and (2) by (%14.3) answered no, and (0) by (0.0%) answered other.

Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made by the (11) by (%78.6) answered yes، and(1) by (%7.1) answered no, and (2) by (%14.3) answered other.

Is there a process which details how and when contact is required by the (11) by (%78.6) answered yes، and(1) by (%7.1) answered no, and (2) by (%14.3) answered other.

Do all projects go through some form of information management assessment by the (9) by (%64.3) answered yes، and(1) by (%7.1) answered no, and (4) by (%28.6) answered other.

Table (4.15) illustrates chi-square teat results for General Questions

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Have the internal and external issues that are relevant to the ISO standard , and that impact on the achievement of its expected outcome of the organization , and been determined	9.57	1	0.000	3.00	Yes
2	Has the organization determined the interested parties that are relevant to the ISO standard	7.14	1	0.000	3.00	Yes
3	Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements	7.14	2	0.000	3.00	Yes
4	Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made	13.00	1	0.000	3.00	Yes
5	Is there a process which details how and when contact is required	13.00	1	0.000	3.00	Yes
6	Do all projects go through some form of information management assessment	7.00	1	0.000	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.15) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Have the internal and external issues that are relevant to the ISO standard , and that impact on the achievement of its expected outcome of the organization , and been determined was (9.57) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Has the organization determined the interested parties that are relevant to the ISO standard was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
4. The value of chi – square calculated to signify the differences between the Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
5. The value of chi – square calculated to signify the differences between the Is there a process which details how and when contact is required was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
6. The value of chi – square calculated to signify the differences between the Do all projects go through some form of information management assessment was (7.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.16) illustrates the frequency and percentage for Supplier relationship

No	**Items**	**Yes**	**No**	**Other**
1	Is information management included in contracts established with suppliers and service providers	10	0	4
		71.4	0.0	28.6
2	Are suppliers provided with documented management requirements	11	0	3
		78.6	0.0	21.4
3	Do supplier agreements include requirements to address information management within the service & product supply chain	11	0	3
		78.6	0.0	21.4
4	Are suppliers subject to regular review and audit	7	2	5
		50.0	14.3	35.7

Source: IPM SPSS 24 package

From the above table result shows:

Is information management included in contracts established with suppliers and service providers by the (10) by (%71.4) answered yes، and(0) by (%0.0) answered no, and (4) by (%28.6) answered other.

Are suppliers provided with documented management requirements by the (11) by (%78.6) answered yes، and (0) by (%0.0) answered no, and (3) by (%21.4) answered other.

Do supplier agreements include requirements to address information management within the service & product supply chain by the (11) by (%78.6) answered yes، and (0) by (%0.0) answered no, and (3) by (%21.4) answered other.

Are suppliers subject to regular review and audit by the (7) by (%50.0) answered yes، and (2) by (%14.3) answered no, and (5) by (%35.7) answered other.

Table (4.17) illustrates chi-square teat results for Supplier relationship

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Is information management included in contracts established with suppliers and service providers	2.57	1	0.000	3.00	Yes
2	Are suppliers provided with documented security requirements	4.57	1	0.000	3.00	Yes
3	Do supplier agreements include requirements to address information management within the service & product supply chain	4.57	1	0.000	3.00	Yes
4	Are suppliers subject to regular review and audit	2.71	2	0.000	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.17) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Is information security included in contracts established with suppliers and service providers was (2.57) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Are suppliers provided with documented management requirements was (4.57) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Do supplier agreements include requirements to address information management within the service & product supply chain

was (4.57) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

4. The value of chi – square calculated to signify the differences between the Are suppliers subject to regular review and audit was (2.71) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.18) illustrates the frequency and percentage for Complains

No	**Items**	**Yes**	**No**	**Other**
1	Has the organization identified and documented all relevant legislative, regulatory or contractual requirements related to security	12	0	2
		85.7	0.0	14.3
2	Does the organization keep a record of all intellectual property rights and use of proprietary software products	9	3	2
		64.3	21.4	14.3
3	Are records protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative regulatory contractual and business requirements	12	0	2
		85.7	0.0	14.3

Source: IPM SPSS 24 package

From the above table result shows:

Has the organization identified and documented all relevant legislative, regulatory or contractual requirements related to system by the (12) by (%85.7) answered yes، and(0) by (%0.0) answered no, and (2) by (%14.3) answered other.

Does the organization keep a record of all intellectual property rights and use of proprietary software products by the (9) by (%64.3) answered yes، and(3) by (%21.4) answered no, and (2) by (%14.3) answered other.

Are records protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative regulatory contractual and business requirements by the (12) by (%85.7) answered yes، and(0) by (%0.0) answered no, and (2) by (%14.3) answered other.

Table (4.19) illustrates chi-square teat results for Complains

No	**Phrases**	**Chi-square value**	**df**	**Sig.**	**Median**	**Interpretation**
1	Has the organization identified and documented all relevant legislative, regulatory or contractual requirements related to management	7.14	1	0.000	3.00	Yes
2	Does the organization keep a record of all intellectual property rights and use of proprietary software products	6.14	2	0.000	3.00	Yes
3	Are records protected from loss,	7.14	1	0.000	3.00	Yes

	destruction, falsification and unauthorized access or release in accordance with legislative regulatory contractual and business requirements					

Source: IPM SPSS 24 package

The results of table (4.19) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Has the organization identified and documented all relevant legislative, regulatory or contractual requirements related to security was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Does the organization keep a record of all intellectual property rights and use of proprietary software products was (6.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Are records protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative regulatory contractual and business requirements was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.20) illustrates the frequency and percentage for 1 Management responsibilities to employment

No	**Items**	**Yes**	**No**	**Other**
1	Are managers (of all levels) engaged in driving Security within the business	12	0	2
		85.7	0.0	14.3
2	Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply security in accordance with established policies and procedures	10	2	2
		71.4	14.3	14.3
3	Do all employees, contractors and 3rd party users undergo regular ISO 27001:2013 awareness training appropriate to their role and function within the Organization	11	2	1
		78.6	14.3	7.1

Source: IPM SPSS 24 package

From the above table result shows:

Are managers (of all levels) engaged in driving management within the business by the (12) by (%85.7) answered yes، and(0) by (%0.0) answered no, and (2) by (%14.3) answered other.

Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply security in accordance with established policies and procedures by the (10) by (%71.4) answered yes، and(2) by (%14.3) answered no, and (2) by (%14.3) answered other.

Do all employees, contractors and 3rd party users undergo regular ISO awareness training appropriate to their role and function within the organization by the (11) by (%78.6) answered yes، and(2) by (%14.3) answered no, and (1) by (%7.1) answered other.

Table (4.21) illustrates chi-square teat results for 1 Management responsibilities to employment

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Are managers (of all levels) engaged in driving system within the business	7.14	1	0.000	3.00	Yes
2	Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply system in accordance with established policies and procedures	9.14	2	0.000	3.00	Yes
3	Do all employees, contractors and 3rd party users undergo regular ISO awareness training appropriate to their role and function within the organization	13.00	2	0.000	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.21) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Are managers (of all levels) engaged in driving system within the business was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply security in accordance with established policies and procedures was (9.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Do all employees, contractors and 3rd party users undergo regular system awareness training appropriate to their role

and function within the organization was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.22) illustrates the frequency and percentage for Human resources management

No	**Items**	**Yes**	**No**	**Other**
1	Are background verification checks carried out on all new candidates for employment	12	0	2
		85.7	0.0	14.3
2	Are these checks approved by appropriate management authority	12	0	2
		85.7	0.0	14.3
3	Are all employees, contractors and third party users asked to sign confidentiality and nondisclosure agreements	13	0	1
		92.9	0.0	7.1
4	Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role	12	1	1
		85.7	7.1	7.1

Source: IPM SPSS 24 package

From the above table result shows:

Are background verification checks carried out on all new candidates for employment by the (12) by (%85.7) answered yes، and(0) by (%0.0) answered no, and (2) by (%14.3) answered other.

Are these checks approved by appropriate management authority by the (12) by (%85.7) answered yes، and(0) by (%0.0) answered no, and (2) by (%14.3) answered other.

Are all employees, contractors and third party users asked to sign confidentiality and nondisclosure agreements by the (13) by (%92.9) answered yes، and(0) by (%0.0) answered no, and (1) by (%7.1) answered other.

Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role by the (12) by (%85.7) answered yes، and(1) by (%7.1) answered no, and (1) by (%7.1) answered other **.**

Table (4.23) illustrates chi-square teat results for Human resources management

No	**Phrases**	**Chi-square value**	**df**	**Sig.**	**Median**	**Interpretation**
1	Are background verification checks carried out on all new candidates for employment	7.14	1	0.000	3.00	Yes
2	Are these checks approved by appropriate management authority	7.14	1	0.000	3.00	Yes
3	Are all employees, contractors and third party users asked to sign confidentiality and nondisclosure agreements	10.28	1	0.000	3.00	Yes
4	Is there a process to ensure user access rights are removed on termination of	17.28	2	0.000	3.00	Yes

	employment or contract, or adjusted upon change of role					

Source: IPM SPSS 24 package

The results of table (4.23) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Are background verification checks carried out on all new candidates for employment was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Are these checks approved by appropriate management authority was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Are all employees, contractors and third party users asked to sign confidentiality and nondisclosure agreements was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
4. The value of chi – square calculated to signify the differences between the Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role was (17.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.24) illustrates the frequency and percentage for ISMS resources , competence Awareness and communication

No	**Items**	**Yes**	**No**	**Other**
1	Is the ISO standard adequately resourced	11	2	1
		78.6	14.3	7.1
2	Is there a process defined and documented for determining competence for ISO roles	12	2	0
		85.7	14.3	0.0
3	Are those undertaking ISO roles competent, and is this competence documented appropriately	11	2	1
		78.6	14.3	7.1
4	Is everyone within the organization's aware of the importance of the information security policy	12	2	0
		85.7	14.3	0.0
5	Is there a documented process for terminating or changing employment duties	12	0	2
		85.7	0.0	14.3
6	Are any information security duties which survive employment communicated to the employee or contractor	11	1	2
		78.6	7.1	14.3
7	Is the inventory accurate and kept up to date	10	1	3
		71.4	7.1	21.4

Source: IPM SPSS 24 package

From the above table result shows:

Is the ISO standard adequately resourced by the (11) by (%78.6) answered yes، and(2) by (%14.3) answered no, and (1) by (%7.1) answered other.

Is there a process defined and documented for determining competence for ISO standard roles by the (12) by (%85.7) answered yes، and(2) by (%14.3) answered no, and (0) by (%0.0) answered other.

Are those undertaking ISO standard roles competent, and is this competence documented appropriately by the (11) by (%78.6) answered yes، and(2) by (%14.3) answered no, and (1) by (%7.1) answered other.

Is everyone within the organization's aware of the importance of the information security policy by the (12) by (%85.7) answered yes، and(0) by (%0.0) answered no, and (2) by (%14.3) answered other.

Is there a documented process for terminating or changing employment duties by the (12) by (%85.7) answered yes، and(0) by (%0.0) answered no, and (2) by (%14.3) answered other.

Are any information security duties which survive employment communicated to the employee or contractor by the (11) by (%78.6) answered yes، and(1) by (%7.1) answered no, and (2) by (%14.3) answered other.

Is the inventory accurate and kept up to date by the (10) by (%71.4) answered yes، and(1) by (%7.1) answered no, and (3) by (%21.4) answered other.

Table (4.25) illustrates chi-square teat results for ISO 27001:2013 resources, competence Awareness and communication

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Is the ISO 27001:2013 adequately resourced	13.00	2	0.000	3.00	Yes
2	Is there a process defined and documented for determining competence for ISO roles	7.14	1	0.000	3.00	Yes
3	Are those undertaking ISO roles competent, and is this competence documented appropriately	13.00	2	0.000	3.00	Yes
4	Is everyone within the organization's aware of the importance of the information security policy	7.14	1	0.000	3.00	Yes
5	Is there a documented process for terminating or changing employment duties	7.14	1	0.000	3.00	Yes
6	Are any information security duties which survive employment communicated to the employee or contractor	13.00	2	0.000	3.00	Yes
7	Is the inventory accurate and kept up to date	9.57	2	0.000	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.25) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Is the ISO 27001:2013 adequately resourced was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Is there a process defined and documented for determining competence for ISO 27001:2013 roles was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Are those undertaking ISO roles competent, and is this competence documented appropriately was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
4. The value of chi – square calculated to signify the differences between the Is everyone within the organization's aware of the importance of the information security policy was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
5. The value of chi – square calculated to signify the differences between the Is there a documented process for terminating or changing employment duties was (7.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
6. The value of chi – square calculated to signify the differences between the Are any information security duties which survive employment communicated to the employee or contractor was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
7. The value of chi – square calculated to signify the differences between the Is the inventory accurate and kept up to date was (9.57) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.26) illustrates the frequency and percentage for Risks and opportunities of ISO standard implementation, assessment and treatment of information management risk

No	**Items**	**Yes**	**No**	**Other**
1	Have actions to address risks and opportunities been planned, and integrated into the ISO 27001:2013 processes, and are they evaluated for effectiveness	10	1	3
		71.4	7.1	21.4
2	Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined	13	0	1
		92.9	0.0	7.1
3	Is the information risk assessment process repeatable and does it produce consistent, valid and comparable results	13	0	1
		92.9	0.0	7.1
4	Does the information risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISO , and are risk owners identified	13	0	1
		92.9	0.0	7.1
5	Has an information risk treatment plan been formulated and approved by risk owners, and have residual information risks been authorized by risk owners	12	1	1
		85.7	7.1	7.7
6	Is documented information about the information risk treatment process available	11	1	2
		78.6	7.1	14.3
7	Do secure areas have suitable entry control systems to ensure only authorized personnel have access	14	0	0
		100.0	0.0	0.0
8	Have physical protection measures to prevent natural disasters, malicious attack or accidents been designed in	9	2	3
		64.3	14.3	21.4
9	Are processes to prevent malware spreading in place	14	0	0
		100.0	0.0	0.0
10	Is there a rigorous equipment maintenance schedule	11	1	2
		78.6	7.1	14.3

Source: IPM SPSS 24 package

From the above table result shows:

Have actions to address risks and opportunities been planned, and integrated into the ISO 27001:2013 processes, and are they evaluated for effectiveness by the (10) by (%71.4) answered yes، and(1) by (%7.1) answered no, and (3) by (%21.4) answered other.

Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined by the (13) by (%92.9) answered yes، and(1) by (%7.1) answered no, and (0) by (%0.0) answered other.

Is the information risk assessment process repeatable and does it produce consistent, valid and comparable results by the (13) by (%92.9) answered yes، and(0) by (%0.0) answered no, and (1) by (%7.1) answered other.

Does the information risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISO , and are risk owners identified by the (13) by (%92.9) answered yes، and(0) by (%0.0) answered no, and (1) by (%7.1) answered other.

Has an information risk treatment plan been formulated and approved by risk owners, and have residual information risks been authorized by risk owners by the (12) by (%85.7) answered yes، and(1) by (%7.1) answered no, and (1) by (%7.1) answered other.

Is documented information about the information risk treatment process available by the (11) by (%78.6) answered yes، and(1) by (%7.1) answered no, and (2) by (%14.3) answered other.

Do secure areas have suitable entry control systems to ensure only authorized personnel have access by the (14) by (%100.0) answered yes، and(0) by (%0.0) answered no, and (0) by (%0.0) answered other

Have physical protection measures to prevent natural disasters, malicious attack or accidents been designed in by the (9) by (%64.3) answered yes، and(2) by (%14.3) answered no, and (3) by (%21.4) answered other.

Are processes to prevent malware spreading in place by the (14) by (%100.0) answered yes، and(0) by (%0.0) answered no, and (0) by (%0.0) answered other.

Is there a rigorous equipment maintenance schedule by the (11) by (%78.6) answered yes، and(1) by (%7.1) answered no, and (2) by (%14.3) answered other.

Table (4.27) illustrates chi-square teat results for Risks and opportunities of ISO 27001:2013 implementation, assessment and treatment of information risk management

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Have actions to address risks and opportunities been planned, and integrated into the ISO 27001:2013 processes, and are they evaluated for effectiveness	9.57	2	0.000	3.00	Yes
2	Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined	10.28	1	0.000	3.00	Yes
3	Is the information risk assessment process repeatable and does it produce consistent, valid and comparable results	10.28	1	0.000	3.00	Yes
4	Does the information risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISO 27001:2013, and are risk owners identified	10.28	1	0.000	3.00	Yes
5	Has an information risk treatment plan been formulated and approved by risk owners, and have residual information risks been authorized by risk owners	17.28	2	0.000	3.00	Yes

6	Is documented information about the information risk treatment process available	13.00	2	0.000	3.00	Yes
7	Do secure areas have suitable entry control systems to ensure only authorized personnel have access	1.00	1	0.000	3.00	Yes
8	Have physical protection measures to prevent natural disasters, malicious attack or accidents been designed in	6.14	2	0.000	3.00	Yes
9	Are processes to prevent malware spreading in place	1.00	1	0.000	3.00	Yes
10	Is there a rigorous equipment maintenance schedule	13.00	2	0.000	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.27) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Have actions to address risks and opportunities been planned, and integrated into the ISO 27001:2013 processes, and are they evaluated for effectiveness was (9.57) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Is the information risk assessment process repeatable and does it produce consistent, valid and comparable results was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
4. The value of chi – square calculated to signify the differences between the Does the information risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISO 27001:2013 , and are risk owners identified was (10.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
5. The value of chi – square calculated to signify the differences between the Has an information risk treatment plan been formulated and approved by risk owners, and have residual information risks

been authorized by risk owners was (17.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

6. The value of chi – square calculated to signify the differences between the Is documented information about the information risk treatment process available was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
7. The value of chi – square calculated to signify the differences between the Do secure areas have suitable entry control systems to ensure only authorized personnel have access was (1.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
8. The value of chi – square calculated to signify the differences between the Have physical protection measures to prevent natural disasters, malicious attack or accidents been designed in was (6.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
9. The value of chi – square calculated to signify the differences between the Are processes to prevent malware spreading in place was (1.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
10. The value of chi – square calculated to signify the differences between the Is there a rigorous equipment maintenance schedule was (13.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Hypotheses: -

H1: There is a relationship between the application of information management system and the development of the performance of the institution

Table (4.28) value of the Chi-square test for H1

No	Chi-square	Df	Sig.	Correlation	Statistical significant
24	17.25	2	0.00	0.76	Significant

Source: IPM SPSS 24 package

Table (4.28) shows that the value of the Chi-square test (17.25) by significant value (0.00) it’s less than the probability value (0.05) this means that there is a relationship between the application of information management system and the development of the performance of the institution .

H2: The implementation of ISO 27001: 2013 helps to increase the institutional profitability of stakeholders

Table (4.29) value of the Chi-square test for H2

No	Chi-square	Df	Sig.	Median	Statistical significant
24	18.95	2	0.00	3.0	Significant

Source: IPM SPSS 24 package

Table (4.29) shows that the value of the Chi-square test (18.95) by significant value (0.00) it’s less than the probability value (0.05) this means that there is The implementation of ISO 27001: 2013 helps to increase the institutional profitability of stakeholders.

H3: Application of the standard increases employee satisfaction

Table (4.30|) value of the Chi-square test for H3

No	Chi-square	Df	Sig.	Median	Statistical significant
24	12.14	2	0.00	3.0	Significant

Source: IPM SPSS 24 package

Table (4.30) shows that the value of the Chi-square test (12.14) by significant value (0.00) it’s less than the probability value (0.05) this means that there is Application of the standard increases employee satisfaction .

H4: The use of this standard reduces waste time and money.

Table (4.31) value of the Chi-square test for H4

No	Chi-square	Df	Sig.	median	Statistical significant
24	15.41	2	0.00	3.0	Significant

Source: IPM SPSS 24 package

Table (4.31) shows that the value of the Chi-square test (15.41) by significant value (0.00) it’s less than the probability value (0.05) this means that there is The use of this standard reduces waste time and money .

4.1.3Data analysis for employees:

The first topic Field study procedures:

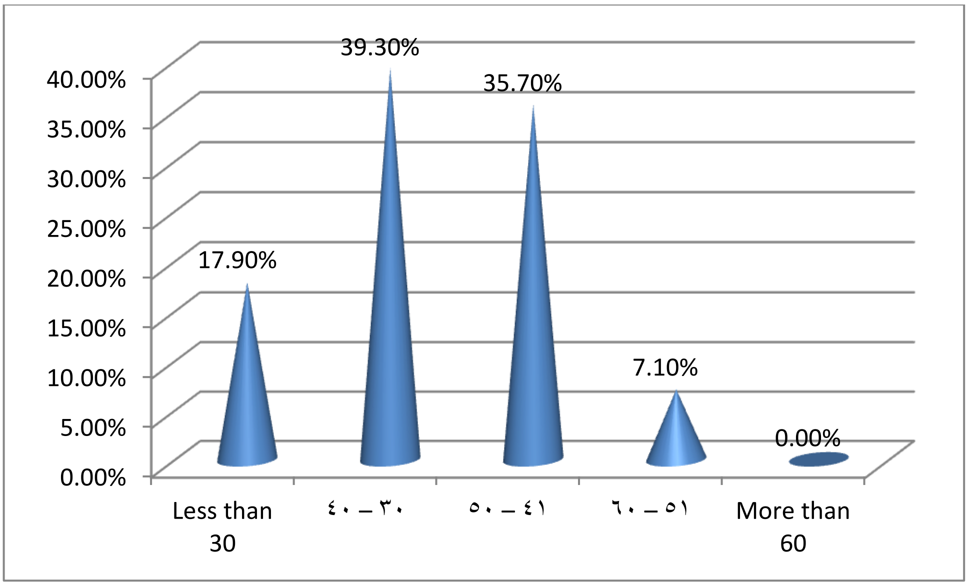
This course deals with the field study procedures under the following sections
First: population and sample of the study

Table (4.32) the frequency and percentage for Number of age

Value	Frequencies	Percentage
Less than 30	5	17.9%
30 – 40	11	39.3%
41 – 50	10	35.7%
51 – 60	2	7.1%
More than 60	0	0.0%
Total	28	100.0%

Source: IPM SPSS 24 package

Figure (4.7) the frequency and percentage for Number of age



Source: excel 2016

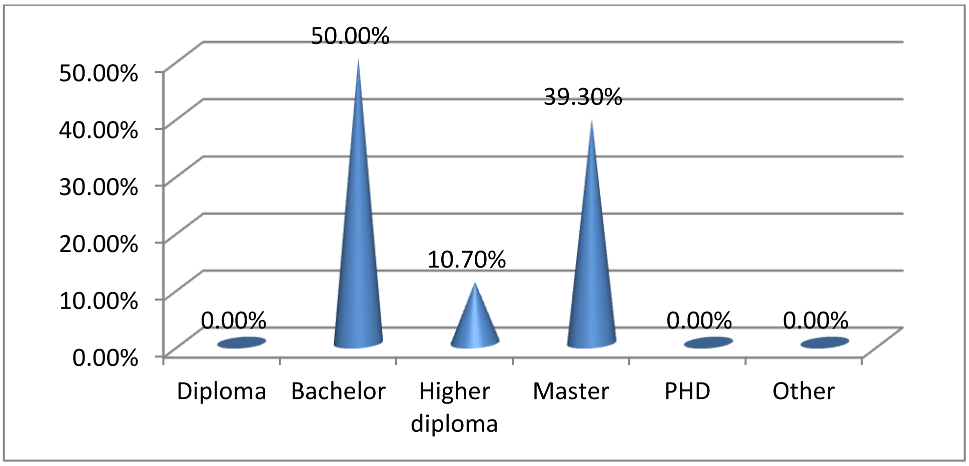
Table (4.7) illustrates the views of the distribution of the age sample by Less than 30 years by (%17.9) and 30-40 years by (%39.3) and 41-50 years by (%35.7) and 51 – 60 by (%7.1) and More than 60 by (%0.0).

Table (4.33) the frequency and percentage for the Qualification

Qualification	Frequencies	Percentage
Diploma	0	0.0%
Bachelor	14	50.0%
Higher diploma	3	10.7%
Master	11	39.3%
PHD	0	0.0%
Other	0	0.0%
Total	28	100.0%

Source: IPM SPSS 24 package

Figure (4.8) the frequency and percentage for the Qualification



Source: excel 2016

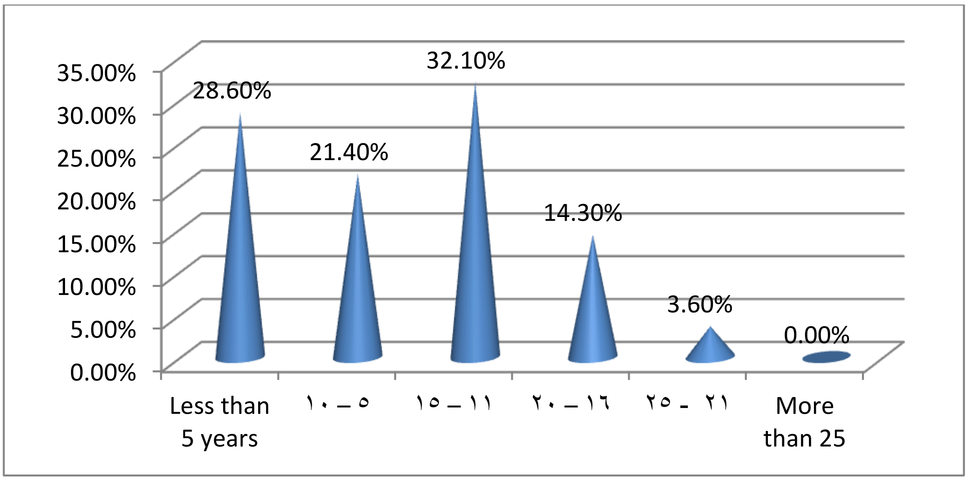
Table (4.8) the views of the distribution of the Qualification Diploma by (%0.0) and Bachelor by (%50.0) and higher diploma by (%10.7) and Master by (%39.3) and Ph.D. by (%0.0) and other by (%0.0).

Table (4.34) the frequency and percentage for the How long have you had your current position

work	Frequencies	Percentage
Less than 5 years	8	28.6%
5 – 10	6	21.4%
11 – 15	9	32.1%
16 – 20	4	14.3%
21 - 25	1	3.6%
More than 25	0	0.0%
Total	28	100.0%

Source: IPM SPSS 24 package

Figure (4.9) the frequency and percentage for the How long have you had your current position



Source: excel 2016

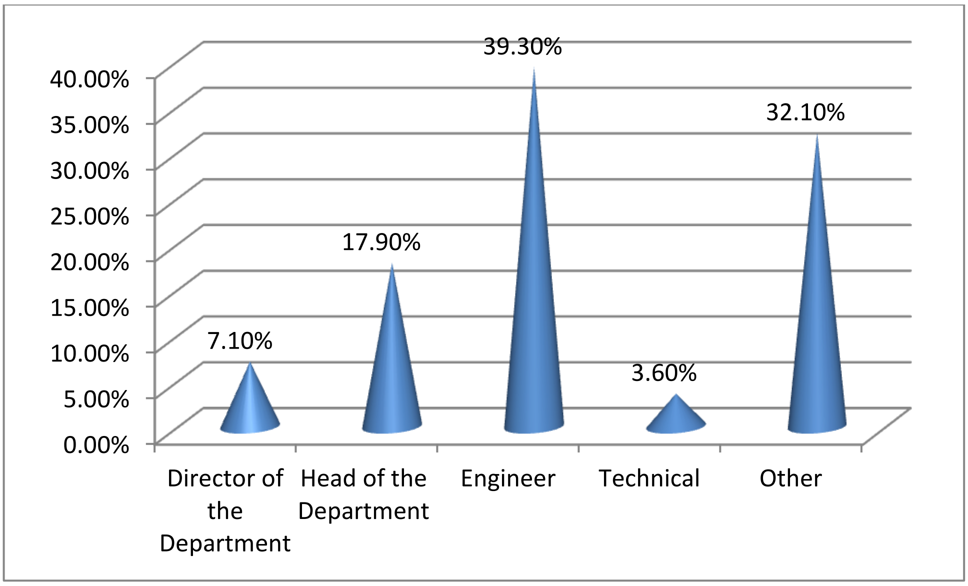
Table (4.9) the views of the distribution of the How long have you had your current position Less than 5 years by (%28.6) and 5-10 by (%21.4) and 11-15 by (%32.1) and 16-20 by (14.3%) and 21-25 by (%3.6) and More than 25 by (%0.0).

Table (4.35) the frequency and percentage for what is your position?

Value	Frequencies	Percentage
Director of the Department	2	7.1%
Head of the Department	5	17.9%
Engineer	11	39.3%
Technical	1	3.6%
Other	9	32.1%
Total	28	100.0%

Source: IPM SPSS 24 package

Figure (4.10) the frequency and percentage for what is your position?



Source: excel 2016

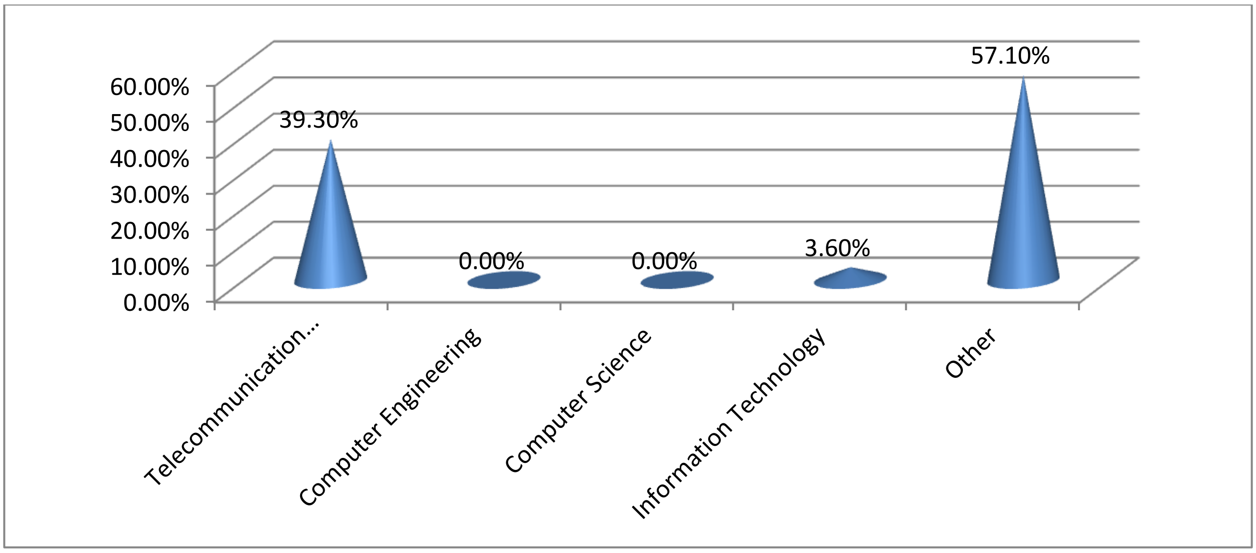
Table (4.10) the views of the distribution of what is your position? Director of the Department by (%7.1) and Head of the Department by (%17.9) and Engineer by (%39.3) and Technical by (%3.6) and Other by (%32.1)

Table (4.36) the frequency and percentage for the Scientific Specialization

Value	Frequencies	Percentage
Telecommunication Engineering	11	39.3%
Computer Engineering	0	0.0%
Computer Science	0	0.0%
Information Technology	1	3.6%
Other	16	57.1%
Total	28	100.0%

Source: IPM SPSS 24 package

Figure (4.11) the frequency and percentage for the Scientific Specialization



Source: excel 2016

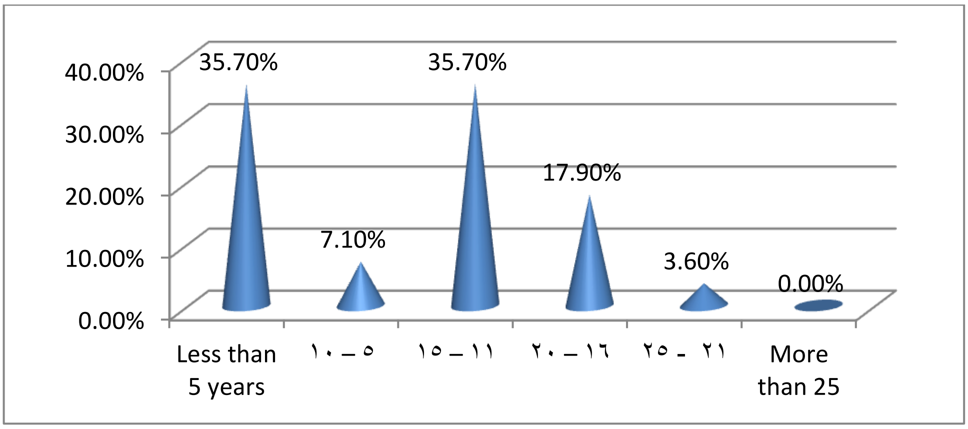
Table (4.11) the views of the distribution of the Scientific Specialization Telecommunication Engineering by (%39.3) and Computer Engineering by (%0.0) and Computer Science by (%0.0) and Information Technology by (%3.6) and Other by (%57.1).

Table (4.37) the frequency and percentage for the How long have you worked in this organization?

work	Frequencies	Percentage
Less than 5 years	10	35.7%
5 – 10	2	7.1%
11 – 15	10	35.7%
16 – 20	5	17.9%
21 - 25	1	3.6%
More than 25	0	0.0%
Total	28	100.0%

Source: IPM SPSS 24 package

Figure (4.12) the frequency and percentage for the How long have you worked in this organization



Source: excel 2016

Table (4.12) the views of the distribution of the How long have you worked in this organization? Less than 5 years by (%35.7) and 5-10 by (%7.1) and 11-15 by (%35.7) and 16-20 by (%17.9) and 21-25 by (%3.6) and More than 25 by (%0.0) .

Second: reliability and validity

Cranach's alpha method: -
Where reliability was calculated using Cranach's alpha equation shown below:

$$\text{Reliability coefficient} = \frac{n}{N-1} * \frac{1 - \text{Total variations questions}}{\text{variation college grades}}$$

$$\text{Validity} = \sqrt{\frac{n}{N-1} * \frac{1 - \text{Total variations questions}}{\text{variation college grades}}}$$

Cranach alpha coefficient = (0.87), a reliability coefficient is high and it indicates the stability of the scale and the validity of the study
Validity coefficient is the square of the islands so reliability coefficient is (0.93), and this shows that there is a high sincerity of the scale and that the benefit of the study.

Table (4.38) Cranach's alpha method

No	Value	reliability	Validity
1	The organization's leadership commitment to the ISO 27001:2013 demonstrated by	0.85	0.92
2	Roles , responsibilities and authorities	0.91	0.95
3	Access control	0.86	0.93
4	General Questions	0.86	0.93
5	Management responsibilities to employment	0.87	0.93
6	ISO resources , competence Awareness and communication	0.86	0.93
7	Risks and opportunities of ISO 27001:2013 implementation , assessment and treatment of information risk management	0.86	0.93
Total		0.89	0.94

Source: IPM SPSS 24 package

The second subject View and analyze data

Table (4.39) the frequency and percentage for the organization's leadership commitment to the ISO 27001:2013 demonstrated by

No	**Items**	**Yes**	**No**	**Other**
1	Do Information management policy exist	27	1	0
		96.4	3.6	0.0
2	Are policies properly communicated to employees	26	1	1
		62.9	3.6	3.6
3	Communicating the importance of effective information management and conformance to ISO 27001:2013 requirements	27	1	0
		96.4	3.6	0.0
4	Are system policies subject to review	24	1	3
		85.7	3.6	10.7
5	Are the reviews conducted at regular intervals	22	2	4
		78.6	7.1	14.3

Source: IPM SPSS 24 package

From the above table result shows:

Do Information management policy exist by the (27) by (%96.4) answered yes، and (1) by (%3.3) answered no, and (0) by (%0.0) answered other.

Are policies properly communicated to employees by the (26) by (%92.9) answered yes، and (1) by (3.6%) answered no, and (1) by (%3.6) answered other.

Communicating the importance of effective information management and conformance to ISO 27001:2013 requirements by the (27) by (%96.4) answered yes، and(1) by (%3.6) answered no, and (0) by (%0.0) answered other.

Are system policies subject to review by the (24) by (%85.7) answered yes، and (1) by (%3.6) answered no, and (3) by (%10.7) answered other.

Are the reviews conducted at regular intervals by the (22) by (%78.6) answered yes، and (2) by (%7.1) answered no, and (4) by (%14.3) answered other.

Table (4.40) chi-square teat results for the organization's leadership commitment to the ISO 27001:2013 demonstrated by

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Do Information management policy exist	24.14	1	0.00	3.00	Yes
2	Are policies properly communicated to employees	44.64	2	0.00	3.00	Yes
3	Communicating the importance of effective information management and conformance to ISO 27001:2013 requirements	24.14	1	0.00	3.00	Yes
4	Are system policies subject to review	34.78	2	0.00	3.00	Yes
5	Are the reviews conducted at regular intervals	26.00	2	0.00	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.40) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Do Information system policy exist was (24.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Are policies properly communicated to employees was (44.64) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Communicating the importance of effective information system and conformance to ISO requirements was (24.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

4. The value of chi – square calculated to signify the differences between the Are system policies subject to review was (34.78) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
5. The value of chi – square calculated to signify the differences between the Are the reviews conducted at regular intervals was (26.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.41) the frequency and percentage for the Roles, responsibilities and authorities

No	**Items**	**Yes**	**No**	**Other**
1	Are the roles within the ISO 27001:2013 clearly defined and communicated	22	3	3
		78.6	10.7	10.7
2	Are the responsibilities and authorities for conformance and reporting on ISO 27001:2013 performance assigned	21	2	5
		75.0	7.1	17.9

Source: IPM SPSS 24 package

From the above table result shows:

Are the roles within the ISO clearly defined and communicated by the (22) by (%78.6) answered yes، and (3) by (%10.7) answered no, and (3) by (%10.7) answered other.

Are the responsibilities and authorities for conformance and reporting on ISO performance assigned by the (21) by (%75.0) answered yes، and (2) by (%7.1) answered no, and (5) by (%17.9) answered other.

Table (4.42) chi-square teat results for the Roles, responsibilities and authorities

No	**Phrases**	**Chi-square value**	**df**	**Sig.**	**Median**	**Interpretation**
1	Are the roles within the ISO 27001:2013 clearly defined and communicated	25.78	2	0.00	3.00	Yes
2	Are the responsibilities and authorities for conformance and reporting on ISO 27001:2013 performance assigned	22.35	2	0.00	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.42) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Are the roles within the ISO 27001:2013 clearly defined and communicated was (25.78) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Are the responsibilities and authorities for conformance and reporting on ISO 27001:2013 performance assigned was (22.35) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.43) the frequency and percentage for the Access control

No	**Items**	**Yes**	**No**	**Other**
1	Is there a documented access control policy	27	0	1
		96.4	0.0	3.6
2	Is there a formal user access registration process in place	27	1	0
		96.4	3.6	0.0
3	Are complex passwords required	18	8	2
		62.3	28.6	7.1

Source: IPM SPSS 24 package

From the above table result shows:

Is there a documented access control policy by the (27) by (%96.4) answered yes، and(0) by (%0.0) answered no, and (1) by (%3.6) answered other.

Is there a formal user access registration process in place by the (27) by (%96.4) answered yes، and(1) by (%3.6) answered no, and (0) by (%0.0) answered other.

Are complex passwords required by the (18) by (%62.3) answered yes، and(8) by (%28.6) answered no, and (2) by (%7.1) answered other.

Table (4.44) chi-square teat results for the Access control

No	**Phrases**	**Chi-square value**	**df**	**Sig.**	**Median**	**Interpretation**
1	Is there a documented access control policy	24.14	1	0.00	3.00	Yes
2	Is there a formal user access registration process in place	24.14	1	0.00	3.00	Yes
3	Are complex passwords required	14.00	2	0.00	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.44) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Is there a documented access control policy was (24.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Is there a formal user access registration process in place was (24.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Are complex passwords required was (14.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.45) the frequency and percentage for the

No	**Items**	**Yes**	**No**	**Other**
1	Has the organization determined the interested parties that are relevant to the ISO 27001:2013	23	2	3
		82.1	7.1	10.7
2	Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements	23	3	2
		82.1	10.7	7.1
3	Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made	23	2	3
		882.1	7.1	10.7
4	Is there a process which details how and when contact is required	20	3	5
		71.4	10.7	17.9

Source: IPM SPSS 24 package

From the above table result shows:

Has the organization determined the interested parties that are relevant to the ISO 27001:2013 by the (23) by (%82.1) answered yes، and (2) by (%7.1) answered no, and (3) by (%10.7) answered other.

Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements by the (23) by (%82.1) answered yes، and (3) by (%10.7) answered no, and (2) by (%7.1) answered other.

Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made by the (23) by (%82.1) answered yes، and (2) by (%7.1) answered no, and (3) by (%10.7) answered other.

Is there a process which details how and when contact is required by the (20) by (%71.4) answered yes، and (3) by (%10.7) answered no, and (5) by (%17.4) answered other.

Table (4.46) chi-square teat results

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Has the organization determined the interested parties that are relevant to the ISO 27001:2013	30.07	2	0.00	3.00	Yes
2	Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements	30.07	2	0.00	3.00	Yes
3	Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made	30.07	2	0.00	3.00	Yes
4	Is there a process which details how and when contact is required	18.50	2	0.00	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.46) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the has the organization determined the interested parties that are relevant to the ISO 27001:2013 was (30.07) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements was (30.07) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made was (30.07) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
4. The value of chi – square calculated to signify the differences between the Is there a process which details how and when contact is required was (18.50) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.47) the frequency and percentage for the Management responsibilities to employment

No	Items	Yes	No	Other
1	Are managers (of all levels) engaged in driving system within the business	24	1	3
		85.7	3.6	10.7
2	Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply system in accordance with established policies and procedures	24	2	2
		85.7	7.1	7.1
3	Do all employees, contractors and 3rd party users undergo regular system awareness training appropriate to their role and function within the Organization	19	4	5
		67.9	14.3	17.9

Source: IPM SPSS 24 package

From the above table result shows:

Are managers (of all levels) engaged in driving system within the business by the (24) by (%85.7) answered yes، and(1) by (%3.6) answered no, and (3) by (%10.7) answered other.

Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply system in accordance with established policies and procedures by the (24) by (%85.7) answered yes، and(2) by (%7.1) answered no, and (2) by (%7.1) answered other.

Do all employees, contractors and 3rd party users undergo regular system awareness training appropriate to their role and function within the organization by the (19) by (%67.9) answered yes، and(4) by (%14.3) answered no, and (5) by (%17.9) answered other.

Table (4.48) chi-square teat results for the Management responsibilities to employment

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Are managers (of all levels) engaged in driving system within the business	34.78	2	0.00	3.00	Yes
2	Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply system in accordance with established policies and procedures	34.57	2	0.00	3.00	Yes
3	Do all employees, contractors and 3rd party users undergo regular system awareness training appropriate to their role and function within the Organization	15.07	2	0.00	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.48) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Are managers (of all levels) engaged in driving system within the business was (34.78) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply system in accordance with established policies and procedures was (34.57) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Do all employees, contractors and 3rd party users undergo regular system awareness training appropriate to their role and function within the organization was (15.07) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.49) the frequency and percentage for the ISO 27001:2013 resources, competence Awareness and communication

No	**Items**	**Yes**	**No**	**Other**
1	Is the ISO 27001:2013 adequately resourced	20	4	4
		71.4	14.3	14.3
2	Is everyone within the organization's aware of the importance of the information management policy	17	8	3
		60.7	28.6	10.7
3	Are any information management duties which survive employment communicated to the employee or contractor	22	2	4
		78.6	7.1	14.3
4	Is the inventory accurate and kept up to date	20	0	8
		71.4	0.0	28.6

Source: IPM SPSS 24 package

From the above table result shows:

Is the ISMS adequately resourced by the (20) by (%71.4) answered yes، and(4) by (%14.3) answered no, and (4) by (%14.3) answered other.

Is everyone within the organization's aware of the importance of the information management policy by the (17) by (%60.7) answered yes، and(8) by (%28.6) answered no, and (3) by (%10.7) answered other.

Are any information management duties which survive employment communicated to the employee or contractor by the (22) by (%78.6) answered yes، and(2) by (%7.1) answered no, and (4) by (%14.3) answered other.

Is the inventory accurate and kept up to date by the (20) by (%71.4) answered yes، and(0) by (%0.0) answered no, and (8) by (%28.6) answered other.

Table (4.50) chi-square teat results for the ISO 27001:2013 resources, competence Awareness and communication

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Is the ISO 27001:2013 adequately resourced	18.28	2	0.00	3.00	Yes
2	Is everyone within the organization's aware of the importance of the information management policy	10.78	2	0.00	3.00	Yes
3	Are any information management duties which survive employment communicated to the employee or contractor	26.00	2	0.00	3.00	Yes
4	Is the inventory accurate and kept up to date	15.14	1	0.00	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.50) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Is the ISO 27001:2013 adequately resourced was (18.28) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Is everyone within the organization's aware of the importance of the information security policy was (10.78) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Are any information management duties which survive employment communicated to the employee or contractor was (26.00) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
4. The value of chi – square calculated to signify the differences between the Is the inventory accurate and kept up to date was (15.14) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Table (4.51) the frequency and percentage for the Risks and opportunities of ISO implementation, assessment and treatment of information risk management

No	Items	Yes	No	Other
1	Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined	19	2	7
		67.9	7.1	25.0
2	Do secure areas have suitable entry control systems to ensure only authorized personnel have access	25	1	2
		89.3	3.6	7.1
3	Are processes to prevent malware spreading in place	24	1	3
		85.7	3.6	10.7

Source: IPM SPSS 24 package

From the above table result shows:

Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined by the (19) by (%67.9) answered yes، and(2) by (%7.1) answered no, and (7) by (%25.0) answered other.

Do secure areas have suitable entry control systems to ensure only authorized personnel have access by the (25) by (%89.3) answered yes، and(1) by (%3.6) answered no, and (2) by (%7.1) answered other.

Are processes to prevent malware spreading in place by the (24) by (%85.7) answered yes، and(1) by (%3.6) answered no, and (3) by (%10.7) answered other.

Table (4.52) chi-square teat results for the Risks and opportunities of ISO 27001:2013 implementation, assessment and treatment of information risk management

No	Phrases	Chi-square value	df	Sig.	Median	Interpretation
1	Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined	16.35	2	0.00	3.00	Yes
2	Do secure areas have suitable entry control systems to ensure only authorized personnel have access	39.50	2	0.00	3.00	Yes
3	Are processes to prevent malware spreading in place	34.78	2	0.00	3.00	Yes

Source: IPM SPSS 24 package

The results of table (4.52) Interpreted as follows:

1. The value of chi – square calculated to signify the differences between the Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined was (16.35) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
2. The value of chi – square calculated to signify the differences between the Do secure areas have suitable entry control systems to ensure only authorized personnel have access was (39.50) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.
3. The value of chi – square calculated to signify the differences between the Are processes to prevent malware spreading in place was (34.78) with P-value (0.000) which is lower than the level of significant value (5%) These refer to the existence of differences statistically.

Chapter Five

Results and Recommendations

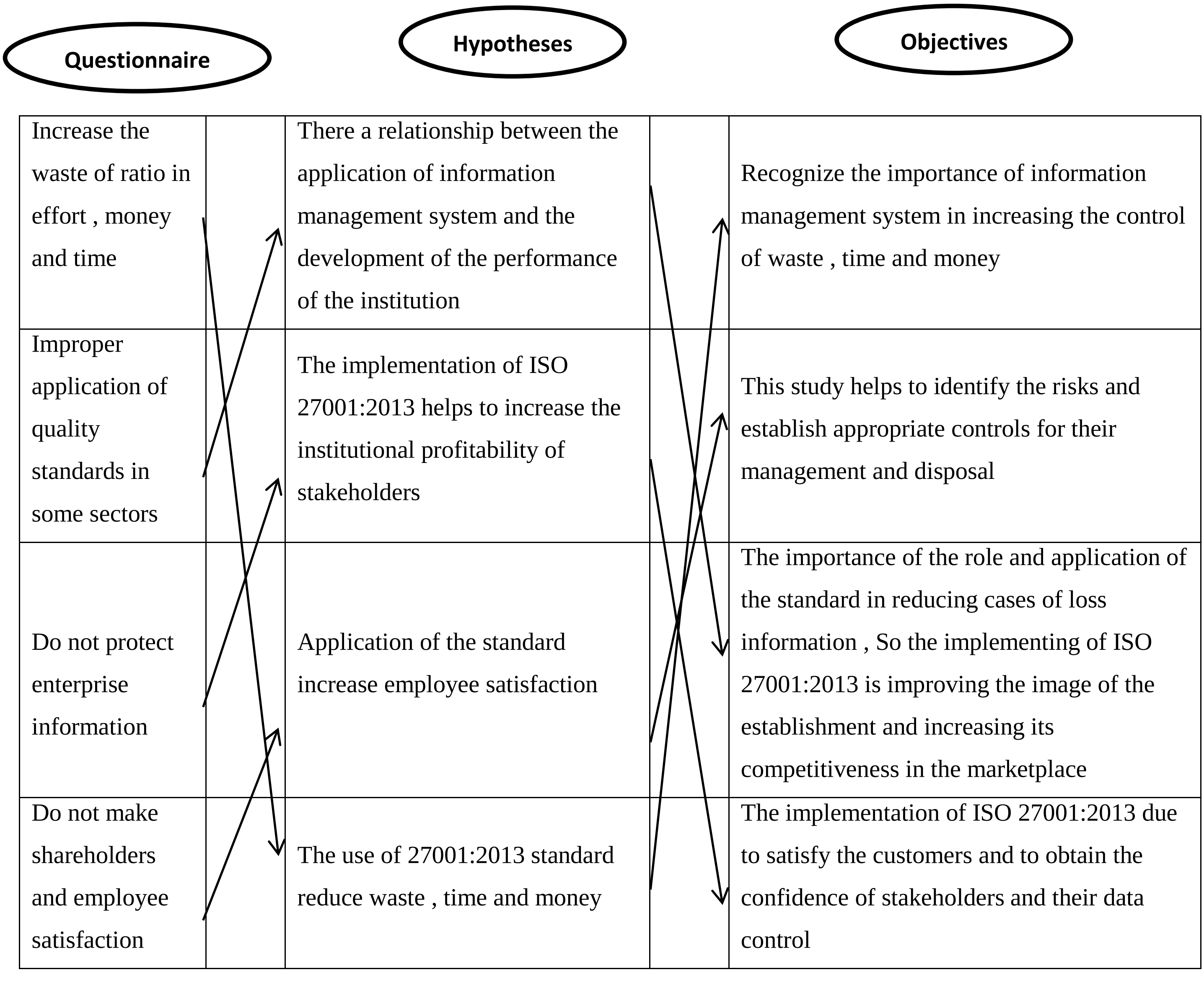
Chapter Five

Results and Recommendations

5.1 Introduction:

This chapter presents a discussion of the results that emerged from data collection methods, including interpretations that attempt to provide logical explanations in relation to the research aim and objectives. The findings are also related to the trends and developments outlined in the literature review in the first chapter. Also this chapter is aimed to summarize the conclusions of the study, acknowledge some limitations, and finally provide recommendations for further research.

5.2 Discussion of results:



Questionnaire		Hypotheses		Objectives
Increase the waste of ratio in effort , money and time		There a relationship between the application of information management system and the development of the performance of the institution		Recognize the importance of information management system in increasing the control of waste , time and money
Improper application of quality standards in some sectors		The implementation of ISO 27001:2013 helps to increase the institutional profitability of stakeholders		This study helps to identify the risks and establish appropriate controls for their management and disposal
Do not protect enterprise information		Application of the standard increase employee satisfaction		The importance of the role and application of the standard in reducing cases of loss information , So the implementing of ISO 27001:2013 is improving the image of the establishment and increasing its competitiveness in the marketplace
Do not make shareholders and employee satisfaction		The use of 27001:2013 standard reduce waste , time and money		The implementation of ISO 27001:2013 due to satisfy the customers and to obtain the confidence of stakeholders and their data control

This descriptive study was carried out to explore the barriers that have been encountered during ISO 27001:2013 standard implementation for the sample organization, determine critical barriers according to top management and employee view, and to recommend actions and measure to overcome these barriers.

So The researcher came to the following :

1. That standard of a relationship between the applications of ISO "Information Management System" affects to the development of performance of the institution.
2. That standard of the implementation of ISO 27001:2013 affects to increase the institutional profitability of stakeholders.
3. That standard of application to the standard affect to increases employee satisfaction.
4. That standard of the use of standard affect to reduce waste of time and money.

- **It has already been found that:**

There is a main role on the Information Management System in developing organization performance.

5.3 Recommendations:

The study recommended several recommendations:

1. Increase interest and awareness in the application of the concept Information Management System of electronic services, service and banking in the rest of telecommunications companies and banking banks and various private and public sectors.
2. The necessity of adopting other sectors to implement and develop the Information S Management System.

5.4 Suggestions for the researchers:

Conducting other studies that include dimensions not covered in the study Such as health, service, education and banking sectors.

References:

Books

1. Challenges and Innovations. Journal of Universal Computer Science, 18, 1598-1607.
2. Deutsch, W. (2014). 6 security policies you need: an introduction to creating effective security policies.
3. ISO 27001 uses a top down, risk-based approach and is technology-neutral
4. Related glossary terms: CESG Good Practice Guides (GPG), IISP (Institute of Information Security Professionals), Jericho Forum, Kitemark, Financial Services Authority (FSA), FTSE 100, UK Government Connect Secure Extranet (GCSX), UK Identity Cards Act This was last updated in September 2009 Posted by: Margaret Rouse
5. Slade, E. (2009). Top 3 Reasons Why Information Security & IT Maintenance is Important

Website

1. http://bizsecurity.about.com/od/creatingpolicies/a/6_policies.html
2. http://ishandbook. bsewall.com/risk/Methodology/IS.html (2009)
3. http://www.slideshare.net/charlesgarrett/ importance-of-a-security
4. http://www.howardcounty.com/Top_3_Reasons_Why_Information_Security_IT_Maintenance_is_Important-a-1224.html
5. http://www.jucs.org/jucs_18_12/an_overview_of_current/jucs_18_12_1598_1607_ editorial.pdf
6. https://www.iso.org/
7. http://www. securityorb.com/2013/10/c-i-a-triangle-security-concepts.html

Appendixes

بسم الله الرحمن الرحيم

جامعة السودان للعلوم والتكنولوجيا

كلية الدراسات العليا

استمارة استبيان

التاريخ : ...... /....../....... م

السلام عليكم ورحمة الله وبركاته

أرجو من كريم سيادتكم ملء الاستبيان المرفق علما بأن هذه البيانات تستخدم لغرض البحث العلمي فقط.

إن هذا الاستبيان معد لغرض الحصول على البيانات التي تتعلق بالجانب الميداني للبحث (التكميلي)لنيل درجة الماجستير في إدارة الجودة الشاملة والامتياز.

بعنوان:

The Role of " ISO Standard 27001:2013 " in Devolving Organization Performance

(دور معيار أيزو 27001:2013 في تطوير أداء المؤسسة)

ولكم جزيل الشكر

الباحثه : سكينه موسى سيد محمد مصطفي

البيانات الاساسية

Age	
a) Less than 30	( )
b) 30 – 40	( )
c) 41 – 50	( )
d) 51 – 60	( )
e) More than 60	( )

	العمر
( )	أ- اقل من 30
( )	ب- 30 – 40
( )	ت- 41 – 50
( )	ث- 51 – 60
( )	ج- اكبر من 60

Qualification	
a) Diploma	( )
b) Bachelor	( )
c) Higher diploma	( )
d) Master	( )
e) PHD	( )
f) Other	( )

	المؤهل
( )	أ- دبلوم
( )	ب- بكلاريوس
( )	ت- دبلوم عالي
( )	ث- ماجستير
( )	ج- دكتوراة
( )	ح- اخري

How long have you had your current position	
a) Less than 5 years	( )
b) 5 – 10	( )
c) 11 – 15	( )
d) 16 – 20	□ ( )
e) 21 - 25	( )
f) More than 25	( )

	عدد سنوات العمل في الوظيفة الحالية
( )	أ- اقل من 5 سنه
( )	ب- 5 – 10 سنه
( )	ت- 11 – 15 سنه
( )	ث- 16 – 20 سنه
( )	ج- 21 – 25 سنه
( )	ح- اكثر من 25 سنه

Wha is your position?	
a) Director of the Department	( )
b) Head of the Department	( )
c) Engineer	( )
d) Technical	( )
e) Other	( )

	الوظيفة
( )	أ- مدير إدارة
( )	ب- رئيس قسم
( )	ت- مهندس
)□ (	ث- فني
( )	ج- اخري

Scientific Specialization	
a) Telecommunication Engineering	( )
b) Computer Engineering	( )
c) Computer Science	( )
d) Information Technology	( )
e) Other	( )

	التخصص
( )	أ- هندسة إتصالات
( )	ب- هندسة حاسوب
( )	ت- علوم حاسوب
( )	ث- تقنية معلومات
( )	ج- اخري

How long have you worked in this organization?	
a) Less than 5 years	( )
b) 5 – 10	( )
c) 11 – 15	( )
d) 16 – 20	( )
e) 21 - 25	□ ( )
f) More than 25	( )

	عدد سنوات الخبرة في المؤسسة
( )	أ- اقل من 5 سنه
( )	ب- 5 – 10 سنه
( )	ت- 11 – 15 سنه
( )	ث- 16 – 20 سنه
( )	ج- 21 – 25 سنه
( )	ح- اكثر من 25 سنه

- **Part One :**

The relationship between the application of Information management system and the development of the organization performance

Statements	**Yes** **نعم**	**No** **لا**	**Other** **أخرى**	**العبارات**
1.1 The organization's leadership commitment to the ISO 27001:2013 demonstrated by : **1.1 إلتزام قيادة المنظمة بمقياس نظام إدارةأمن المعلومات :**				
1.1.1 Do Information Security policy exist?				1.1.1 هل توجد سياسة لأمن المعلومات؟
1.1.2 Are all policies approved by management?				**2.1.1** هل يتم اعتماد جميع السياسات من قبل الإدارة ؟
1.1.3 Are policies properly communicated to employees?				**3.1.1** هل يتم إبلاغ الموظفين بالسياسات بشكل صحيح ؟
1.1.4 Is there Establishing the information management policy and objectives, in consideration of the strategic direction of the organization, and in promotion of continual improvement?				**4.1.1** هل تم وضع سياسة وأهداف لإدارة المعلومات في النظر للإتجاه الاستراتيجي للمنظمة ونحو تعزيز التحسين المستمر ؟
1.1.5 Have measurable ISO 27001:2013 objectives and targets been established, documented and communicated throughout the organization?				**5.1.1** هل تم تحديد أهداف نظام إدارة أمن المعلومات بصورة قابلة للقياس ، وهل تم توثيقها بحيث يمكن تواصلها في جميع أنحاء المنظمة ؟
1.1.6 Ensuring resources are available for the ISO 27001:2013 , and directing and supporting individuals , including management , who contribute to its effectiveness?				**6.1.1** ضمان توافر موارد نظام إدارة أمن المعلومات ، وتوجيه ودعم الأفراد ،بما في ذلك الإدارة ، والذين يساهمون في فعالية الأداء ؟
1.1.7 Communicating the importance of effective information management system and conformance to ISO 27001:2013 requirements?				**7.1.1** إيصال أهمية إدارة نظام المعلومات الفعال و المطابقة لمتطلبات نظام ايزو 27001:2013 ؟
1.1.8 Are system policies subject to review?				**8.1.1**هل تخضع السياسات الأمنية للمراجعة ؟
1.1.9 Are the reviews conducted at regular intervals?				**9.1.1**هل أجريت المراجعات على فترات منتظمة ؟
1.2 Roles , responsibilities and authorities :				**2.1 القوانين والمسؤوليات والصلاحيات:**
1.2.1 Are the roles within the ISO 27001:2013 clearly defined and communicated?				**1.2.1** هل الأدوار داخل نظام أيزو 27001:2013 محددة بوضوح بحيث يسهل توصيلها ؟
1.2.2 Are the responsibilities and authorities for conformance and				**1.2.2** هل هنالك مسؤوليات وصلاحيات موضحة لتقييم وتقديم تقارير معتمدة عن أداء نظام أيزو 27001:2013 ؟

reporting on ISO 27001:2013 performance assigned?				
Access control 1.3 :				**1.3 التحكم في الدخول :**
1.3.1 Is there a documented access control policy?				**1.3.1**هل هناك سياسة موثقة لمراقبة الدخول ؟
1.3.2 Is there a formal user access registration process in place?				**1.3.2**هل هناك عملية تسجيل دخول رسمية للمستخدم في المكان؟
1.3.3 Is there a formal management process in place to control allocation of secret authentication Information?				**1.3.3**هل توجد عملية إدارة رسمية للتحكم في التعرف على المعلومات والتأكد من حمايتها وسريتها ؟
1.3.4 Is media in transport protected against un authorized access, misuse or corruption?				**3.1.4**هل وسائل النقل في مكان محمي ضد الوصول غير المصرح به أو سوء الاستخدام أوالفساد ؟
1.3.5 Are complex passwords required?				**1.3.5**هل كلمات المرور المطلوبة معقدة ؟

- **Part Two :**

The implementation of ISO 27001_2013 with increase the institutional profitability of stakeholders

Statements	**Yes** **نعم**	**No** **لا**	**Other** **أخرى**	**العبارات**
2.1 General Questions :				**1.2 أسئلة عامة :**
2.1.1 Have the internal and external issues that are relevant to the ISO, and that impact on the achievement of its expected outcome of the organization , and been determined?				**2.1.1**هل توجد قضايا داخلية وخارجية ذات الصلة بتطبيق نظام إدارة أمن المعلومات وهل هذا له تأثير على تحقيق نتائج المؤسسة المتوقعة ، وهل يتم تحديدها ؟
2.1.2 Has the organization determined the interested parties that are relevant to the ISO 27001:2013 ?				**2.1.2**هل حددت المنظمة الأطراف المعنية ذات الصلة بنظام إدارة أمن المعلومات؟
2.1.3 Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements?				**2.1.3**هل تم تحديد متطلبات هذه الأطراف المعنية ، بما في ذلك المتطلبات القانونية والتنظيمية والتعاقدية ؟
2.1.4 Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made?				**2.4.1** هل هناك إجراء يوثق متى وممن يتولى الاتصال بالسلطات المعنية (تنفيذ للقوانين وما إلى ذلك) ؟
2.1.5 Is there a process which				**2.5.1** هل هناك عملية تفصّل كيف ومتى يجب الاتصال؟

details how and when contact is required?				
2.1.6 Do all projects go through some form of information management assessment?				**2.6.1**هل تخضع جميع المشروعات لشكل من أشكال تقييم إدارة المعلومات؟
2.2Supplier relationship :				2.2 **العلاقة مع المورد:**
2.2.1 Is information management included in contracts established with suppliers and service providers?				**1.2.2**هل يتم تضمين أمن المعلومات في العقود المبرمة مع الموردين ومزودي الخدمات ؟
2.2.2 Are suppliers provided with documented management requirements?				**2.2.2**هل يتم تزويد الموردين بشروط أمنية موثقة ؟
2.2.3 Do supplier agreements include requirements to address information management within the service & product supply chain?				**3.2.2**هل تتضمن اتفاقيات الموردين متطلبات لمعالجة أمن المعلومات داخل سلسلة خدمة المنتج والمنتجات ؟
2.2.4 Are suppliers subject to regular review and audit?				**4.2.2**هل يخضع الموردون للمراجعة والتدقيق المنتظمين ؟
2. 3. Complains :				**3.2 . الشكاوي :**
2. 3.1 Has the organization identified and documented all relevant legislative, regulatory or contractual requirements related to management?				**1.3.2**هل حددت المنظمة ووثقت جميع المتطلبات التشريعية أوالتنظيمية أوالتعاقدية ذات الصلة المتعلقة بالأمن ؟
2.3.2 Does the organization keep a record of all intellectual property rights and use of proprietary software products?				2.2.3 هل تحتفظ المنظمة بسجل لجميع حقوق الملكية الفكرية واستخدام منتجات البرمجيات الاحتكارية ؟
2.3.3 Are records protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative regulatory contractual and business requirements?				**3.2.3**هل السجلات محمية من الفقد والتدمير والتزوير والوصول أوالإطلاع غيرالمصرح به وفقاً للشروط التعاقدية التشريعية والتزامنية التنظيمية؟

- **Part Three :**

The relationship between the application of ISMS and staff satisfaction

Statements	**Yes** **نعم**	**No** **لا**	**Other** **أخرى**	**العبارات**
3.1 Management responsibilities to employment :				**1.3 مسؤلية الإدارة نحو الموظفين :**
3.1.1 Are managers (of all levels) engaged in driving ISO 27001:2013 System within the business?				**1.3.1**هل يعمل المديرون (من جميع المستويات) في تعزيز نظام أيزو 27001:2013داخل الشركة ؟
3.1.2 Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply system in accordance with established policies and procedures?				**1.3.2**هل يؤدي سلوك الإدارة والسياسة إلى تشجيع جميع الموظفين ، المتعاقدين ومستخدمي الطرف الثالث لتطبيق النظام وفقًا لما هو محدد وفقا لسياسات والإجراءات ؟
3.1.3 Do all employees, contractors and 3rd party users undergo regular security awareness training appropriate to their role and function within the Organization?				**1.3.3**هل يخضع جميع الموظفين والمتعاقدين ومستخدمي الطرف الثالث للتدريب التوعوي الأمني المنتظم المناسب لدورهم ووظائفهم داخل المنظمة ؟
3.2. Human resources security :				**2.3 حماية الموارد البشرية :**
3.2.1 Are background verification checks carried out on all new candidates for employment?				**2.3.1**هل تجري اختبارات التحقق من الخلفية على جميع المرشحين الجدد للعمل ؟
3.2.2 Are these checks approved by appropriate management authority?				**2.3.2**هل تتم الموافقة على هذه الإختبارات من قبل سلطة الإدارة المناسبة ؟
3.2.3 Are all employees, contractors and third party users asked to sign confidentiality and nondisclosure agreements?				**2.3.3**هل يطلب من جميع الموظفين والمتعاقدين ومستخدمي الطرف الثالث التوقيع على اتفاقيات السرية وعدم الإفصاح ؟
3.2.4 Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role?				**3.2.4**هل هناك عملية لضمان إزالة حقوق وصول المستخدم عند إنهاء العمل أو العقد ، أو تعديلها عند تغيير دوره الوظيفي ؟
3.3. ISMS resources , competence , awareness and communication:				**3.3 المصادر، الكفاءة ، التوعية والإتصال بنظام إدارة أمن المعلومات :**
3.3.1. Is ISO 27001:2013 adequately resourced?				**1.3.3** هل توجد موارد بشكل كافي لنظام إدارة أمن المعلومات ؟
3.3.2. Is there a process defined and documented for determining competence for ISO 27001:2013roles?				**2.3.3**هل هناك عملية محددة وموثقة لتحديد الكفاءة المناسبة لأدوار نظام إدارة أمن المعلومات ؟
3.3.3. Are those undertaking ISO 27001:2013 roles competent, and is this competence documented				**3.3.3** هل هؤلاء الذين يقومون بأدوار نظام إدارة أمن المعلومات مختصين ، وهل هذه الكفاءة موثقة بشكل مناسب ؟

appropriately?				
3.3.4 Is everyone within the organization’s aware of the importance of the information management policy?				**4.3.3** هل كل شخص في المؤسسة يدرك أهمية سياسة أمن المعلومات ؟
3.3.5 Is there a documented process for terminating or changing employment duties?				**3.3.5**هل هناك عملية موثقة لإنهاء أوتغيير مهام التوظيف ؟
3.3.6 Are any information management duties which survive employment communicated to the employee or contractor?				**3.3.6**هل أي مهام أمنية متعلقة بالمعلومات التي تحمي تعاملات الموظف أو المتعاقد ترسل إليه ؟
3.3.7 Is the inventory accurate and kept up to date?				**3.3.7**هل يتم تخزين المعلومات بشكل دقيق ويتم تحديثها ؟

- **Part Four:**

The relationship between the application of ISO 27001:2013 and reduce of time and cost

Statements	**Yes** **نعم**	**No** **لا**	**Other** **أخرى**	**العبارات**
4.1 Risks and opportunities of ISO implementation , assessment and treatment of information security risk : **1.4المخاطر وفرص تنفيذ نظام إدارة أمن المعلومات وتقييم ومعالجة المخاطر التي تواجه أمن المعلومات :**				
4.1.1 Have actions to address risks and opportunities been planned, and integrated into the ISO 27001:2013 processes, and are they evaluated for effectiveness?				**1.1.4** هل لديك إجراءات لفرص معالجة المخاطر بشكل مخطط له ، وهل هنالك تكامل داخل نظام إدارة أمن المعلومات حيث يمكن تقييمه بشكل فعال؟
4.1.2 Has an information risk assessment process that establishes the criteria for performing information risk assessments, including risk acceptance criteria been defined?				**2.1.4**هل لديك عملية لتقييم مخاطر أمن المعلومات بحيث يمكن إنشاء ووضع معايير لتقييم تلك المخاطر ، بما في ذلك المخاطر التي تم تعريفها ووضع معايير مقبولة لها؟
4.1.3 Is the information risk assessment process repeatable and does it produce consistent, valid and comparable results?				**3.1.4** هل هنالك عملية لتقييم مخاطر أمن المعلومات وهل قابلة للتكرار بحيث تعطي نتائج متسقة وصحيحة وقابلة للمقارنة ؟
4.1.4 Does the information risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISO 27001:2013, and are risk owners identified?				**4.1.4** هل يتم تحديد عملية تقييم مخاطر أمن المعلومات المرتبطة بفقدان السرية والنزاهة وتوافر المعلومات في نطاق نظام إدارة أمن المعلومات ، وهل يتم تحديد أصحاب تلك المخاطر ؟
4.1.5 Has an information management risk treatment plan been formulated and approved by risk owners, and have residual information management risks				**5.1.4** هل لديك خطة لمعالجة مخاطر إدارة المعلومات وهل تمت صياغتها والموافقة عليها من المالكين ، وهل هناك أذن لحماية أدارة المعلومات المتبقية من قبل أصحاب المصلحة ؟

been authorized by risk owners?				
4.1.6 Is documented information about the information management risk treatment process available?				**1.4.6** هل المعلومات موثقة حول معالجة مخاطر أمن المعلومات وهل هذه العملية متاحة ؟
4.1.7 Do secure areas have suitable entry control systems to ensure only authorized personnel have access?				**4.1.7**هل توجد في المناطق الآمنة أنظمة ملائمة للتحكم في الدخول لضمان وصول الأفراد المصرح لهم فقط ؟
4.1.8 Have physical protection measures to prevent natural disasters, malicious attack or accidents been designed in?				**4.1.8** هل تم تصميم تدابير الحماية المادية لمنع الكوارث الطبيعية أوالهجمات الضارة أوالحوادث التي تم تصميمها ؟
4.1.9 Are processes to prevent malware spreading in place?				**4.1.9**هل هناك عمليات لمنع انتشارالبرمجيات الخبيثة في المكان؟
4.1.10 Is there a rigorous equipment maintenance schedule?				**1.4.10**هل هناك جدول زمني دقيق لصيانة المعدات ؟

بسم الله الرحمن الرحيم

جامعة السودان للعلوم والتكنولوجيا

كلية الدراسات العليا

استمارة استبيان

التاريخ : ...... /....../....... م

السلام عليكم ورحمة الله وبركاته

أرجو من كريم سيادتكم ملء الاستبيان المرفق علما بأن هذه البيانات تستخدم لغرض البحث العلمي فقط.

إن هذا الاستبيان معد لغرض الحصول على البيانات التي تتعلق بالجانب الميداني للبحث (التكميلي)لنيل درجة الماجستير في إدارة الجودة الشاملة والامتياز.

بعنوان:

The Role of ” ISO Standard 27001:2013 ” in Devolving Organization Performance

(دور معيار أيزو 27001:2013 في تطوير أداء المؤسسة)

ولكم جزيل الشكر

الباحثه : سكينه موسى سيد محمد مصطفي

البيانات الاساسية

Age	
f) Less than 30	( )
g) 30 – 40	( )
h) 41 – 50	( )
i) 51 – 60	□ ( )
j) More than 60	( )

العمر	
ح- اقل من 30	( )
خ- 30 – 40	( )
د- 41 – 50	( )
ذ- 51 – 60	( )
ر- اكبر من 60	( )

Qualification	
g) Diploma	( )
h) Bachelor	( )
i) Higher diploma	( )
j) Master	□)
k) PHD	( )
l) Other	( )

المؤهل	
خ- دبلوم	( )
د- بكلاريوس	)□ (
ذ- دبلوم عالي	( )
ر- ماجستير	( )
ز- دكتوراة	( )
س- اخري	( )

How long have you had your current position	
g) Less than 5 years	□ ( )
h) 5 – 10	( )
i) 11 – 15	( )
j) 16 – 20	( )
k) 21 - 25	( )
l) More than 25	( )

عدد سنوات العمل في الوظيفة الحالية	
خ- اقل من 5 سنه	( )
د- 5 – 10 سنه	( )
ذ- 11 – 15 سنه	( )
ر- 16 – 20 سنه	)□ (
ز- 21 – 25 سنه	( )
س- اكثر من 25 سنه	( )

What is your position?	
f) Director of□ he Department	( )
g) Head of□ he Department	( )
h) Engineer	( )
i) Technical	( )
j) Other	( )

الوظيفة	
ح- مدير إدارة	)□ (
خ- رئيس قسم	( )
د- مهندس	( )
ذ- فني	( )
ر- اخري	( )

Scientifi Specialization	
f) Telecommunication Engineering	( )
g) Computer Engineering	( )
h) Computer Science	( )
i) Information Technology	( )
j) Other	( )

التخصص	
ح- هندسة إتصالات	( )
خ- هندسة حاسوب	( )
د- علوم حاسوب	)□ (
ذ- تقنية معلومات	)□ (
ر- اخري	( )

How long have you worked in this organization?	
g) Less than 5 years	( )
h) 5 – 10	( )
i) □1 – 15	( )
j) 16 – 20	( )
k) 21 - 25	( )
l) More than 25	( )

عدد سنوات الخبرة في المؤسسة	
خ- اقل من 5 سنه	( )
د- 5 – 10 سنه	( )
ذ- 11 – 15 سنه	( )
ر- 16 – 20 سنه	( )
ز- 21 – 25 سنه	( )
س- اكثر من 25 سنه	( )

- **Part One : The relationship between the application of Information security management system and the development of the organization performance**

Statements	Yes نعم	No لا	Other أخرى	العبارات
1.1 The organization's leadership commitment to the ISO 27001:2013 demonstrated by :				**1.1 إلتزام قيادة المنظمة بمقياس أيزو 27001:2013 :**
1.1.1 Do Information management policy exist?				1.1.1 هل توجد سياسة لإدارة المعلومات ؟
1.1.2 Are policies properly communicated to employees?				**2.1.1**هل يتم إبلاغ الموظفين بالسياسات بشكل صحيح؟
1.1.3 Communicating the importance of effective information management and conformance to ISO 27001:2013 requirements?				**3.1.1** إيصال أهمية إدارة المعلومات الفعال و المطابقة لمتطلبات نظام أيزو 27001:2013 ؟
1.1.4 Are ISO 27001:2013 policies subject to review?				**4.1.1**هل تخضع السياسات الأمنية للمراجعة ؟
1.1.5 Are the reviews conducted at regular intervals?				**5.1.1**هل أجريت المراجعات على فترات منتظمة ؟
1.2 Roles , responsibilities and authorities :				**2.1 القوانين والمسؤوليات والصلاحيات:**
1.2.1 Are the roles within the ISO 27001:2013 clearly defined and communicated?				**1.2.1** هل الأدوار داخل نظام أيزو 27001:2013 محددة بوضوح بحيث يسهل توصيلها ؟
1.2.2 Are the responsibilities and authorities for conformance and reporting on ISO 27001:2013 performance assigned?				**1.2.2** هل هنالك مسؤوليات وصلاحيات موضحة لتقييم وتقديم تقارير معتمدة عن أداء نظام إدارة أمن المعلومات ؟
Access control1.3 :				**1.3 التحكم في الدخول :**
1.3.1 Is there a documented access control policy?				**1.3.1**هل هناك سياسة موثقة لمراقبة الدخول ؟
1.3.2 Is there a formal user access registration process in place?				**1.3.2**هل هناك عملية تسجيل دخول رسمية للمستخدم في المكان؟
1.3.3 Are complex passwords required?				**1.3.3**هل كلمات المرورالمطلوبة معقدة ؟

- **Part Two : The implementation of ISO 27001_2013 with increase the Institutional profitability of stakeholders**

Statements	Yes نعم	No لا	Other أخرى	العبارات
2.1 General Questions :				**1.2 أسئلة عامة :**

2.1.1 Has the organization determined the interested parties that are relevant to the ISO 27001:2013 ?				**2.1.1** هل حددت المنظمة الأطراف المعنية ذات الصلة بنظام أيزو 27001:2013 ؟
2.1.2 Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements?				**2.2.1**هل تم تحديد متطلبات هذه الأطراف المعنية ، بما في ذلك المتطلبات القانونية والتنظيمية والتعاقدية ؟
2.1.3 Is there a procedure documenting when, and by whom, contact with relevant authorities (laws enforcement etc.) will be made?				**2.3.1** هل هناك إجراء يوثق متى وممن يتولى الاتصال بالسلطات المعنية (تنفيذ للقوانين وما إلى ذلك)؟
2.1.4 Is there a process which details how and when contact is required?				**2.4.1** هل هناك عملية تفصّل كيف ومتى يجب الاتصال ؟

- **Part Three : The relationship between the application of ISO 27001:2013 and staff satisfaction**

Statements	**Yes** **نعم**	**No** **لا**	**Other** **أخرى**	**العبارات**
3.1 Management responsibilities to employment :				**1.3 مسؤلية الإدارة نحو الموظفين:**
3.1.1 Are managers (of all levels) engaged in driving management within the business?				**1.3.1**هل يعمل المديرون (من جميع المستويات) في تعزيز الأمن داخل الشركة ؟
3.1.2 Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply management in accordance with established policies and procedures?				**1.3.2**هل يؤدي سلوك الإدارة والسياسة إلى تشجيع جميع الموظفين ، المتعاقدين ومستخدميا لطرف الثالث لتطبيق التأمين وفقًا لما هو محدد وفق السياسات والإجراءات ؟
3.1.3 Do all employees, contractors and 3rd party users undergo regular security awareness training appropriate to their role and function within the Organization?				**1.3.3**هل يخضع جميع الموظفين والمتعاقدين ومستخدميا لطرف الثالث للتدريب التوعوي الأمني المنتظم المناسب لدورهم ووظائفهم داخل المنظمة؟
3.2. ISO 27001:2013 resources , competence Awareness and communication:				**2.3 المصادر، الكفاءة ، التوعية والإتصال بنظام أيزو 27001:2013 :**
3.2.1. Is the ISO 27001:2013 adequately resourced?				**1.2.3** هل توجد موارد بشكل كافي لنظام إدارة أمن المعلومات ؟
3.2.2 Is everyone within the organization's aware of the importance of the information management policy?				**2.2.3** هل كل شخص في المؤسسة يدرك أهمية سياسة إدارة المعلومات؟
3.2.3 Are any information management duties which survive employment communicated to the employee or contractor?				**2.3.3**هل أي مهام أمنية متعلقة بالمعلومات التي تحمي تعاملات الموظف أوالمتعاقد ترسل إليه ؟
3.2.4 Is the inventory accurate and kept up to date?				**2.3.4**هل يتم تخزين المعلومات بشكل دقيق ويتم تحديثها ؟

- **Part Four: The relationship between the application of ISO 27001:2013 and reduce of time and cost**

Statements	Yes نعم	No لا	Other أخرى	العبارات
4.1 Risks and opportunities of ISO standard implementation , assessment and treatment of information management risk : **1.4المخاطر وفرص تنفيذ معيار أيزو 27001:2013 وتقييم ومعالجة المخاطر التي تواجه إدارة المعلومات :**				
4.1.1 Has an information management risk assessment process that establishes the criteria for performing information management risk assessments, including risk acceptance criteria been defined?				**1.1.4**هل لديك عملية لتقييم مخاطر إدارة المعلومات بحيث يمكن إنشاء ووضع معايير لتقييم الأداء
4.1.2 Do secure areas have suitable entry control systems to ensure only authorized personnel have access?				**4.1.2**هل توجد في المناطق الآمنة أنظمة ملائمة للتحكم في الدخول لضمان وصول الأفراد المصرح لهم فقط ؟
4.1.3 Are processes to prevent malware spreading in place?				**4.1.4**هل هناك عمليات لمنع انتشارالبرمجيات الخبيثة في المكان؟
4.1.4 Is the information management risk assessment process repeatable and does it produce consistent, valid and comparable results?				**5.1.4**هل هنالك عملية لتقييم مخاطر إدارة المعلومات وهل قابلة للتكرار بحيث تعطي نتائج متسقة وصحيحة وقابلة للمقارنة ؟