UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES AND ACADEMIC ADVANCEMENT

Implementation of ISMS in Accordance ISO/IEC 27001/2013 at Oraconcept Information Technology Company

A Thesis

Submitted to the College of Graduate Studies and Academic Advancements

in Partial Fulfillment of the Requirement for the Degree of Master of Science in Information System

Prepared By:

Elhadi Ibrahim Hussien Arzoun

Supervisor By:

Dr. Azhari QismAllah

January 2016

Abstract

Organizations of all sizes rely on information and its quality to take informed decisions regarding on company strategy and objectives. To ensure good quality of information, organizations have to implement appropriate information security measures. Confidentiality, Integrity and Availability are three most relevant security requirements for quality of information. However ensuring them continues to be a challenge

ISO/IEC 27001 is the most used standard within the information security field. It is used by organizations that manage information on behalf of others and it is applied to assure the protection of critical client information. In general, applying ISO standards could be costly and require expert people or consultant.

This research tries to Implements the processes of Information Security Management System. In accordance with two International Standards, (ISO/IEC 27001) and (ISO/IEC 27002), at Oraconcept information technology company to Measure the activities required for a documented ISMS (information security management system) as much as possible and to be conformant with (ISO/IEC 27001), the Thesis focuses on obtaining the details of current situation of Oraconcept information technology company and the compliance level of it with ISO/IEC 27001. Focuses on issues at the IT department such as (System Security Requirements, Development and Maintenance) then providing some help for the problem of selecting the most efficient controls for the ISMS within Oraconcept information technology company by using the (PDCA) methodology (PLAN-DO-CHECK-ACT).

المستخلص

تعتمد المنظمات على المعلومات ونوعيتها في اتخاذ قرارات مستنيرة فيما يتعلق باستراتيجية الشركة وأهدافها. ولضمان نوعية جيدة من المعلومات فان الشركات تلجأ لتنفيذ تدابير امنية معينة لتضمن(سرية البيانات- سلامة البيانات- توفر البيانات).هذة العوامل تشكل أهم ثلاثة متطلبات لامن وسلامة المعلومات . غير أن ضمان سرية هذة المعلومات لا يزال يمثل تحديا.

(ISO/IEC 27001) هو اكثر المعاير استخداماً لضمان أمن المعلومات حيث تستخدمة المنظمات والشركات لضمان حماية المعلومات من عمليات الوصول غير المصرح والضياع .فأنة و بصفة عامة، فأن تطبيق معايير المنظمة الدولية للتوحيد القياسي (ISO) يمكن أن تكون مكلفة وتحتاج الى خبراء.هذا البحث يركز على تطبيق اجراءات نظام امن معلومات متوافق مع(ISO/IEC ٢٧٠٠١) و (ISO/IEC 27002) في شركة اوراكونسبت للتقنية المعلومات عن طريق تطوير الانشطة ومتطلبات نظام امن المعلومات.

هذا البحث يركز على جمع تفاصيل الوضع الراهن في شركة اوراكونسبت تقنية المعلومات في قسم تقنية المعلومات على مستوى التوافق مع معاير(ISO/IEC 27001) مع التركيز على القضايا المهمة (تامين نظم المعلومات و تامين تطوير نظم المعلومات و الصيانة) ثم تقديم المساعدة في اختيار الضوابط الفعالة التي تتناسب مع الاحتياج الحالي مع استخدام منهجية (PLAN-DO-CHECK-ACT)(PDCA).

1.1 Introduction

In small company there are issues of guarantying the secure of sensitive customer, financial and business. There is no Strategic information planning of budgets to cover the costs of securing assets like medium and big companies also the lack of budgeting will lead to not recruitment of professional staff in charge of information security which reflected negatively on the level of insurance of information. In business market information are very sensitive that why it's give a company competitive advantage that why information security management system is very important to establish even if it's not perfect isms can give customer and possible business partners a motivation to deal with company because they will know that there information's will be secured. (ISO/IEC 27001:2013) gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls (ISO/IEC 27001:2013).

(ISO/IEC 27001:2013) is a models used for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) , ISMS are achieved by applying a suitable set of controls (policies, processes, procedures, organizational structures, and software and hardware functions).This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls each clause defining security controls contains one or more main security categories(ISO/IEC 27001,2013)[1].

1.2 Problem Statement

Oraconcept is a software company which had the sources of systems and needed to be secured from staff and outsiders. Oraconcept had software sales Contracts and Annual maintenance Contract (AMC) with other companies which need ISMS in order to secure of sensitive companies, customer, financial and business information. The problem of Oraconcept Company that they had lack in budget in order to implement the (ISO-27001) and get the certificate .Rareness of professional staff how is in charge of information security which reflected on the level of information security.

Chapter one research Document define Research motivations, objectives of research, Methodology flown and the Expected outcome

1.3 Research Motivations

a. To analysis and Implement some of ISO-27001 controls and define the conformant of it in Oraconcept Information technology company
b. Define Risk plan and assessment to be conformant with ISO-27001
c. Use of ISO-27001 controls to reduce Information security risks and to comply with standards
d. Help to standard the work of an information technology companies with ISO-27001 information security management system(ISMS)
e. Oraconcept company manage Service level Agreements (SLA) which need Information Security Standard in order to Deliver Effective and Efficient information technology Services and software products
f. Study the Previous Implementations of ISO-27001 in companies.
g. Address Information security problems and risks and define treatment plans and information security policy in the information technology companies (Small and mid-size companies).

1.4 Research Objectives

a. To define scope and prepare planning to manage information security issues in the Information Technology companies (Small and mid-size companies) as case study Oraconcept information company a mid-size company with 8 years' experience in Sudan information technology market.
b. To measure the information technology companies comforting with ISO/IEC 27001 standard.
c. To using "Gap Analysis Method" to show current situation of the Oraconcept Information technology company Information Security Management system and define some of the gaps with ISO-27001 Standard controls

1.5 Scope Definition

Scope of the project will be identified by define the most critical parts of Oraconcept company Departments, work processes, technology used, information assets in Company even contracts with other companies according to risk assessment document and statement of applicability (SOA).

a. Decide Which Framework Will Be Used

There are various frameworks available the most widespread are ISO 27001 (for information security management), ISO/IEC 27002:2013 Code of Practice for Information Security Management. (ISO/IEC, 27002:2013)

b. . Identify Human And Assets Resources

Collect the data of the current recourses and the Information of the company such as the stocks data financial data and company client's data

c. Get The Management Support

It's very important to get the organization management desire to accomplish the project as planned before .this acceptance will lead to success the project[

1.6Methodology

The research is using ISMS cycle and it's known as PDCA model Methodology Shown in figure (1.1)

PLAN -DO -CHECK-ACT

A. Plan: Establish ISMS policy objectives processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives. Establish ISMS procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and business objectives.

1: Assign Oraconcept Responsibility for Information Security

2: Establish Information Security Governance

3: Perform a Gap Analysis

4: Develop a Project Implementation Plan

5: Identify and Classify Information Assets

6: Identify and Assess Risks

7: Plan for Risk Management

8: Develop an Agency Information Security Plan

9: Define Information Security Policy and Procedure Framework

10: Develop Information Security Policies

B. Do: Implement and operate the ISMS policy, controls, processes, and procedures.

11: Implement Risk Mitigation Strategy

12: Implement Agency Awareness Raising Program

13: Prepare an Incident Response Plan

14: Business Continuity and Disaster Recovery Plan

15:Check: Monitor and Review Information Security

C. Check**:** Assess and where applicable measure process performance against ISMS policy, objectives, and practical experience and report the results to management for review

16: Monitor and Review Information Security

D. Act: Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS

17: Maintain Information Security Management and ensure continual improvement [2].

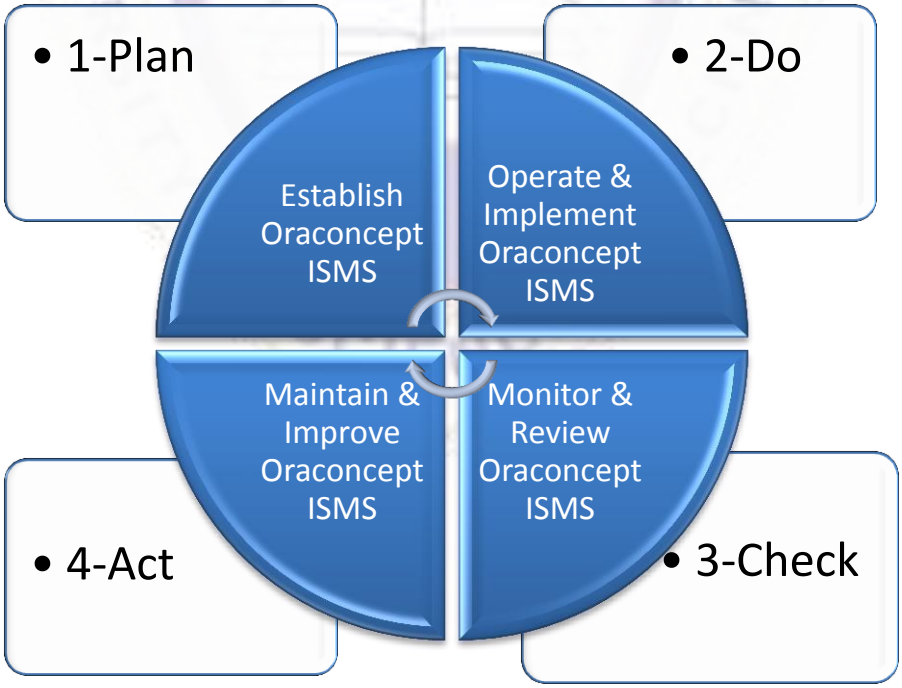

Figure (1.1): (PDCA) Methodology

1.7Expected Outcomes

Analysis and Develop Information Secuirty Management System Polices and procedures for Small& Mid-Size companies which improve business Process and define the Effectiveness and Efficiency of the Information Security Management System (ISMS) implementation using ISO-27001 Controls.

a. Improve Information Security Managements System
b. Try to Reduce expenses related to information security incidents
c. Create a Policies and Procedures for continual improvement of the information security using ISO-27001
d. Measure the Conformant of ISO-27001 standard Controls related to secure the Information in Oraconcept company.

1.8Research Structure

Chapter one (introduction) define the problem statement, research motivation, research objectives, methodology, expected outcomes and research structure.

Chapter two (Background) provides the related research on Information Security. Firstly, some basic concepts about Information Security will be given. Next, an explanation of what ISO/IEC 27001 and how they are used will be given.

Chapter three (Information Security Management System Requirements)concentrates on general information about the case study and Methodology, concept of ISO/IEC 27001 which are applied and the extracted documents.

Chapter four (ISMS Implementation) presents the Implementation of (PDCA) Methodology.

Chapter five (Conclusions and Recommendation) represents the results and the discussion of these results and recommendations for future works.