International Journal of Scientific Research in Multidisciplinary Studies
Vol.3, Issue.11, pp.4-13, December (2017)

Research Paper
E-ISSN: 2454-9312
P-ISSN: 2454-6143

Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen

A. A. Nasser

Dept. of information system, College of Science , Sa'adah University, Sa'adah, Yemen

Corresponding Author: adelru2009@mail.ru, Tel.: +967-772417767

Available online at: www.isroset.org

Received: 05/Nov/2017, Revised: 20/Nov/2017, Accepted: 12/Dec/2017, Published: 31/Dec/2017

***Abstract*—** This Information is one of the most important assets of the company. Protecting information requires a broad range of controls. Organizations should make sure that they are covering the full range of controls needed to protect the confidentiality, integrity, and availability of business information from the full range of threats. ISO/IEC 27001:2013 is one of the leading standards of information security. It is the code of practice including 114 controls in 14 different domains. This research was conducted to find out the level of information security in the Yemeni Academy for graduate studies (YAGS) regarding the compliance of implementation of this standard. The results showed maturity level of information security in the YAGS is at level 2. The value of the gap between the value of the maturity level of the current and expected level of maturity value is 3.19. This mains that many control weaknesses exist, related security policies and procedures should be developed and security management system and culture should be implemented. The detailed results of benchmarking based on the ISO27001 standard, the method used to measure the maturity level for each security control domain, and the improvement recommendations are presented.

***Keywords*—** Gap analysis; Compliance; ISO 27001; Maturity level; Maturity model

I. INTRODUCTION

The development in information and communication technology has created a significant leap in improving business's efficiency and accuracy and increasing its productivity. Moreover, IT assets – such as data, networks, hardware, and software – is now considered as one of the resources and essential operators of successful business organizations in the twenty-first century[1,2,3]. These organizations are increasingly dependent on such information assets in the implementation of their activities and commercial operations[4,5]. At the same time, there emerged the negative side of using technology since it opened the way for the development of the methods of informational threats such as breaching the safety, availability and confidentiality of the organizations' information assets and expanded the range of internal and external risks and threats, which these organizations face. As a result, the challenges of information security are increasing in the light of the rapid technological development.

Furthermore, their economic, political and security consequences increase as the organizations go further in adopting technologies and computerized systems. The increase and consequences of these threats and risks are inversely proportional to the modernity and efficiency of security means and strategies followed by these enterprises to protect their information assets. Hence, protecting the organizational information assets, increasing the reliability of their systems and technologies, searching solutions for these challenges which bear many complexities - and which include the technological, organizational and human (cultural) aspects – is incumbent upon the organizations and researchers in this field.

The Yemeni Academy for Graduate Studies – one of the modern educational institutions, based in Sanaa, Yemen that provide learning services in graduate studies - like any other modern intuitions that use information systems and technologies in operating their work, could be exposed to internal and external security threats and risks. Therefore, it has to take the required measures to protect its information assets through integrated strategies, which include the application of information security management systems besides the application of information security culture as a part of its organizational culture[1,6,7,8,9,10,11,12].

A. Research problem:

Information technology administration at the Yemeni Academy for Graduate Studies works closely with the different administrations at the academy and relies on technological solutions in computerizing the institution's operations. However, the existence of security gaps in its systems could be a major source of threats to which the institutions security system may be subject, and affects the confidentiality, safety and availability of its vital assets which otherwise must be secured. Moreover, lack of awareness about using these technologies, and the improper ways employees handle information and its technologies - with or without intent – may result in no less damages than those of the previous ones, especially when the employee has access to data of high sensitivity such as accounts and students' data and their academic records. The administration has a special plan to protect the assets or reduce the risks that may threaten them but without a systematic risk assessment. Hence, the academy is in urgent need to improve its information security system according to international standards. The first step to achieve this is self-assessment of the reality of information security known as gap-measurement[13,14]. From the main problem of the research, the following sub-problem is formulated:

What the is the gap in the actual situation of information security at The Yemeni Academy for Graduate Studies according to the international standard (ISO/IEC:27002:2013)?

From this problem arises the following questions:

- To what level does The Yemeni Academy of Graduate Studies comply with the requirements of information security in international standards ISO / IEC: 27001: 2013?
- What is the size of the gap between the actual level of information security practices at the Yemeni Academy and the level that the Yemeni Academy of Higher Studies seeks to achieve according to the requirements of ISO / IEC: 27001: 2013?
- What controls are the most vulnerable points bringing about potential threats, and what solutions can be recommended to improve them?

B. Study Objectives:

This research aims at finding out the information security practices at the Yemeni Academy for Graduate Studies and assessing the extent of their compliance with the requirements of information security. It, also, attempts to measure the gap between the actual level of information security practices at the academy and the level it seeks to achieve in compliance with the requirements of ISO / IEC: 27001. Moreover, the study aims to discover the fields of control that represent vulnerable points in their security practices and set the necessary recommendations to enhance the compliance to the standards, reduce the gap and improve the information security practices.

C. Significance of the Study:

1) Theoretical significance:

The significance of this study emerges from the significance of the topic it deals with, i.e. information security according to ISO/IEC:27001 standard. It is significant as it sheds the light on the issue of information security in the different fields of control, which this standard provides. What, also, makes it significant is the importance of information assets and the consequences if security breaches occur at institutions and systems. It becomes even more significant in the environment under investigation (The Yemeni Academy for Graduate Studies), which is considered as one of the most important pillars of higher education in Yemen. Moreover, this research would benefit the employees in IT Management at the academy, and would contribute in raising their awareness on how to deal with this subject so as not to be an obstacle that limits the academy's efficiency.

Furthermore, the study is significant as it enhances the understanding of managing self-assessment of information security, ensuring a proper management of information security, which ensures the continuity of work. Information security is no longer an issue that each institution's technicians handle separately. Rather, it is handled by politicians, strategists and decision makers who translate it into policies and strategies.

2) Empirical Significance: The study's empirical significance resides in the following:

- Spotlighting the vulnerabilities and how to encounter them
- Providing the academy with conditions and procedures that should be followed to improve its level of information security and the results IT IS HOPED TO YIELD and which may contribute in improving the policies of information security.
- Preparing a working plan for the application of international standards for information security at the Yemeni Academy for Graduate Studies in case a certificate of information security is to be obtained.
- The academic importance represented in training students on how to evaluate the actual level of security at institutions as part of the requirements of the syllabus of information security policies for the program of Master in Information Management Systems at the academy.

D. Study Limits:

1) *Thematic Limits:* The study is limited to attempting to find out the measure of the gap and the extent of compliance of information security practices at the Yemeni Academy for Graduate Studies with the requirements set by the international information security standard (ISO 27001:2003).
2) *Spatial Limits*: The study was limited to The Yemeni Academy for Graduate Studies, Sanaa
3) *Time Limits:* This study was conducted during the period from April to June 2017.

E. Study Sample:

IT management office at the Yemeni Academy for graduate studies is the targeted sample in this study.

The rest of paper is organized as follows, Section I contains Introduction, Section II contains the review of previous related work in various resent security analysis, standards, and maturity models, Section III describes methodology of research, Section IV contains results , discussion and recommendations for improving the information security management in the YAGS, Section V contains conclusions of research work, Section VI describes the future scope. The last section contains the references.

II. LITERATURE REVIEW:

A. The Importance of the information security assessment

There are several studies on the development of information security systems and culture at organizations, and all of them agree on the importance of applying information security systems and culture by going through a proper life cycle to achieve its desired goals. The most significant conclusions these studies have shown are:

- Information security systems are of great importance for business organizations as they become the main key to planning and management in modern enterprises to endure the safety, availability and confidentiality of information [2,13,14,15,16]. They, also, has to pay close attention to their administration BY designing and implementing information security strategies in an active and effective way[7].
- the appropriate rules should be taken for establishing and applying the systems in order to encounter the internal and external risks to which the organization might be exposed[6,14];
- Technical solutions are important for the institution and should be implemented properly to combat threats and risks or to automatize some processes such as the application of firewalls in institution's system[1,6,7,14].
- Technical solutions need to be operated and managed by people; implementation of information security technical solutions is not enough for protection. The effectiveness of information security controls depends upon the efficiency of people who implement them and who are in charge of their use, and on the efficiency of the administrative policies and practices[1,11,12].
- Users are in continuous interaction with technologies and information assets to carry out their tasks and duties, and the risks user-oriented risks have more impact on the enterprise compared to external risks[1,8,9,10].
- Organizations need to adopt an integrated strategy that combines information security and organizational culture by establishing security practices and procedures as documented practical and technical bases for protection from information security risks that beset their business and technical infrastructure[[1,6,7,8,9,10,11,12]. This is supported with procedures that determine the detailed steps to be followed on how to carry out tasks based on technical and theoretical knowledge to prevent any external security breaches, and through the application of information security culture - such as the practices that determine the mechanism in which controls are implemented - and working on it by the user, which help in protection from the risks of internal threats and breaches.
- The internal and external security threats made the international organizations seek to adopt specific security policy standards [2,13,14,15,16] that draw up an integrated policy to put the concept of information security into practice at institutions, from analysis of risks to the application of security controls to minimize these risks.
- Assessment of information security risks applicable to any organization depends heavily on the nature of its business and its technical structure. Therefore, identifying information security risks and areas of related policy that apply to Yemeni institutions requires an understanding of the practical and technical aspects of these institutions, and the categorization of policies is done depending on a set of their own controls such as access control and continuity of work and compliance with international standards.

- Many of the best practices for information security management have been develop. Most important of these are Developed several best practices for information security management, the most important of which is the ISO 7799 standard, the updated version of the ISO 27000 standard, Control Objectives for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL), national guidelines for information security such as (NIST 800-53), etc. Studies [2],[13,14,16],[13] have shown that the application of these standards and guidelines is constantly increasing worldwide for the sake of improving the level of information security in the institutions and, in particular, to meet the requirements imposed on these institutions by legal and auditing institutions, national or international. It revolves around the need to follow a set of security compliance regulations during the implementation of the structure of information security management in the organizations business [6].

We conclude from the above that the subject of the research problem is of utmost importance and that the assessment of the security situation is part of the system of information security management. It is the first step in the management of information security risks to identify vulnerabilities in the information security systems at the enterprise, it helps determine the type of protection strategies and policies to be taken and their priorities, and it must be based on an appropriate international standard.

B. Gap analysis

Compliance is the process of comparing the actual information security operations of organizations with international ISM legal, regulatory, and internal requirements relevant to the organization, In this case, it is a reference to the standards and laws related to information security. COBIT, ISO27K, and ITIL are examples of standards. [16,18]. Evaluation the information security compliance level in organizations with internationally recognized standards is growing in importance, because it has become popular as a common basis for information security measurement, [2,13,14,15,16,17]. The compliance has the greatest effect on information security policy compliance[17], evaluates and audits the difference between the expected standards of organizational situations, and the reality in the organization [16] helps organizations determine their conformity to the controls listed in this standards [16,19]and delivers useful outputs to the certification process for the next stage of ISM certification [16]. For our case study, the compliance is the process of comparing the applied security controls at the YAGS with those in ISO27001. The Gap analysis is a tool or a technique that enables an organization to compare its actual performance with the standards [14].

C. ISO 27001:2013

There are common international security standards available, these standards provide systematic management approach to adopt the best practice controls, quantify the level of accepTable risk and implement the appropriate measures which protect the confidentiality, integrity, and availability (CIA) [6]. BS7799, (COBIT), (ITIL) and NIST 800-53 [5].BS 7799 standard was established by British Standard Institute (BSI) in 1995 [11]. ISO 17799 has been derived from BS7799 in 2000. ISO 17799 Part 2 (2002) established the code-of-practice and the specifications of an Information Security Management System (ISMS) [6,20].

ISO/IEC 27001 is the international standard for information security management which defines a set of controls and requirements to establish, implement, operate, monitor, review, maintain and improve an information security management system (ISMS). ISO/IEC 27001-2005 has been prepared to reemphasize the code-of practice of ISO 17799 with few Amendments and additions of controls that will enhance and improve the ISMS further [6,21]. The ISO/IEC 27001:2013 Standard is the second edition of the standard and replaces the first edition ISO/IEC 27001:2005 Standard.

ISO27001 has a key characteristic that it:

- Covers all types of organizations, irrespective the size of organization [13,22,23,24];
- Defines the key elements of information security management defines the key elements of information security management and also the ways it is implemented and maintained [2];
- Provides guidelines obtain international certificates from a third party [20,21,23,24];
- It was to prove that the security controls exist and operate in accordance with the requirements of the standard [23,24];
- Describes the system as the overall management of business risk approach that aims to establish, implement, operate, monitor, and maintain ISMS [14,23,24].

It is therefore important for the YAGS as a small size organization, to evaluate their information security compliance level, comparing their actual information security operations controls with those in ISO27001:2013. ISO/IEC 27001: 2013, domain requirements and security controls. Security controls have 14 security control clauses, 35 Control Objectives and Controls have 114[25], can be seen in Table 1.

D. Maturity Model

The idea of information security standards that have models with measurable effects on the business becomes more present in practice and more respected by experts [26]. Maturity models defined as a structured collection of elements that describe the characteristics of effective processes or products [27], It also defines the order in which security elements must be implemented, encourages the use of standards of best practices and provides a means to compare security programs[14], used regularly in the field of Information Systems as an approach for organizational assessment [14,28] as a benchmark comparison tool to evaluate the ability of organizations to meet the objectives of security [29]. Any systematic framework for carrying out benchmarking and performance enhancement that has continuous improvement processes, can be considered a Maturity Model [14]. in the constituent literature, a maturity model used to describe, explain and evaluate growth life cycles, can be used for assessing and/or achieving compliance since they allow the measurement of a maturity level and, by identifying the gap between the current and pursued level[7], helps to understand the effects that are expected from the organization [26], allows the planning of efforts, priorities and objectives in order to achieve the goals proposed, and identifies project or organizational strengths, weaknesses and benchmarking information [30]. Thus, Maturity implies perfect or explicitly defined, managed, measured, and controlled systems. In general, maturity models have the following properties [31]:

- The development of a single entity is simplified and described with a limited number of maturity levels (usually four to six);
- Levels are characterized by certain requirements, which the entity has to achieve on that level;
- Levels are ordered sequentially, from an initial level up to an ending level (the latter is the level of perfection).

There are common mature modules available and these are NIST, GISM, ISM3, CITI-ISEM, COBiT, OISM3, SSE/CM, and CERT/CSO. The COBIT maturity model is widely used for IT governance, and for the purpose of this study, it was decided to use the COBiT model, because it is focused toward auditing specific procedural awareness and adaptation [14, 32,33] and presents a set of indicators, which are more focused on the controls of activities than in their execution. These controls assist in optimizing the IT investment, provided measures to ensure servicing and administering standards of measurement to assess when there is an error in its use , help management full its IT governance responsibilities[14] and allows the organization to measure its current maturity level against a specific standard[7], in this case, ISO27001.

Table I. Security Objective (O) And Control(C) Numbers For Each Clause Iso/Iec 27001: 2013

Clauses	O	C
A.5 Information security policies management	1	2
A.6 Organization of information security	2	7
A.7 Human resource security	3	6
A. 8 Asset management	3	10
A.9 Access control	4	14
A.10 Cryptography	1	2
A.11 Physical and environmental security	2	15
A.12 Operations security	7	14
A.13 Communications security	2	7
A.14 System acquisition, development and maintenance	3	13
A.15 Supplier relationships	2	5
A.16 Information security incident management	1	7
A.17 Information security aspects of business continuity management	2	4
A. 18 Compliance	2	8

III. RESEARCH METHODOLOGY

The study has used the analytical descriptive method to analyses the existing system and identify its compliance with the international information security standard. it, also, has applied case study method, through which relevant data has been collected.

This part describes how research, where there are details about the material or the materials, tools, sequence of steps to be made in a systematic, logical so it can be used as underlines, are clear and easy to resolve the problems, analysis of results and the difficulties encountered. The sequence of steps problem-solving research are:

- Define the objective of research ;
- Literature review ;
- Design of the searching tool used for data collection;
- Data analysis; and
- Finding and recommendation's

This approach toward a detailed security maturity model takes a management systems approach. It involves the compliance and the gap of the 114 controls in 14 (domains) which comprise the ISO27001. The maturity values are determined by the security requirements of the organization. During implementation two issues needed to be addressed the questions and their maturity values. This was resolved by designing the questions using the ISO27001 standard controls and carefully determining and agreeing on their maturity values (weight). Each control has a statement of application, which was converted to the questions

(statements), questions were asked, and then we made maturity value of each answer. The control maturity values are the average of maturity values of its questions and the clause maturity values are the average of maturity values of its controls. Some examples of the extracted question's regarding the control's requirement, are presented in Table2, the list of agreed COBiT maturity values, their descriptions and maturity levels assessment criteria represented in Table 3.a and 3.b [6,34]. This model has its measurement basis supported by the maturity scale of COBiT. [6]. The maturity values was achieved by surveying and interviewing the relevant responsible people in the YAGS (IT department manager, this department is responsible for all data processing operations in the YAGS, Human resource manager and Data Entry consultants), to have a clear picture of the all processes and conditions, together with the review of documentary evidence in order to verify the compliance level of the main clauses, and the controls of Annex A in the standard. Some examples of the extracted question's regarding the control's requirement can be seen in Table 2, in Tables 3.a and Tables 3.b shown the description of maturity values and the Maturity level Assessment Criteria.

Table 2.Some examples of the extracted question's regarding the control's requirement

Controls	Q
A.7.1.1	1. Are background verification checks carried out on all new candidates for employment? 2. Are these checks approved by appropriate management authority? 3. Are the checks compliant with relevant laws, regulations and ethics? 4. Are the level of checks required supported by business risk assessments?
A.7.1.2	1. Are all employees, contractors and third party users asked to sign confidentiality and nondisclosure agreements? 2. Do employment / service contracts specifically cover the need to protect business information?

Table 3.A .maturity values and their description

Maturity value-level	Description
0 – Non Existent	There is no recognition of the need for internal control.
1– Initial / Adhoc	There is some recognition of the need for internal control.
2 – RepeaTable But Intutive	Controls are in place but are not documented.
3 – Defined Process	Controls are in place and are adequately documented.
4 – Managed and Measurable	There is an effective internal control and risk management environment
5 - Optimized	An organization wide risk and control program provides continuous and effective control and risk mitigation.

TABLE 3.b .Maturity Level Assessment Criteria

Maturity Index	Maturity Level
0 – 0.50	0 – Non Existent
0.51 -1.50	1 – Initial / Adhoc
1.51 – 2.50	2 – RepeaTable But Intutive
2.51 – 3.50	3 – Defined Process
3.51 – 4.50	4 – Managed and Measurable
4.51-5.00	5 - Optimized

Based on the obtained information, we made compliance analysis. The current levels of compliance with the principle of the code of practices have been categorized using the following definitions:

- Compliant: The organization is fully compliant with the specific are of ISO27001.
- Partially compliant: The organization has gone some way towards being compliant, but still requires additional work to be undertaken.
- Non-compliant: The organization does not have the controls in place to satisfy the requirement of ISO27001.

Finally, the step is finding the results of the maturity benchmarking against ISO27001, and the scores used for benchmarking are explained below:

- Maturity score below 1.65: The organization should start implementation of overall security measures.
- Maturity score between 1.66 and 3.25: The organization has taken significant steps to enhance security.
- Maturity score above 3.26: The organization fulfils defined measures, thus the probability of high risks is marginal.

IV. RESULTS AND DISCUSSION

A. Summary Of The Maturity Level

The respondent's calculation summary per clause by using Descriptive methodology obtained a result as shown in Table 4 and figure 1.

Table 4. Summary of the Value Maturity Level per Clause

N	Clause	Maturity Index	ML
1	A5	0.00	0
2	A6	1.25	1
3	A7	2.00	2
4	A8	1.86	2
5	A9	3.15	3
6	A10	0.50	0
7	A11	3.36	3
8	A12	3.03	3
9	A13	1.50	1
10	A14	2.11	2
11	A15	2.33	2
12	A16	0.57	1
13	A17	2.17	2
14	A18	1.60	2

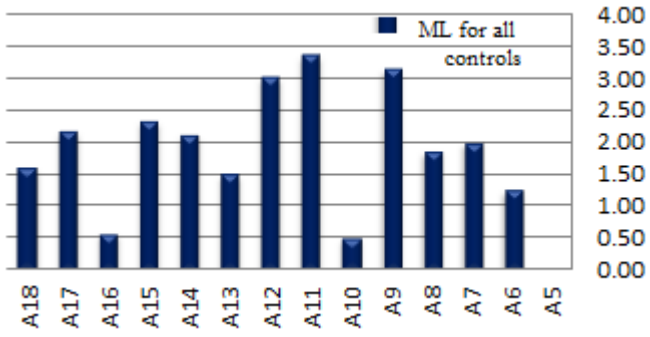

Fig 1. Measurements graphs in maturity level per clauses

Table 5 shows the compliance level for all the 144 requirement controls, and it can be seen that:

- 5.26 % of the controls that were reviewed found out to be compliant with ISO27001 standards.
- 84.21 % of the controls that were reviewed found out to be partly compliant with ISO27001 standards.
- 10.53 % of the controls that were reviewed found out to be non-compliant with ISO27001 standards.

Table 5.Domain compliant level

Domain	Req. controls	compliant	Partly compliant	Non compliant
A5	2	0	0	2
A6	7	0	5	2
A7	6	0	6	0
A8	10	0	10	0
A9	14	2	11	1
A10	2	0	1	1
A11	15	0	15	0
A12	14	4	9	1
A13	7	0	6	1
A14	13	0	12	1
A15	5	0	4	1
A16	7	0	6	1
A17	4	0	4	0
A18	8	0	7	1
total	144	6	96	12

The result shown in Figure 1 indicates that some of the controls are more mature than others; it is evident that A5 controls show 100 % non-compliance, this is due to the nonexistence of an approved security policy. It can be seen that the controls A-10 exhibit 50 % of non-compliance, and once again this is due to the lack of implementation of effective security policy for the using of cryptographic controls within these domain controls. it is also evident that 84.21 % of the controls that were reviewed found out to be partly compliant, show high percentage of partly compliance in 92.85 % of domains exhibit more than 50 % of non-compliance, 30.76 % of them (A7, A8, A11, A17) show 100% partly compliance, and this due to that, the organization has gone some way towards being compliant, but still requires additional work to be undertaken. While the 5.26% of the controls within 14.28 % of domains(A12, A9) seems to have low percentage of compliance, not above than 29%, this is due to internal security procedure being put in place by the team responsible for user registration, secret authentication information usage, information backup, logging and monitoring sections, . While the 94, 74 % of controls, within 85.72% of domains, have seemed to have the lowest (0) percentage of compliance. Which means the very high compliance distance between the current conditions with the standard.

After knowing the maturity level of information security for all controls, and determining the expected maturity level, which equals 5 (Optimized), as a compliance goal level in the YAGS. Then the value gap for each clause are gotten then averaged to obtain the value of the overall gap. The summary value gap of all controls per clauses can be seen in Table 6.

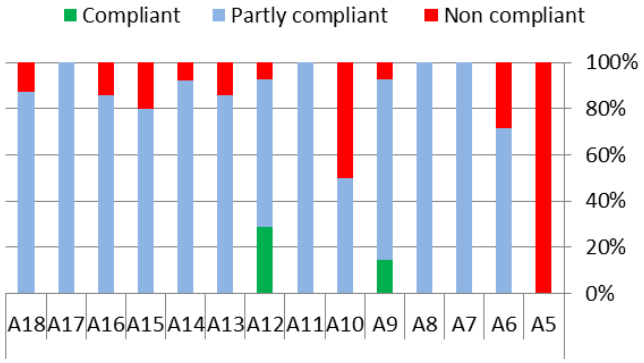

Fig 2 Gap analysis compliance level

Table 6 Summary of The Maturity Level gap per clause

N	Clauses	Maturity Level		
		Current	*Expected*	*Gap*
1	A5	0.00	5.00	5.00
2	A6	1.25	5.00	3.75
3	A7	2.00	5.00	3.00
4	A8	1.86	5.00	3.14
5	A9	3.15	5.00	1.85
6	A10	0.50	5.00	4.50
7	A11	3.36	5.00	1.64
8	A12	3.03	5.00	1.98
9	A13	1.50	5.00	3.50
10	A14	2.11	5.00	2.89
11	A15	2.33	5.00	2.67
12	A16	0.57	5.00	4.43
13	A17	2.17	5.00	2.83
14	A18	1.60	5.00	3.40
avg	All	1.81	5.00	3.19

Figure 3 displays the results of a gap analysis of maturity levels for all domains, comparing value maturity level current and expected per clause.

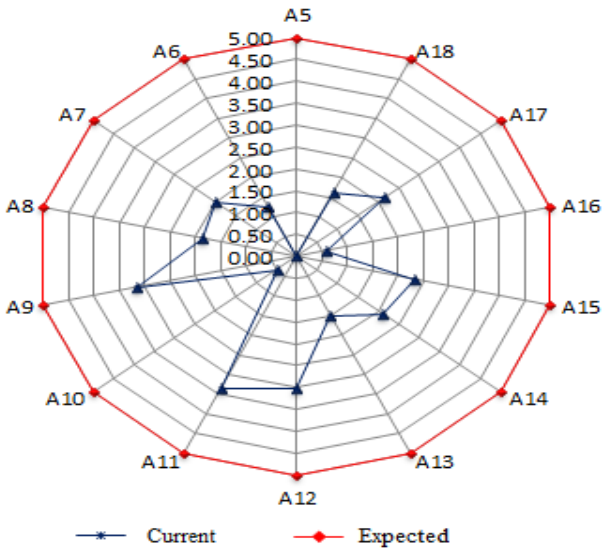

Fig 3 Comparing value maturity level current and expected per clause.

The result shown in Figure 3, displays the results of the maturity benchmarking against ISO27001.It is obvious that some of the controls are more mature than others, the score of only 7.14% of domains (A11) lies above 3.26. This that's means, The YAGS fulfills defined physical and environmental security measures, thus the probability of high risks is marginal in this section, it also can be seen that the score of 35.71 % of domains, lies below 1.65. This is due to the nonexistence of an approved security policy in general and policy for the specific purposes: using of cryptographic controls, the information transferring, supplier relationships, mandating the implementation and assessment of security controls and policy compliance. It is also due to the nonexistence of procedures for some controls: contacting with authorities, security assessment projects, responsibility management and information transfer. Also, this due to the lack of implementation of internal security procedure for communications security and incident management. Other domains score lies between 1.67- 3.25. This implies that some steps have been done to improve the security in related domain.

The results obtained from the measurement of the level of Maturity for information security in the YAGS is level 2 (repeaTable but intuitive). Results of the questionnaire management to obtain an average value for all of the clauses is 1.81 range of 0 to 5. And the value of the gap between current security conditions and the condition of the expected 3.19. From this value can be concluded that the security information on the second level, is repetitive but intuitive. Thus the results of the analysis means that the procedure contained in the delivery and support of control have been developed in the process to handle the task, and followed by everyone involved. No approved security policy in general and no policy for the using of cryptographic controls, the information transferring, supplier relationships, mandating the implementation and assessment of security controls and policy compliance. No procedures for contacting with authorities, security assessment projects, responsibility management and information transfer. There is a lack in the implementation of internal security procedure for communications security and incident management. The gap analysis is initially used to identify the weaknesses in the organization's procedures, the security that can be achieved through technical means is limited, and should be supported by appropriate policies and procedures. Identifying which controls should be in place requires careful planning and attention to detail. The non-existence or a lack of implementation of policies and procedures in the sections discussed in the previous results may cause : weakness in employees participation in organizational efforts, needed to preserve the information assets; Increasing the external and internal risks that the institution may face as a result of gaps in its security system, and difficulties in identifying the sensitive information systems and resources and protection methods necessary for them. And for solving this, the YAGS should start implementation of overall security measures, some recommendations are:

- Planning and determining the scope of public and specific systems most important policies and procedures according to their objectives.
- Conducting the self-assessment of risk for the specific systems policies development. While for the general policies development, the results of the evaluation can be determined based on the results of this research.
- Evaluation the risks of information security systematically, classified of risk according to the priority of implementation based on specific qualitative and quantitative factors.
- Conducting an Information Security Culture Assessment (ISCA to reduce the risk that employee behavior poses to the protection of information and to ultimately inculcate a compliance culture with fewer incidents (institutionalization wave).
- Developing Policies and procedures according to the results obtained in the evolution phases

V. CONCLUSION

An information security management system is an great importance for business organizations as they become the main key to planning and management in modern enterprises. it is required to monitor, review and improve the information

security of the organisation. It is a continuous process that deals with security policies and procedures development and implementation in order to define who will do what, when and how, in order to prevent the threats. The gap analysis is the first step toward identify the existence of security weakness in the organisations systems. This should be a continuous process.to ensure long term protection against security breaches. The security that can be achieved through technical means is not enough for protection and should be supported by appropriate policies and procedures.

VI. FUTURE SCOPE

The information system security audits using the Hierarchical Multilevel gap analysis model based on ISO 27001standard, because the ISO 27001 security domains do not provide insight into which group in the organization is responsible for an activity[14] and Information security culture assessment, because the effectiveness of information security controls also depends upon the efficiency of people who implement them and who are in charge of their use.

REFERENCES

[1] A. Martins, J. Eloff , "*Information security culture*", IFIP TC11 17th International Conference on Information Security (SEC2002): Security in the Information Society: Visions and Perspectives, Cairo, Egypt,2002.

[2] A. Itrada, S. Sultan, M. Al-Junaidi, R. Qaffaf, F. Mashal, and F. Daas, "*Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a case study"*, Jordan Journal of Mechanical and Industrial Engineering , Vol. 8,no. 2, pp.102 – 118, April. 2014.

[3] K.Samota, J.patel, *"Resent IT trends: A Review paper"*,International journal of scientific research in multidisciplinary Studies", Vol. 3, Issues 5 , pp. 1 – 7, May. 2017

[4] M. Lauren and L. Tim, *"A Model for Improving e-Security in Australian Universities"* , Journal of Theoretical and Applied Electronic Commerce Research, ISSN 0718–1876 Electronic Version, Vol. 1, Issues 2 , pp. 90 – 96, August. 2006.,

[5] K. Knapp, F. Morris,M. Thoms, and B. Anthony , *"Information security policy: An organizational-level process model"* Computer &. Security, vol.28,no,7, pp.493-508, 2009

[6] M. Dey,"*Information security management - a practical approach*" ,in Proceeding AFRICAN 2007 Conference, 2007.

[7] S. E. Chang, and C. S. Lin , "*Exploring organizational culture for information security management*" , Industrial Management & Data Systems, vol.107,issue 3, pp. 438 – 458, 2007.

[8] G. Dhillon, *"Violation of safeguards by trusted personnel and understanding related Information Security concerns"* , Computers & Security, Vol. 20, Issue 2,pp. 165-172, April 2001.

[9] N. Gaunt, *"Practical approaches to creating a security culture"*, International Journal of Medical Informatics, vol.60,Issue 2, Nov.2000

[10] H.S. Venter, and J.H.P Eloff , *"Network Security: Important Issues"* , Network Security, Vol. 2000, Issue 6, Jun. 2000.

[11] M. Andress, *"Manage people to protect data"* , InfoWorld, Vol. 22, Issue 46, Nov. 2000.

[12] S. Von,B, "*Information Security - The Third Wave?* ",Computers and Security, Vol. 19, Issue 7,pp. 615-620, Nov. 2000.

[13] C. Candiwan, *" Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia"*, In Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014), pp. 50-58,Nov.2014, Kuala Lumpur, Malaysia.

[14] Al-Mayahi and S. P. Mansoor, *"ISO 27001 gap analysis – case study"* , presented at 2012 International Conference on Security and Management (SAM '12), Las Vegas, 2012.

[15] F. H. Ermana, and M. I. Tanuwijaya,*"Security audit information system based on the ISO 27001 Standards"*,PT. BPR Jatim (STIKOM), Surabaya. 2012.

[16] B. Karabacak, and I.Sogukainar, *"A quantitative method for iso 17799 gap analysis"* , Computers and Security journal, Elsevier, vol. 25(6), pp. 413–419, 2006.

[17] P. Ifinedo,"*Understanding information systems security policy compliance: anintegration of the theory of planned behaviour and the protection motivation theory"*, Computers & Security, Vol. 31, No. 2011, pp. 83-95.,2014.

[18] R. Gabriel, S. Sowa, and J. Wiedemann, *"Improving information security compliance – A process-oriented approach for managing organizational change,"* in Multikonferenz Wirtschaftsinformatik 2008 (MKWI 2008), Berlin, 2008

[19] K. Julisch, "*Security compliance: The next frontier in security research,"*, In NSPW '08: Proceedings of the New Security Paradigms Workshop 2008, pp 71-74,ACM, 2008.

[20] British Standards Institute, Information security management, part 2: "Specification for Information Security Management Systems. Technical Report BS 7799-2", 1999.

[21] ISO/IEC 17799:2000, Information technology – Security techniques – Code of practice for information security management, Geneva, Switzerland: International Organization for Standardization, 2000.

[22] N. Mayer, *"A Cluster Approach to Security Improvement according to ISO/IEC 27001"*, presented at the Software Process Improvement, 17th European Conference, EuroSPI 2010.

[23] S. T. Arnason and K. D. Willett, *"How to Achieve 27001 Certification: An Example of Applied Compliance Management*, ",in Aurbach publication, Taylor & Francis Group LLC, 2008 .

[24] Nurbojatmiko, A. Susanto, E. Shobariah,*"Assessment of ISMS based on standard ISO/IEC 27001:2013at DISKOMINFO Depok City"*, In 4th International Conference on Cyber and IT Service Management, April, 2016.

[25] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements. International organization for standardization

[26] B. Stevanović, *" Maturity Models in Information Security"*, International Journal of Information and Communication Technology Research,vol.1,no.2,2011

[27] Project Management Institute (PMI), *"Organizational project management maturity model knowledge foundation(OPM3)"*, Newtown Square, Pennsylvania USA,.2003

[28] T. Mettler, and P. Rohner. *"Situational Maturity Models as Instrumental Artifacts for Organizational Design "*, In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, Bew York, 2009.

[29] M. F. Saleh, *"Information Security Maturity Model*", International Journal of Computer Science and Security (IJCSS), Vol.5, Issue 3, pp: 316-337, 2011.

[30] K. Judev and J. Thomas, *"Project management maturity models: The milver bullets of competitive advantage?*", Project Management Journal, vol. 33, 2002.

[31] G. Klimko, *"Knowledge management and maturity models: Building common understanding"* ,Proc. of the 2nd European Conference on Knowledge Management, 2001.

[32]]S. Woodhouse*, "An isms (Im) - maturity capability model*," in IEEE 8th International Conference on Computer and Information Technology Workshops, July, 2008.

[33] C.S.Leem, S. Kim, and H.J.Lee, *"Assessment methodology on maturity level of isms,"* Knowledge-Based Intelligent Information and Engineering Systems, Pt 3, Proceedings, vol. 3683:Springer-Verlag Berlin, pp. 609 – 615, 2005..

[34] T K Gusti Ayu, I Made Sukarsa and I Putu Agung B, *" Governance Audit of Application Procurement Using COBiT Framework"*, Journal of Theoretical and Applied Information Technology (JATIT)‖. Vol 59. No.2. pp 342 – 351,.2014,

Author Profile

Dr. A. A. Nasser pursed Bachelor of Science from South- west State University, Russia in 2007 and Master of Science from South- west State University, Russia in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of information system, Sa'adah University and Head of computer and information technology department, college of graduate studies, Dar Al-Salam international university for scince and technology, Yemen. He has published more than 25 research papers in reputed international journals and conferences. and it's most of thim available online in elibrary.ru . His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy,Iinformation System Application in Health and Education. He has 5 years of teaching experience and 2 years of Research Experience.

