International Journal of Scientific Research in Multidisciplinary Studies
Vol.3, Issue.11, pp.14-23, December (2017)

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

Hierarchical Multilevel Information security gap analysis models based on ISO 27001: 2013

A. A. Nasser Al-Shameri[1]

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 research was conducted to introduce the hierarchical multilevel models, based on categorization of security controls in ISO 27001:2013 standard. And 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 for all MTO, Responsibility categories in all security aspects. The value of the gap between the value of the maturity level of the current and expected level of maturity value is a 2.88 for MTO domains and 2.84 for responsibility groups. 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; MTO , Multilevel model, Compliance; ISO 27001; Maturity level;

I. INTRODUCTION

A management system is a set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives. The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations. An Information Security Management System (ISMS) as a part of this overall management system contains all methods and instruments the management should use to establish, implement, operate, monitor, review, maintain and improve information security in all tasks and activities. The ISMS implemented in different organizations with different motivations, The establishment and implementation of the ISMS in an organization Influenced by the organization's needs and objectives, security requirements, the processes employed and the size and structure of the organization.

A common challenge for many organisations has been to operationalize the ISMS requirements, and decide in which processes they should embed measurement controls in order to ensure that deviations in relation to the ISMS processes are detected and addressed as part of the on-going improvement.

Choosing what to measure, setting targets and deciding how to operationalize those also poses a challenge for many organisations. During the last couple of years, interest in becoming ISO 27001 certified or the use of the ISO 27001 as a best practice framework has rapidly grown. Today, a lot of companies, government institutions and municipalities require either ISO 27001 certification or must adhere to the best practices in the standard. It's also increasingly incorporated into tender requirements or used during procurements. ISO 27001 requires a certain level of IT governance to be in place, such as involvement from management, understanding and use of IT as a helper/enabler to achieve the business goals in an effective way. Doing that means knowing the current and emerging risks and their impact, and avoiding the worst IT-related risks. This requires a deep understanding of the organisation, business processes, IT processes, external requirements and strategic goals[1]. That equates to a higher degree of required maturity of the organisation. 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).

Alison Anderson and Dennis Langley developed a security management system [2] based on the security studies of different organizations, and proposed three groups for monitoring the internal security policy implementation: Information system, Information system assets, and Information system environment. According to [3] , the ISO27001 security domains do not provide insight into which group in the organization is responsible for an activity. And management, technical and operational model (MTO) was introduced by them, This approach is based on ISO 17799:2005 for evaluating and continuously improving ISMS. In this model , the ISO 27001:2005 controls was grouped into three categories management, technical and operational controls.

In 2006, STOPE Model (Strategy, Technology, Organization, People and Environment) was introduced by [4]. This approach is based on "six sigma" by using ISO 17799:2005 for evaluating and continuously improving ISMS. In 2017, Another framework assessment was introduced by [5],this framework is based on SANS Critical controls and/or ISO27032) as guidance for the scoring of the maturity levels, with a mapping to ISO 27001:2005, COBiT 4.1 and COBiT 5.0. For evaluating and continuously improving ISMS, the ISO 27001:2005 controls in this framework, was grouped into six responsibility categories: (Strategy and Policies, Organization, People, Processes, technology and facilities controls).

The benefits of this categorizations are fully described by the [6],the main of them ,an organization can identify which part of their organization needs more attention regarding relevant threats, also an organization can benefit can identify which part of their organization needs more attention regarding relevant vulnerabilities[6], provides a common language for all to view and manage information security activities[3].

The information criteria refers to the fundamental aspects of information security which are basic requirements for business information security and provide the maintenance requirements of the business, namely confidentiality, integrity and availability (CIA model) [7,8], CIA Model was introduced by [9]. This approach is based on "particular security goals" by using ISO 17799:2005 for evaluating ISMS.

ISO/IEC 27001:2013 Standard is the second edition of the standard and replaces the first edition ISO/IEC 27001:2005 Standard. Discovering , studying, and modeling the new updated controls in this standard can help organizations to examine and evaluate their current security management systems , And the proposed integrated multilevel model can considered as a framework for measuring and monitoring performance and integrating better management practices, which are more aligned to traditional organisational structure, with a various security aspects, roles and responsibilities. And organization can identify which part of their organization needs more attention according to the new updated and improved international standard requirements regarding relevant vulnerabilities.

On other hands, According to practical observations and literature review, the organizations of different industries have different information security requirements, as well as different opinions and practices for establishing information security principles . Many of organizations evaluate security level by using expert system because each and every organizational department need the absolutely flaw less performance of the security strategies, and using this technology evaluation of security strategies on the basis of various key performance attributes that have been validated. For obtaining the desired level of performance, the hierarchical structure of the evaluation criteria must be built firstly, and then the Analytic Hierarchy Process is used, where the weights of evaluation criteria are determined by pairwise comparison. so the building of hierarchical structure relationships is the first step to do this.

We conclude from the above that the subject of the research is of utmost importance. It is the first step in the information security risk assessment at the enterprise according to international standards, it provide a basic analysis hierarchy structures, that can used to identify the weights of evaluation criteria, regarding relevant needs of organization and the basic inputs for risk assessment evolution. From the above, the following problem is formulated: How to improve the process of information security assessment according to the international standard (ISO/IEC:27002:2013) by using hierarchical multilevel models?

From the main problem of the research, the following sub-problem is formulated:

- What are the models, that can be used for design the hierarchical multilevel security gap analysis models based on controls defined in the updated ISO 27001:2013 standard ?
- How to establish of a hierarchical structure to be aligned to traditional organizational structure and responsibilities for the evolution of information security gap analysis assessment ?
- 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 for graduate studies seeks to achieve for all multi-level dimensions of purposed model?
- What control multilevel categories in each are the most vulnerable points bringing about potential

threats, and what solutions can be recommended to improve them?

This research aims to improve the information security practices at the Yemeni Academy for Graduate Studies by classification of security controls using a multilevel hierarchical models and assessing the extent of their compliance in the all hierarchy dimensions, structures and responsibility classes 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 by using this models with the requirements of ISO / IEC: 27001. Moreover, the study aims to discover the organizational and responsibility 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.

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 models, Section III describes methodology of research, Section IV contains results and discussion Section V contains conclusions and future scope. The last section contains the references.

II. LITERATURE REVIEW:

According to [3], The ISO27001:2005 eleven security domains do not provide insight into which group in the organisation is responsible for an activity. They proposed a model based on the organisations structure was developed. The security domains are grouped into three categories based on responsibility:

- Management Controls, which include the following domains: security policy, organisation of information security and compliance.
- Technical Controls, which include the following domains:asset management, physical and environmental security and communications & operations management.
- Operational Controls, which include the following domains: systems acquisition, development & maintenance, access control, IS incident management and business continuity management.

The main benefits, as it was presented by them are that , the model provides greater focus and better understanding on where within the organisation the responsibility lies for each domain. and provides a common language for all to view and manage information security activities.

Another framework assessment was introduced by [5],this framework classification of controls to six responsibility groups, author classified the ISO 27001: 2005 Annex controls by this classification model to :

- (SP) Strategy and Policies Controls: provide management direction and support for information security in accordance with business requirements, risks and relevant laws and regulations.
- (O)Organization Controls: Manage information security within the organization through an embedded and structure and set of roles and responsibilities.
- (PE)People Controls: Ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
- (PR) process Controls: Ensure that system and infrastructure development, maintenance and access is performed in a secured way and comply to the information policies, standards and procedures, and laws and regulations. Information security weaknesses and business interruptions should be counteract adequately avoiding unintended negative business exposure.
- (T) Technology Controls: Ensure the protection of information in networks, the protection of the supporting infrastructure and the secure exchange of information within the organization and with any external entity.
- (F)Facilities Controls: Prevent loss, damage, theft or compromise of organization’s premises and information and interruption to the organization’s activities.

The information criteria refers to the fundamental aspects of information security[7] [8]:

- Confidentiality (C): All information must be protected according to the degree of privacy of their content, aimed at limiting its access and used only by the people for whom they are intended;
- Integrity (I): All information must be kept in the same condition in which it was released by its owners, in order to protect it from tampering, whether intentional or accidental; and

- Availability (A): All the information generated or acquired by an individual or institution should be available to their users at the time they need them for any purpose.

In 2016, web based analytic hierarchy process (ahp) assessment model for information security policy of commercial banks was introduced by [9]. This approach is based on Tudor Framework "organizational information security architecture framework (Compliance, Organization / Infrastructure, Security Baselines/ Risk Assessments, User Awareness and Training and Polices, Standard, and Procedures),TUDOR (2006)" this framework classification of controls to five groups, author classified the ISO 27001: 2005 Annex controls by this classification model to :

- Compliance Controls (C): Compliance
- Organization / Infrastructure Controls (O): Organization of information security)
- Security Baselines/ Risk Assessments Controls(SR): (Physical and environment security/ Operations management/ communications management/ Information systems acquisition & development &maintenance/ Information security incident management/ Information security aspects of BCM),
- User Awareness and Training Controls (AT): (Human resource security/ Supplier relationships),
- Polices, Standard, and Procedures Controls (PSP): (Information security policy/ Access Control/ Asset management/ Cryptography).

Each security control in security domains, clauses and responsibility or role class, should address directly or indirectly one or more of three basic information security aspects. Furthermore, each category might have specific security requirements imposed by its particular security goals, for an activity.

In the work [10], the information security gap analysis based on ISO 27001: 2013 requirements was conducted as a case study at the Yemeni academy for graduate studies, This research aimed 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, attempted 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 aimed 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. The data that was obtained in this work, as a results of maturity level of information security in academy, we will used to find out the relevant gap and compliance level by using the proposed in this work integrated hierarchical multilevel model.

III. RESEARCH METHODOLOGY

The study has used the analytical descriptive method to classify the information security controls in ISO 27001:2013 standard, for building a multilevel hierarchical models for information security assessment, and to analyses the existing system, 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 ;
- Building of the integrated hierarchical multilevel models for information security gap analysis
- Design of the searching tool used for data collection;
- Data analysis; and
- Finding and recommendation's

A) ISO 27001 standard

The main part of both ISO 27001 and ISO 27002 is Annex A, which plays an important role in the ISMS implementation procedure. ISO/IEC 27001: 2005, domain requirements and security controls. Security controls have 11 security control clauses, 39 Control Objectives and Controls have 133, can be seen in Table 1.a [11].while the ISO/IEC 27001: 2013, domain requirements and security controls. Security controls have 14 security control clauses, 35 Control Objectives and Controls have 114, can be seen in Table 1.b [12].

Table I.a Security Objective (O) And Control(C) Numbers For Each Clause Iso/Iec 27001: 2005

Clauses	O	C
A5 Security Policy	1	2
A6 Organization of Information Security	2	11
A7 Asset Management	2	15
A8 Human Resources Security	3	9
A9 Physical and Environmental Security	2	13
A10 Communications & Operation Management	10	32
A11 Access Control	7	25

A12 IS Acquisition, Development & Management	6	16
A13 Information Security Incident Management	2	5
A14 Business Continuity Management	1	5
A15 Compliance	3	10

Table I.b 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

- ISO 27001: 2013 MTO , CIA, Responsibility Models

The security domains was categorized based on (MTO model) to : management, technical and operational controls,:

Management clauses: Information security policies; Organization of information security; Supplier relationships and Compliance.

Technical controls: Asset management; Physical and environmental security; Operations security and Communications security.

Operational controls: Human resource security; Access control; Cryptography; System acquisition, development and maintenance; Information security incident management and Information security aspects of business continuity management.

Each security control in security domains, should address directly or indirectly one or more of three basic information security aspects. Furthermore, each category might have specific security requirements imposed by its particular security goals, for an activity. MTO-CIA classification of controls by clauses can be seen in Fig 1. For better management practice, in the second model, controls was grouped into sex others categories, which describe the organizations structure and responsibility more detailed: (SP) Strategy and Policies Controls; (O)Organization Controls; (PE)People Controls; (PR) process Controls;(T) Technology Controls and (F)Facilities Controls . MTO-Responsibility classification of controls by clauses can be seen in Fig 2

In the small organizations, several roles carried out by the same person, and management does not identify the role with overall responsibility for managing information security. In our research a new based role model was developed, with attention to the staff roles and responsibilities definitions, and with the considerations that overall responsibility for the tasks remains at the management level , one person is appointed to the promotion and coordination processes and each employ is responsible for his original task and for maintaining information security in the workplace and in the organization. In this model, controls was categorized into seven role (function) based classes, The model is the role based classification of controls, in this case each organization has its role and responsibility matrix, roles such as chief information officer (CISO), information security officer, information security architect, information security coordinator and data proprietor (administrative official), data custodian (technician staff) and each of them has responsibility in one function or more in security management system. . In this model, controls was categorized into seven role (function) based classes: (1)Top management, (2)Administration, (3)Human resources,(4) Training, (5)Software, (6) CISO and (7) Information Technology. The MTO-role based classification of controls by clauses can be seen in Fig 3. While the Fig 4 illustrates the integrated MTO, ROLE Based and Tudor (organizational information security architecture) frame works.

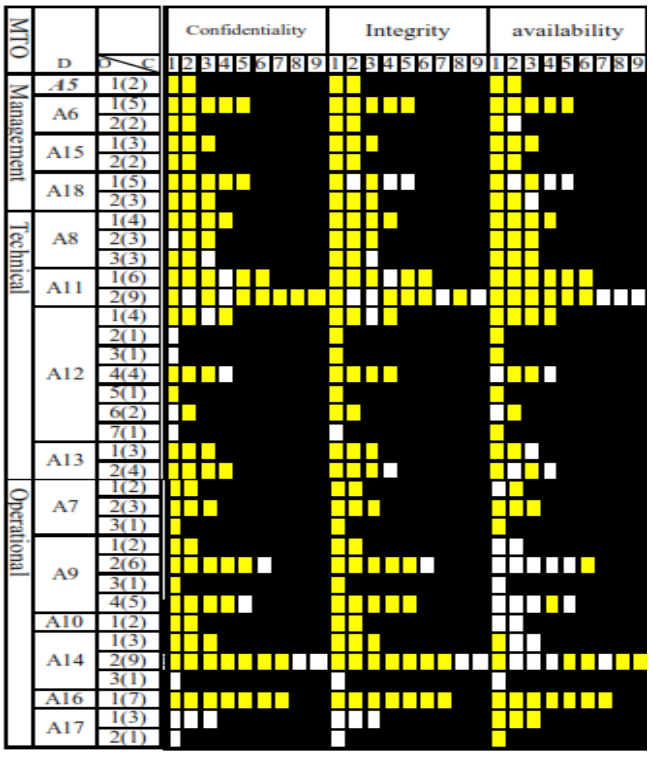

Fig 1 MTO - CIA classification of controls by clauses

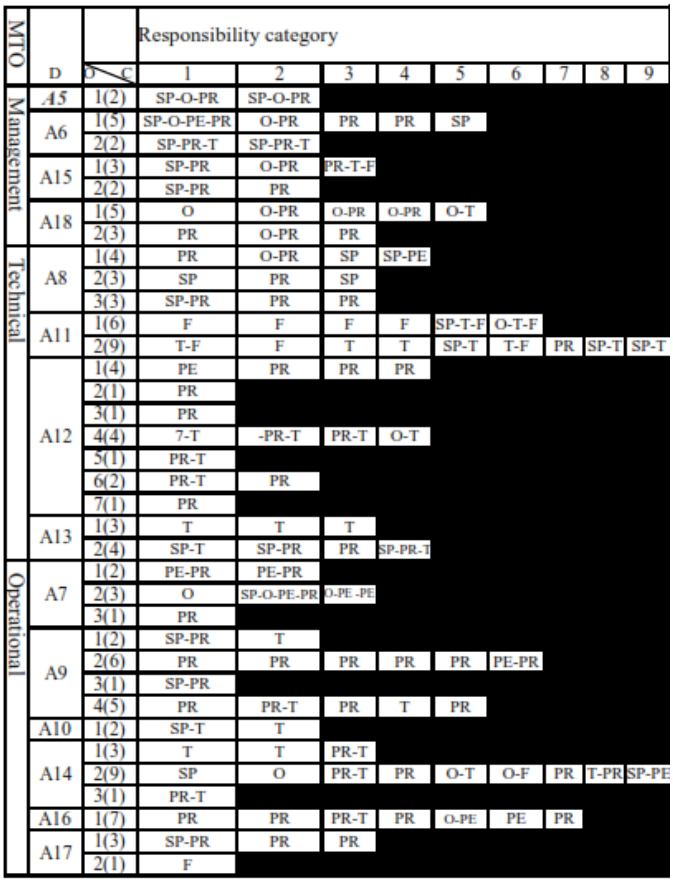

Figure 2- MTO, Clauses and Responsibility classification of controls

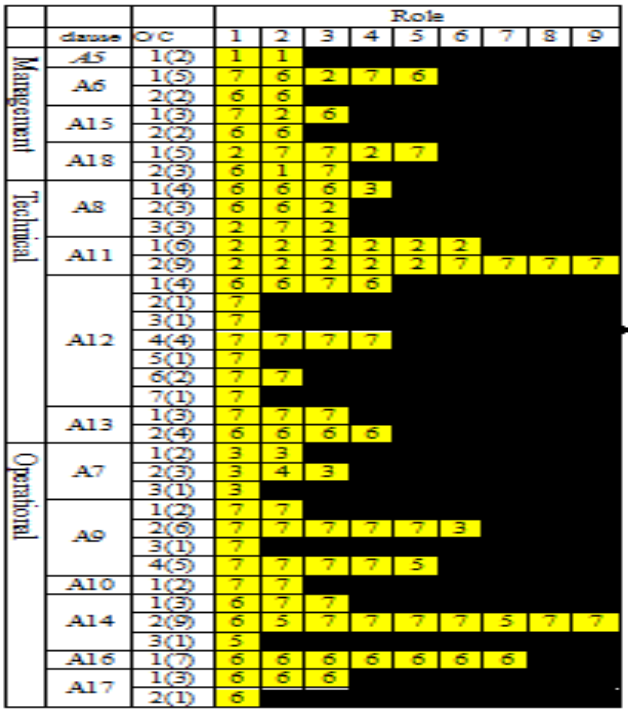

Fig 3 MTO, Role based classification of controls by clauses

The Fig1,2,3 and 4, illustrate the following relationships For clauses A.7 as an example, A.7security clause addressed to operational control domains , and covers 3 objectives, first objective has 2 controls, each of them addressed to people and process control classes, while the third objective has only one control which addressed to process responsibility, A7.1.1 control addressed to only two of the control aspect (C,A), while the other all controls addressed all of three basic information security aspects. And by the role, the controls in A7 controls grouped in two groups , (3)Human resources for and (4) Training as shown in table 3.

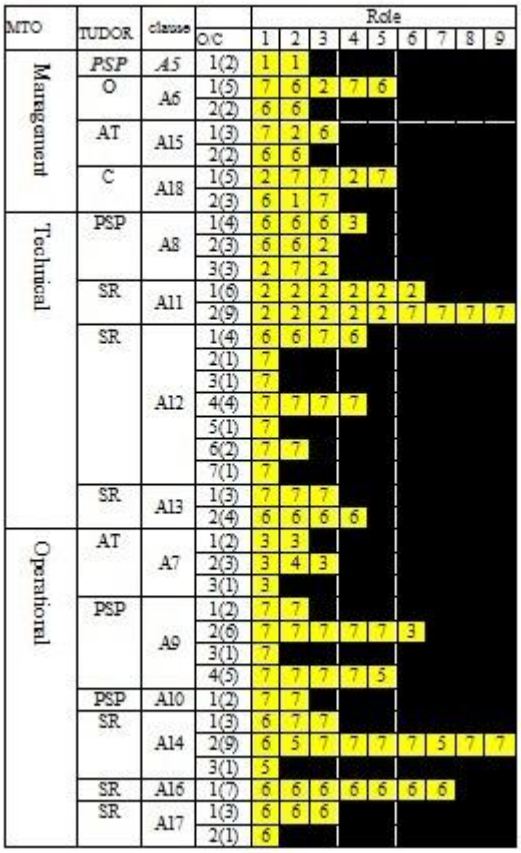

Fig 4 MTO, Role based (R), Tudor (TU) classification of controls by clauses

TABLE 3 CLASSIFICATION MATRIX OF CONTROLS

MTO	TU	A.7	R	Responsibility Category						CIA class		
				SP	*O*	*PE*	*PR*	*T*	*F*	*C*	*I*	*A*
O	AT	A.7.1.1	3			√	√			√	√	
		A.7.1.2	3			√	√			√	√	√
		A.7.2.1	3		√					√	√	√

		A.7.2.2	4	√	√	√	√			√	√	√
		A.7.2.3	3		√	√	√			√	√	√
		A.7.3.1	3				√			√	√	√

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 5.a and 5.b [13,14]. This model has its measurement basis supported by the maturity scale of COBiT. [13]. 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 4, in Tables 5.a and Tables 5.b shown the description of maturity values and the Maturity level Assessment Criteria.

Table 4.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 5.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 5.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

The respondent's calculation summary by using descriptive methodology obtained a result as shown in Tables 6,7.

Table 6 Summary of The Value Maturity Level of all C,I and A control classes per MTO domain

N	Control category	CC		IC		AC	
		I	L	I	I	L	I
1	Management Controls	1.30	1	1.40	1	1.46	1
2	Operational Controls	2.63	3	2.97	3	3.11	3
3	Technical Controls	2.45	2	2.50	2	2.46	2

Table 7 Summary of The Value Maturity Level of C,I and A control categories per responsibility class

N	Control category	CC		IC		AC	
		I	L	I	L	I	L
1	Strategy and Policies	1.63	2	1.61	2	1.47	1
2	Organization	1.60	2	1.51	2	1.63	2
3	People	1.89	2	1.89	2	2.10	2
4	Process	1.98	2	2.07	2	2.00	2
5	Technology	2.52	3	2.50	2	2.75	3
6	Facilities	3.44	3	3.44	3	3.33	3

Based on the result from Tables 6 and 7 for each process obtained graphs as in the Figures below.

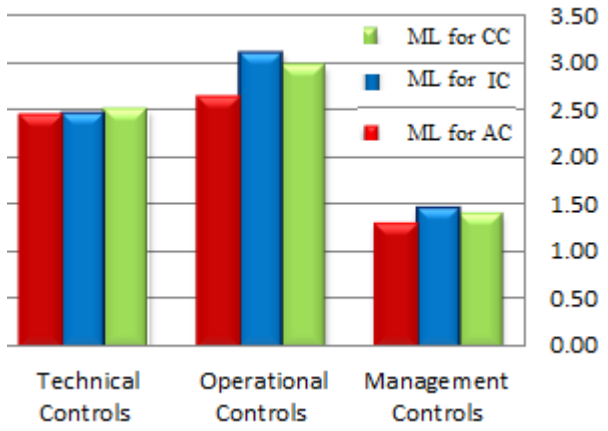

Fig.4 illustrates the average value of maturity level for all C,I, and A controls per MTO domain

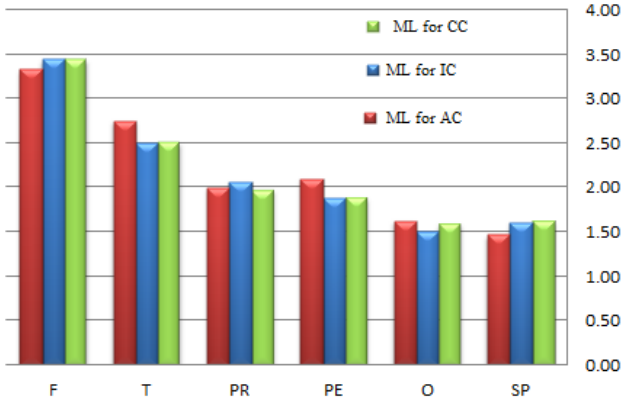

Fig 5 Measurements graphs in maturity level for all C,I, and A controls per responsibility class

After knowing the maturity level of information security for all control domains and categories, and determining the expected maturity level, which equal 5 (Optimized) , as a compliance goal level in Academy. Then the value gap for each clause are gotten then averaged to obtain the value of the overall gap. Table 6 illustrates the average value gap of maturity level for all C,I, and A controls per MTO domain, while the Table 9 illustrates the average value gap of maturity level for all C,I, and A controls per responsibility class.

Table 8 Summary of The Maturity Level gap of all C,I, and A controls per MTO domain

D	Maturity Level						
	Exp.	Confidentiality		Integrity		Availability	
		Cur.	Gap	Cur.	Gap	Cur.	Gap
M	5	1.30	3.70	1.40	3.60	1.46	3.54
O	5	2.63	2.37	2.97	2.03	3.11	1.89
T	5	2.45	2.55	2.51	2.49	2.46	2.56

Table 9 Summary of The Maturity Level gap of all C,I and A controls per responsibility class

Cl.	Maturity Level						
	Exp.	Confidentiality		Integrity		Availability	
		Cur.	Gap	Cur.	Gap	Cur.	Gap
SP	5	1.63	3.37	1.61	3.39	1.47	3.53
O	5	1.60	3.40	1.51	3.49	1.63	3.37
PE	5	1.89	3.11	1.89	3.11	2.10	2.90
PR	5	1.98	3.12	2.07	2.93	2.00	3.00
T	5	2.52	2.48	2.50	2.50	2.75	2.25
F	5	3.44	1.56	3.44	1.56	3.33	1.67

The results of overall maturity level average value of all controls classes per all control categories and, can be seen in Table 10,a. The overall distance average gap to all control list as shown in table 10 is a 2.88 for MTO domains and 2.84 for responsibility groups, the gap to C classes is 3.87 and 2.82 , to I class is 3.71 and 2.83. while to A class is 2.66 and 2.79.

Table 10- Summary of The Value Maturity Level Average of all control categories

Average value: Index, Maturity Level						
Group	CC		IC		AC	
	I	L	I	L	I	L
MTO groups	2.13	2	2.29	2	2.34	2
Responsibility Classes	2.18	2	2.17	2	2.21	2

From all of this values we can conclude that the security information are on the second level, ie repeatable but intuitive.

In this research, and based on all previews results using all models of control classification (MTO domains and

responsibility classes) and for all control categories (C,I, and A control categories),it has found the following score result as shown in table 11.

The results of the current maturity level of the lowest contained for for 33.33 % of MTO domains (management domain) and responsibility classes(SP,O) with a value of below 1.65 so that the value gap (the gap) between the value of the current maturity level with the maturity level in this clause over 3.35 (the value of the gap is highest). While the value of the current maturity level that is highest for 16.66% of responsibility classes (F) of controls, with a maturity level value above 3.26 for all control categories, so that the value of the gap in this clause below 1.74 (the lowest value of the gap). But The value of the current maturity level that is between 1.66 and 3.25 for 66.66% of MTO domains and for 50% of responsibility classes. Thus the higher the value gap clause, the more likely the clause is to get a security breach and the lower value of the gap in clause then the less likely the clause is to get security problems. From these findings, the Academy may act in areas related to their points of difference between expectation and perception of information security level

Table 11 The Maturity Level result score of all control categories

Group	ML between 0 and 1.65		ML Between 1,66 and 3.25, %		ML above 3.26 ;%	
	Sub group	%	Sub group	%	Sub group	%
MTO domains	M	33,33	O and T	66,66		
Responsibility classes	SP,O	33.33	PR,PE and T	50	F	16,66

V. CONCLUSIONS AND FUTURE WORKS

This research aimed to improve the information security practices at the Yemeni Academy for Graduate Studies by classification of security controls using a multilevel hierarchical models and assessing the information security level in each dimensions of this models, assessing the extent of their compliance in them. 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 by using proposed models with the requirements of ISO / IEC: 27001. The multilevel - hierarchical models for classification was designed, and its application to improve the information security management practice was conducted by analyzing the information security gap analysis in Academy. For future research, the use of this multilevel hierarchical model in a decision making methods and expert system applications associated with Ahp and fuzzy ahp and the proposal of indicators to assess the information security risk is suggested

REFERENCES

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

[1] Anderson, A., Longley, D., and Kwok, L.F., "Security modeling for organizations", CCS '94 Proceedings of the 2nd ACM Conference on Computer and communications security, , p. 241- 250, New York, 1994.

[2] 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.

[3] Saleh, M. S., Alrabiah, A., and Bakry, S. H., "Using ISO 17799:2005 information security management: a STOPE view with six sigma approach" , International journal of network management, v. 17, 2007, pp.85- 97.

[4] DNB Framework Information Security, point to consider: Available from http://www.toezicht.dnb.nl/en/binaries/51-230769.XLSX

[5] Bahareh S., Hannes F. and Iman S., Evaluating the effectiveness of ISO 27001:2013 based on Annex A, 9th International Đorkshop on Frontiers in Úvailability, Reliability and Đecurity (FARES 2014), Đniversity of Fribourg, Đwizerland, Sep 11, 2014

[6] Rosmiati, Imam Riadi, Yudi Prayudi , "A Maturity Level Framework for Measurement of Information Security Performance" , International Journal of Computer Applications (0975 – 8887),Volume 141 – No.8, May 2016

[7] S. Faris, H. Medromi, S. El Hasnaouni, H. Iguer and A.Sayouti, "Towards an Effective Information Security Risk Management of Universities Information Systems Using Multi Agent System", Itil, Iso 27002, Iso 27005ǁ, (IJACSA) Intermasional Journal of Advanced Computer Science and Application, Vol. 5 No. 6 2014, pp 114 –118.

[8] S. M. Wu, D. Guo, W. T. Lin and M. H. Li "web based analytic hierarchy process (ahp) assessment model for information security policy of commercial banks", IJABER, Vol. 14, No. 2 (2016): 951-960

[9] A. A. Nasser, Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Postgraduate Studies, Sana'a, Yemen, ",International journal of scientific research in multidisciplinary Studies", Vol. 3, Issues 12 , pp. 1 – 9, DEC. 2017

[10] Information security management systems requirements, International Standards ISO/IEC 27001 Std., 2005.

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

[12] M. Dey,“*Information security management - a practical approach*” ,in Proceeding AFRICAN 2007 Conference, 2007.

[13] 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)ǁ. 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.

