Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Towards A New Maturity Model for Information Security Management

Oussama MATRANE
Laboratory of Electronics & Information Processing
The Faculty of Sciences Ben Sik,
Av Avenue Driss El Harti B.P 7955,
Sidi Othmane, Casablanca, Morocco

Mohammed TALEA
Laboratory of Electronics & Information Processing
The Faculty of Sciences Ben Sik,
Av Avenue Driss El Harti B.P 7955,
Sidi Othmane, Casablanca, Morocco

Chafik OKAR
EST Berrchid, University Hassan I,
Morocco

Abstract*— *Maturity Models are significant tools to ensure continuous improvement of systems and activities. They follow self-assessment and provide a means of benchmark of these activities linked to best practices. Many Maturity Models have been developed for management Information system and specifically, information security management. In the recent years, management of information security becomes very important for the activities of organizations and helps to increase performance. In this context, this article suggests a new maturity model for information security management in order to identify and explore the strength and weaknesses of particular organization's security. It is intended as a tool to evaluate the ability of organizations to meet the objectives of security.

Key-Words: Maturity Models, Information Security, Management, Performance, Organizations.

I. INTRODUCTION

The frequent changes in the organization nowadays, need an alignment of business processes on business strategies, which, at the same time, require a set of methods, tools, management practices and the adaptation of information and communication technologies [1]. Besides, the development of information and communication technology and the spread of the Internet are not only remarkably changing individual lifestyles and business conduct but also explosively creating new businesses [2]. However, adverse changes and effects such as hacking, viruses and personal information leaking are also rapidly increasing [3]. Moreover, Business environment continues to change with an increasing dependence on information technology and pervasive use of the Internet [4].

In this context, Information is a very important asset for any modern organization. Protecting its security and critical data are very important and becoming a top priority for many organizations [5]. Besides, most of the organizations are very much concerned about the ownership of their data [6]. Therefore, information security concerns are at the heart of information systems, both at technological and organizational levels [7], and has become a major concern for computer professionals [8].

Information security is identified as the protection of integrity, confidentiality and availability with the respect to information assets of any organization [9] [10]. It involves identifying unique threats and challenges which need to be addressed by implementing the appropriate countermeasures [11]. Information security can be also considered, as requirements that are including the types and levels of protection necessary for equipment, data, information, application, and facilities to meet security policy [12].In general, information security is not only a technical issue but also a behavioural issue involving users [13].

In spite of growing interest for information security, the adoption of the international standard on information security management (ISO/IEC 27001) is still very low. This standard provides requirements to manage an Information Security Management System [14] which is based on the Deming cycle PDCA and broadly use the risk analysis [15].
On the other hand, since information security has a very important role in supporting the activities of the organization, we need a standard or benchmark which regulates governance over information security. Therefore, several standards Governance has been created, which leads to information security such as PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT. However, some of these standards are not well adopted by the organizations, with a variety of reasons.
In this paper, we will describe a new maturity model for Information Security Management based on the concept of maturity model, the critical success factors of RSA framework and Process management of ITIL. The objective of this paper is to provide a maturity model in Information Security Management for helping organizations to assess its maturity and to give a road map of improving its information security management.

II. MATURITY MODELS

According to the Jugdev and Thomas [16] maturity models identify project or organizational strengths, weaknesses and benchmarking information. A maturity model is a structured collection of elements that describe the characteristics of effective processes or products [17].

In general, maturity models have the following properties [18] [19]:

- 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);

Maturity models are used to describe, explain and evaluate growth life cycles. The basic concept of all models is based on the fact that things change over time and that most of these changes can be predicted and regulated [20]. The concept of maturity models is increasingly being applied within the field of Information Systems as an approach for organizational development or as means of organizational assessment [21] [22]. In order to identify and explore the strength and weaknesses of particular organization's security, a wide range model Maturity has been developed [23]. It is intended as a tool to evaluate the ability of organizations to meet the objectives of security [24]. There is for example: information security maturity model (ISMM) [24], Elements of the Barrick Security Management System: BARRICK SECURITY METHODOLOGY [25], The ESG information security management maturity model [26].

III. CRITICAL SUCCESS FACTORS (CSFS) OF SECURITY MANAGEMENT

Critical success factor (CSF) refers to an element that is necessary for an organization or project to achieve its mission. It is a critical factor or activity required for ensuring the success of a company or an organization [27]. The concept of "success factors" was developed by Daniel in 1961 of McKinsey & Company and was refined by Rockart in 1981. According to Boynlon and al. 1984, "Critical success factors are those few things that must go well to ensure success for a manager or an organization, and, therefore, they represent those managerial or enterprise area, that must be given special and continual attention to bring about high performance. CSFs include issues vital to an organization's current operating activities and to its future success." [28].

An exploratory empirical study has pinpointed the critical success factors that play a vital role in ensuring that an information security policy leads to enhanced information security in an organization [29].

For the present study, on the basis of the analysis of the different definitions of ISM present in literature, the Critical Success Factors (CSFs) for maturity model ISM proposed by RSA Framework for security management [30], have been chosen.

IV. INFORMATION SYSTEM MANAGEMENT SECURITY

The ISMS consists of processes, procedures, and resources that can be software. It does not provide a method for assembling the necessary information or a pattern on how to structure that information [31]. ISMS includes a series processes for systematically establishing, documenting and continuous managing procedures to improve the safety and reliability of the assets of an enterprise, and for realizing information confidentiality, integrity and availability which are the goals of information security, and includes the continuous enhancement of information security [32].

In this section we give an overview of ISMS standards; ISO27001, the ESG and ITIL. The overview includes profile and methodology used in each standard in implementing ISMS for organizations. These overviews will help readers easily understand functions, behaviors and position of each on the big figure and whole ISMS's strategies [33].

→ ISO27001:

ISO, founded on February 23, 1947, promulgates worldwide proprietary industrial and commercial standards, has headquarters in Geneva, Switzerland [34]. It has 163 national members out of the 203 total countries in the world. The international standard of ISO 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within an organization [35]. The ISO27001 standard provides a model for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) [36] .Also, The ISMS Standard ISO/IEC 27001 provides a series of security process based on well-known Plan-Do-Check-Act (PDCA) model that is used by other ISO management standard such as ISO 9001 (Quality Management System), ISO 14001 (Environmental Management System), ISO/IEC 20000-1 (IT Service Management) and several others. [37]. This standard aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS [38].

→ITIL:

The ITIL originated as a collection of books, each covering a specific practice within IT Service Management, was built around a process-model based view of controlling and managing operations often credited to W. Edwards Deming and his plan-do-check-act (PDCA) cycle [39], as IT Services Management Standards and Best Practices [40] contains of 8 main components, they are: Service Support, Service Delivery, ICT Infrastructure Management, Security Management, Application Management, Software Asset Management, Planning to Implement Service Management, Small-Scale Implementation. Figure 1 describes IT services Management of ITIL [41].

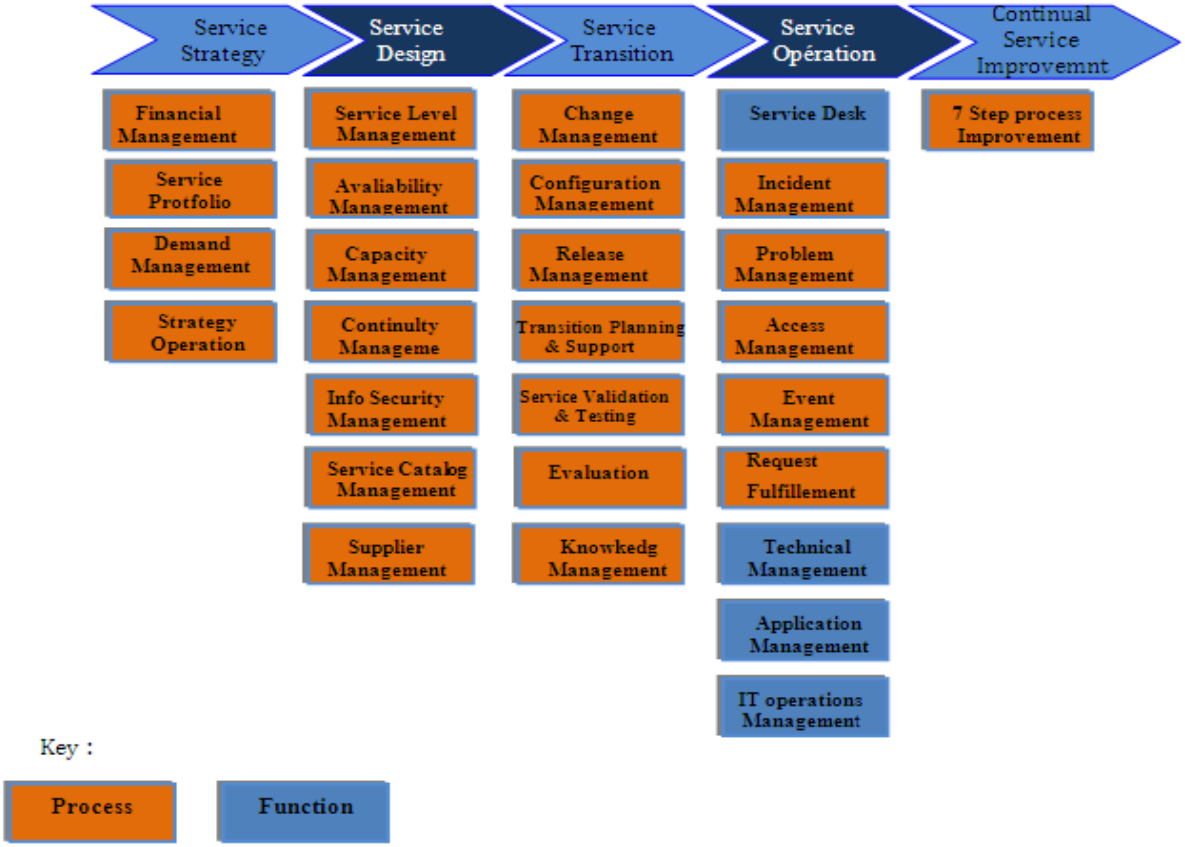

Fig. 1 TIL v3 Phases and Process Areas

→ The ESG information security management maturity model:

As companies face a more dangerous threat landscape, they are actively evolving old security defenses into a more formal information security management framework.

Based on this evolutionary trend, ESG has developed a four-phased security management maturity model described in the figure. Find about the right data, decision-making process and security operations model that can help you make intelligent security investments, quickly react to changes within IT and keep your business secure. Figure 2 describes the model ESG [42].

Fig. 2 The ESG Information Security Management Maturity Model

V. NEW MATURITY MODEL INFORMATION SECURITY MANAGEMENT IS3M

The most current standards, practices and frameworks, COBIT, ITIL and others, are prescriptive. They describe "What" needs to be done, but not "How "to do it. Providing the "How" is not the intent of COBIT and ITIL [43].The same holds true for information security management standards, which mainly focus on the existing of processes and not the content of what it is securing. Information security management standards like ISO 27001, GASPP/GAISP and SSE-CMM which are widely utilized and advocated by researchers and practitioners alike have a limitation in that they focus on ensuring that security processes exist while being unconcerned about how these security processes can be accomplished in practice [44].

On the other hand, research in the field of information systems security (ISS) is heavily dominated by conceptual and theoretical research, as has been shown by Siponen et al. [45].

Based on the literature review, there seems to be a lack of researches in the field of Information Security Management and maturity models. Hence there is a need for a model that assesses the maturity of this type of project.

The Purpose of the paper is to extend current knowledge and understand of Information Security Management practice. In particular, the paper aims to develop a preliminary version of a maturity model for Information Security Management based on the concept of CSFs of RSA framework, the process area of ITIL and the concept of maturity.

The suggested maturity model of information management security is considered as a tool, intended to assess the degree of maturity of organizations, in the ability to meet the objectives of security, namely, confidentiality, integrity, and availability, while preventing attacks and achieving the organization's mission despite attacks and accidents. We aim by this new maturity model to help effectively all type of organization, to implement simply this model in their business strategies. It can be seen as a high-level roadmap for large organizations. The proposed model is built essentially on the following three dimensions:

1.Maturity level dimensions for CSF:

- Level 1(initial): there is no process area and process is chaotic.
- Level 2 (defined): is the level where Information Security Management processes are documented, standardized, and integrated into a standard implementation process for the organization and managed based on quantitative models and tools.
- Level 3 (managed): Process and activities are controlled and managed based on quantitative models and tools.

2. Standard life cycle stages of Information Security Management.

3. The critical success factors (CSFs) of RSA Framework.

The new maturity model for information security management is composed of 5 distinct phases that encompass historical practices and future aspirations. It is called The 5 Managements (5M) of information security.

- **Level 1** → Business Management: This is to synthesize the key objectives and resources that must be protected to achieve them. This allows to integrate the security into all the processes and structures and to support external requirements (regulatory compliance, etc...) and internal (business lines, policies, etc...).
- **Level 2**: → Risks Management: This is to quantify the actual level of risk and to bring closer to the acceptable level by the company. This helps to identify, order risk and control project to reduce risk.
- **Level 3**: → Operations Management: This is to evaluate the daily running of security operations and their ability to provide an optimum ratio cost /security. This aligns processes and controls policies to reduce the rate of conversion of risk in incidents.
- **Level 4**: → Incidents Management: This is to assess the ability of the company to respond to security incidents to ensure that the level of risk tolerance is never exceeded. This allows detecting, analyzing, processing and communicating security events to minimize their effects and costs of resolution. It is vital to be able to detect and analyze very quickly for taking appropriate measures to limit its impact.
- **Level 5**: → Problems Management: A 'Problem' is the unknown cause of one or more incidents, often identified as a result of multiple similar incidents. The objective of Problem Management is to minimize the impact of problems of security on the organisation. Problem Management plays an important role in the detection and providing solutions to problems (work arounds & known errors) and prevents their reoccurrence.

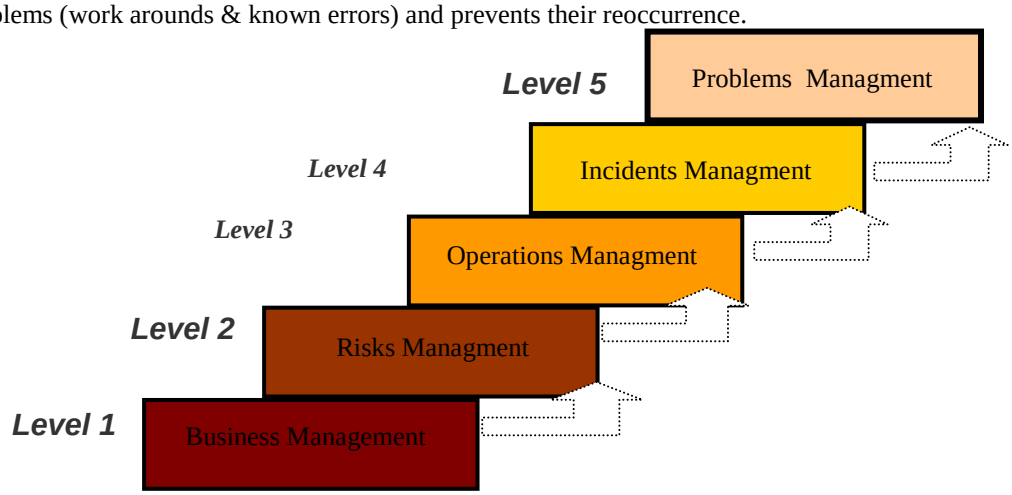

Fig3. Maturity Level of Information Security Management

This new maturity model of information security management is structured on 5 levels of maturity. To adapt our model to any complex information security system and to be suited with any type of organizations, we choose for assessing the maturity of CSF, the staged representations which consists on three levels. Hence, in each level of the model, we incorporate CSFs of RSA framework. We assess the one. If level 3 is reached in all CSFs of the level, we must keep it and we validate the level to pass to the next maturity level of information security management.

For each maturity level, the model defines key improvement factors that a firm can use to move up to the next higher maturity level. It can define an improvement roadmap using key improvement factors.

We describe the maturity model for information security management in table 1.

Table1. Maturity Model of Information Security Management

Maturity Level Of Information Security Management	**CFSs of Information Security Management**	**Maturity level 1 (initial)**	**Maturity level 2 (defined)**	**Maturity level 3 (Managed)**
Business Management	*Definition of business objectives*	Business objectives are not defined	Some business objectives are defined	Business objectives are clearly defined
	Objectives of risk level	Level security has not been quantified to define the risk	Level security has been quantified to define the risk	Level security has been well quantified to define the risk
	Definition of critical business resources	Critical business resources are not defined	Critical business resources are defined	Critical business resources are clearly defined
Risk Management	*Understanding of internal and external threats*	The manager security doesn't understand internal and external threats	The manager security understand internal and external threats	The manager security understand very well internal and external threats
	Identifying vulnerabilities	Vulnerabilities are not defined	Vulnerabilities are defined	Vulnerabilities are clearly defined
	Classification of resources with high value	There is no classification resources with high value	There is classification resources with high value	There is a good classification resources with high value
Operations Management	*Prioritization of work based on risk*	There is no prioritization of work based on risk	There is some prioritization of work based on risk	There is a clear prioritization of work based on risk
	Adding security checks required	Required checks of security is not added	Required checks of security is partially added	Required checks of security is completely added
	Improving supervision and visibility	The supervision and visibility is not improved	The supervision and visibility is partially improved	The supervision and visibility is entirely improved

Incidents Management	*Identification of security events*	The security events is not identified	The security events is partially identified	The security events is completely identified
	Prioritization by business impact	Prioritization is not determinated by business impact	Prioritizations are partially determinated by business impact	Prioritizations are completely determinated by business impact
	Report to business managers	No report is realized to business managers	Some report is realized to business managers	Business managers have all reports
Problems Management	*Avoiding Repeated Incidents*	The metrics of repeated incidents are not established	Some metrics of repeated incidents are established	The metrics of repeated incidents are clearly established
	Minimizing Impact Of Problems	The metrics of problems are not defined	The metrics of problems are partially defined	The metrics of problems are entirely defined
	Initiating actions to prevent recurrence of incidents	Actions of prevent recurrence incidents are not initiated	Some actions of prevent recurrence incidents are initiated	Most of actions prevent recurrence incidents are initiated

VI. CONTRIBUTION

The proposed maturity model of information security management can be considered as one of the widespread areas in the field of improving organizational security. It is oriented essentially for enterprises in order to be more performing in terms of information security management. It identifies organizational strengths and weaknesses by providing steps of improvement. It defines also a level maturity for any organizations that have the ambitions to improve its security strategies. Thus, it reflects good security practices recognized at each stage.

By integrating management of services ITIL, in particular, problems management and incidents management, and CSFs of RSA framework with the concept of maturity, we have developed a new maturity model in information security management that makes possible for any organizations to see where it stands and how it can improve its information security management. Thus, it provides a methodology for enterprises to develop an improvement roadmap to his information security management by reaching specified maturity level of CSF.

VII. CONCLUSIONS

The paper contributes in creating a new concept of maturity model in information security management. Five levels management maturity and tree level in each process of management has been developed to evaluate and provide a road map to improve its ability in preventing the information. The new model maturity helps organizations by proceeding through the five levels of Maturity Management, to have a better understanding of where they are and how to proceed. Thus, this new maturity model contains a set of best practices based on the critical success factors. Besides, by integrating a process of problems management of ITIL, we facilitate the detection and providing solutions to problems of information security in enterprises.

For the future work, an empirical study will be performed to aid in validating and to demonstrate the effectiveness of the proposed model of Information Security Management. Hence, a survey will be distributed to different Moroccan organizations to evaluate its maturity in information security management and the result will be published in the near future.

REFERENCES

[1] P. B. Nassar, Y. Badr, F. Biennier, K. Barbar *"Securing Collaborative Business Processes: A Methodology for Security Management in Service-Based Infrastructure*", IFIP International Federation for Information Processing, Ifip Aict 384, 2012, pp. 480–487.

[2] D. Botta, K. Muldner, K. Hawkey, K. Beznosov, "*Toward understanding distributed cognition in IT security management: the role of cues and norms*", Cognition, Technology & Work, Volume 13, Issue 2, June 2011, pp 121-134

[3] C. Park†, S. Jang, Y. Park, "*A Study of Effect of Information Security Management*

System [ISMS] Certification on Organization Performance", IJCSNS International Journal of Computer Science and Network Security, Vol.10 No.3, March 2010, pp 10-21.
[4] H. Rhee, Y. U. Ryub, Ch. Kimc, "*Unrealistic optimism on information security management*", computers & security, 31, pp: 221-232, 2012.
[5] N. K.Sharma, P. Kumar Dash, Effectiveness of Iso 27001, as an information security system: analytic study of financial aspects", Far East Journal of Psychology and Business, Dec 2012, Vol. 9 No. 3.
[6] S.A. Almulla, C. Y. Yeun, "*Cloud computing security management", Engineering Systems Management and Its Applications (ICESMA)*, April 1 2010, pp: 1-7
[7] É. Dubois, P. Heymans, N. Mayer, R. Matulevičius, "A Systematic Approach to Define the Domain of Information System Security Risk Management", Intentional Perspectives on Information Systems Engineering 2010, pp 289-306.
[8] I. Aguirre, S. Alonso, "Improving *the Automation of Security Information Management: A Collaborative Approach*", IEEE Security & Privacy, 2012, pp: 55-59.
[9] ISO/IEC 27001:2005 – *Information technology – Security techniques – Information security management systems – Requirements*. Institute of Innovative Technologies EMAG, Poland, 2012.
[10] ISO/IEC 27002:2005 – *Information technology - Security techniques - Code of practice for information security management* (formerly ISO/IEC 17799). Institute of Innovative Technologies EMAG. Poland, 2012.

[11] D. Zissis, D. Lekkas, "*Addressing cloud computing security issues*", Future Generation Computer Systems, Volume 28, Issue 3, March 2012, p: 583–592.
[12] A. Chikh, M. Abulaish, S. Irfan Nabi, K. Alghathbar, "*An Ontology Based Information Security Requirements Engineering Framework"*, Sta, Ccis 186, pp. 139–146, 2011.
[13] Y. Banga, D. Leeb, Y. Baec, J. Ahnc, "Improving *information security management: An analysis of ID–password usage and a new login vulnerability measure*", International Journal of Information Management, 2012, pp: 409-418.
[14] O. Mangin, B. Barafort, P. Heymans, E. Dubois, "*Designing a Process Reference Model for Information Security Management Systems*", Software Process Improvement and Capability Determination Communications in Computer and Information science Volume 290, 2012, pp 129-140.
[15] J. Baginski, A. Białas, "*Validation of the Software Supporting Information Security and Business Continuity Management Processes*", Complex Systems and Dependability, AISC 170, 2012, pp. 1–17.
[16] K. Judev and J. Thomas, "*Project management maturity models: The milver bullets of competitive advantage*?" Project Management Journal, vol. 33, 2002.
[17] OPM3, "*Organizational project management maturity model*", Newtown Square, Pennsylvania USA, Project Management Institute.2003.
[18] G. Klimko, "*Knowledge management and maturity models: Building common understanding*," Proc. of the 2nd European Conference on Knowledge Management. 2001.
[19] R. Weerdmeester, C. Pocaterra and M. Hefke, "*VISION Next Generation knowledge management*," Information Societies Technology (IST) Programme. 2003.
[20] Irena Hribar Rajterič, "*Overview of Business Intelligence Maturity Models*", Management, Vol. 15, 2010, 1, pp. 47-67S. Koçoglu, Z. Imamoglu, H. Ince, H. Keskin, "The *effect of supply chain integration on information sharing: Enhancing the supply chain performance*", Procedia Social and Behavioral Sciences, Vol. 24, 2011, pp. 1630-1649.
[21] Ahern, D., A. Clouse, and R. Turner, CMMI distilled: A practical introduction to integrated process improvement. 2004, Boston, London: Addison-Wesley.
[22] Mettler, T. 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*. 2009. Philadelphia, Pennsylvania: ACM.
[23] Amer, S.H. and J. John A. Hamilton, *Understanding security architecture, in Proceedings of the 2008 Spring simulation multiconference*. 2008, Society for Computer Simulation International: Ottawa, Canada. p. 335-342.
[24] M. F. Saleh, "Information Security Maturity Model", International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011, pp: 316-337.
[25] J. Sokalsky, I. Gonzales, "*Barrick's Security Management System*", Barrick's Security Commitment of Barrick Gold Corporation, 2012.
[26] EMC Corporation, "The *ESG Information Security Management Maturity Model*", Category : Risk Management, Type : White Paper, July 08 2011.
[27] Rockart, John F., "*Chief executives define their own data needs*", Harvard Business Review 1979 (2), pages 81-93.
[28] Faycal Fedouaki, Chafik Okar, Semma El Alami, "*A maturity model for Business Intelligence System project in Small and Medium-sized Enterprises: an empirical investigation IJCSI International Journal of Computer Science Issues*, Vol.10, Issue 6, No1, November 2013.
[29] M. Al-Awadi, K. Renaud, "Success *Factors In Information Security Implementation in Organisations*", Department: Computing Science, University of Glasgow, 2010.
[30] Emc Corporation, « *Rsa Security Management, An integrated approach to risk management, operations and incidents* », 2011, www.rsa.com
[31] K. Beckers, S. Faßbender, M. Heisel, J. Küster, H. chmidt, "*Supporting the Development and Documentation of ISO 27001 Information Security Management Systems through Security Requirements Engineering Approaches*", Engineering Secure Software and Systems, Volume 7159, 2012, pp 14-21.

[32] C. Park, S. Jang, Y. Park, "*A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance*", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.3, March 2010, pp: 10-21.
[33] H. Susanto, M. N. Almunawar, Y. Tuan, "Information *Security Management System Standards: A Comparative Study of the Big Five*", International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05, October 2011, pp: 23-29.
[34] ISO History and Definition www.iso.org
[35] http:// wikipedia.org/wiki/ISO
[36] A. Gillies, "*Improving the quality of information security management systems with ISO27000*" The TQM Journal, Vol. 23 Iss: 4,2011, pp.367 – 376.
[37] E. Humphreys, "*Information security management system standards*" , Datenschutz und Datensicherheit - DuD, Volume 35, Issue 1, January 2011, pp 7-11
[38] A. Alfantookh. An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls. Computer Sciences, King Saud University. 2009.
[39] Basie von Solms. 2005. Information Security Governance – Compliance Management vs Operational Management. Computer & Security Journal. Elsevier, Science Direct

[40] http://www.itil.org/en/vomkennen/itil/ueberblick/index.php
[41] Office of Government Commerce, 2007, ITIL v3 Library, TSO.
[42] J. Oltsik, Senior Principal Analyst, White Paper, "*The ESG Information Security Management Maturity Model*", July, 2011.
[43] D. Milicevic, M. Goeken, "*Social Factors in Policy Compliance – Evidence found in Literature to Assist the Development of Policies in Information Security Management.",* 46th Hawaii International Conference on System Sciences, 2013, pp : 4476-4484.
[44] J. Lindström, S. Samuelsson, D. Harnesk and A. Häger fors, "*The need for improved alignment between actability, strategic planning of IS and information security*", 13th International ITA Workshop, Krakow, Poland, 2008, pp. 14-27.
[45] M. Siponen, R. Willison, and R. Baskerville, "*Power and Practice in Information Systems Security Research*", ICIS 2008 Proceedings, 2008, Paper 26.

