ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEMS FRAMEWORKS IN ORGANIZATIONS

Tariq A.Baqi Al- sofi*1, Dr.Nagi Ali Al-Shaibany*2, Dr. Abdualmajed Ahmed Al-Khulaidi*3
Yasmeen Mohammed Almekhlafi*4

*1 IT Student, IT Management, Sana’a University, Yemen.
*2 Assistant Professor, IT Management, Sana’a University, Yemen.
*3 Associate Professor, Computer Science, Sana’a University, Yemen.
*4 Computer Science Student, FCIT, Thamar University, Yemen.

ABSTRACT

The information security management system (ISMS) is a set of standards, which the companies use to protect their information, mainly focuses on closing the gap in the security systems and processes through risk management. Information systems Management needs to meet three main objectives of information security: confidentiality, integrity and availability. This paper first conducts a comprehensive literature review to investigate the main factors that contribute to the success of Information Security Management. Additionally, The paper summarizes investigations into existing information security management frameworks and models. In addition to identifying the advantages and disadvantages for each framework and model, It was concluded that the best research, from the point of view of the researcher, is the framework that all the success factors that contribute to the implementation of ISMS system including technical, organizational and human aspects.

Keywords: information, Security, analysis, framework, Information Security Management Systems.

I. INTRODUCTION

Information is one of the sensitive assets owned by organizations, so it needs protection commensurate with its value, the information is intangible capital, and there is difficulty in assessing its value[1]. While information is valuable and important to organizations, it is vulnerable to threats and major security violations from within and outside the organization such as phishing, social engineering, viruses, worms and others. Therefore, information security has become important to the organization because not only the internal information of the organization must be preserved, but also customer information must be taken into account, so information security is an important and critical strategic issue in organizational management.

Many organizations have made great efforts in managing and processing the security of their information. It has become necessary for you to develop policies, procedures, controls and regulatory structures to reduce the risks surrounding them or to implement the information security management system initiatives developed by international organizations.

The goal from the information security management system is the protection of the confidentiality, integrity and availability and to limit and control from any possible damage if the vulnerabilities are exposed[2]. It will help organizations identify appropriate controls, reduce risks and manage them properly through many technical and non-technical factors [3]. There are several private and government institutions It develops standards, frameworks and legal regulations to regulate a suitable level of information security and the use of technology in the right way. There are many standards used for information technology governance, which is a good starting point for leading the information security management and continuous improvement approach. Information security such as PRINCE2, COBIT, PMMM, ISO27001, BS7799, COSO, SOA, ITIL and PCI DSS [4]. In this paper, we analyze and compare the most common standards with analysis of some frameworks and standards that have been developed by researchers and with mention of the disadvantages and advantages of each framework and standard.
II. PROBLEM STATEMENT

With the organizations relying on technological development and communications in creating, storing and exchanging information among themselves, the bad side of technology emerged from threats, penetrations and violations of this information [5]. Therefore, there was an urgent need to protect information from all forms of threats, so there were attempts by researchers, scientists and organizations to provide protection for this information and it more appropriate methods are an information security management framework to strategically address threats [6]. And in this research we analyzed information security management systems frameworks.

III. ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORK IN ORGANIZATIONS

The principle behind the ISMS standards is that organizations must design and awareness of information security scenarios; Implementing a coherent set of policies and processes for managing risks, weaknesses and applications of their information assets you must have an effective and effective ISMS standard in the long run, adapting to developments in internal organization and external environment. There are many standards, models and framework for information management such as BS7799, PCIDSS, PMMM, ISO 27001, COSO, ITIL and COBIT and et al. In this section we provide an overview and analysis of the four largest ISMS standards; ISO27001, COBIT, ITIL and PCIDSS [7].

ISO/IEC 27001 standard

The International Organization for Standardization (ISO) is a global organization whose functions collects and manages various standards for various disciplines. The family of ISO 27000 standards is originally as a British standard 7799 in 1995 and later as ISO 17799 [8].

The ISO7001 family was designed as a framework for managing information security in various organizations that includes all policies and procedures on how to manage and control data [9].

The ISO2700 standard also provides a model for creating, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.

ISO / IEC 27001 can be considered a comprehensive system that combines The risk management, management of security, governance and compliance. It helps the organization to ensure the right people, processes and technologies are in place for the business model and facilitate a proactive, appropriate approach to managing security and risks.

COBIT (Control Objectives for Information and related Technology)

COBIT is a framework of best practices in IT governance created by Information on Systems Audit and Control Association (ISACA) to reduce the gap between technology and business requirements, as it gives technology auditors, senior management and all technology users procedures and processes how to manage technology risks in order to ensure the integrity of the information system [10].

COBIT contains five main principles as follows: Strategic Alignment; Delivery value resource management; Risk Management; Performance measure [11].

It also consists of 34 information technology processes to contribute to the effectiveness of internal controls over financial reporting reliability.

Information Technology Infrastructure Library (ITIL)

ITIL is the best practice framework to managing IT services for any organization. It was established in the late 1980s by the UK government, under the auspices of the Central Computer and Telecommunication Agency (CCTA) [12].

There has been development and modification of ITIL, and now we are ITIL v4.

ITIL Initial Edition comprises of a library of 31 related books covering all aspects of providing IT services. Between 2000 and 2004 this initial version was revised and replaced by ITIL V2; This consisted of seven more connected and coherent books rolled into an overarching framework. After a major update ITIL v3 was published in 2007 and consists of five core publications covering the service life cycle. In the 2011 editions were
It was posted to address commentary, improve clarity and consistency across ITIL’s five core posts, and introduce some secondary elements to staying up-to-date and meeting industry demand. The course is as follows: Service Strategy, Service Design, Service Transition, Service Operations and Continuous Service Improvement [13] [14]

**Payment Card Industry - Data Security Standard (PCI DSS)**

The PCI is a set of comprehensive requirements to improve the security of payment any account data. It is an information security standard to any organization which deals with cardholder information of leading credit card providers for example the American Express, MasterCard Worldwide and Visa Inc. PCI Compliance focuses on three steps: evaluation, reform, and reporting [15]

PCI DSS addresses 12 main requirements for control measures that are divided into topics including network Cardholder data protection, software for Vulnerability management, measures of access control, monitoring of Network, testing and information security policy. Each requirement is divided into sub requirements [16]

**Table-1:** Show Comparison between information security standards and frameworks

<table>
<thead>
<tr>
<th>Element</th>
<th>ISO27001</th>
<th>PCIDSS</th>
<th>COBIT T</th>
<th>ITIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategy of Information security</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Organization security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Corporate governance</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Compliance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Disaster recovery planning</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Management the user</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>incident management</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Technical operations</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Physical and environmental controls</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Security of human resource</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Security police and procedure</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Risk Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access Control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Assets Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**IV. OVERVIEW OF INFORMATION SECURITY MANAGEMENT FRAMEWORKS**

At present, there is no single superior information security management framework that can cover all potential issues and can be easily implemented in an organization. Therefore, Presently there are too many ISMS frameworks, it has been proposed by scientists, researchers, international organizations, companies, and government initiatives to protect and manage information security. All frameworks focus on their own perspective, and in this scientific paper we summarize some of them.

The researchers in [17] designed information security management framework for the Malaysian academic environment adapted from standards ISO 27001, MyMIS, COBIT, COSO and iso27001. The five main aspects were studied: the information security policy, management risk, access control, training and awareness programs and compliance, and through the study it was found that support for top management and training and awareness programs are the most important success factors for adopting an information security policy, This framework is more comprehensive and applicable to implementation for Management the Information Security for Malaysian Academic Environment , but the study was not mentioned the budget allocated to information security and incident management.
The researchers in [18], proposed the initial framework adopting From FFIEC, COBIT, ISO 27002 and PCI data security standard, For the governance of information security in the banking system, the framework has been classified into three main levels: the operational level, the technical level and the strategic level. This framework has focused on employee culture and behavior and considered it an important component of information security and In any bank, there must be controls for external parties that provide support for the information security of the bank, In this study, it was not mentioned despite its importance.

**Fig. 1:** Framework To Manage Information Security[17]

**Fig. 2:** Framework For The Governance Of Information Security[18]
In [19], Heru Susanto et al. designed a practical framework for assessing and monitoring the Information Security Management System (ISMS), called I-SolFramework System. The program assists stakeholders in assessing their level of readiness for implementing ISO 27001 for information security. The authors in this paper built the framework from the best important successful factors for ISMS consisting of the organization, stakeholders, the tools and technology, policy, culture, and knowledge. The researcher did not address the environmental and physical aspects, which are considered one of the most important aspects of information security, while his focus was on stakeholders.

![Fig-3: Framework to the development ISMS [19]](image)

In [20], Kazemi et al., designed a model consisting of the most important successful factors in implementing the ISMS in the Iranian municipality organization. Taking expert opinions, the model includes seven factors that are considered the most important success factors: support from top management, information security policy, responsibilities of job, motivation to employee, outreach and training programs to employee, compliance with international information security standards, and the use of the services of external information security consultants in implementing ISMS. The result of this study was to determine the most important factors, in a descending order, as follows: support from top management, policy to Information security and Training and awareness programs for employees are the most important factors for the success of implementing the information security management system. Although he did not study other factors concerning technology and organization policies.

Mohsa Mohsani in [21] designed a form to answer several questions. What are the strengths and weaknesses of information security in banks? What is the degree of commitment to ISMS in the bank? What is the degree of commitment to the information security management system in the bank? The model is designed according to four COBIT standards, NIST 800-66, ITIL and ISO27001. Result of a study of security policy in Iranian banks have average scores below 3.0 and their ISMS compliance is very low. Other factors have an average score of more than 3.0. Banks have realized the importance of meeting the requirements of the standards, however, they did not take the necessary measures to implement security guarantees, especially in the area of implementing security policies.

Abdellateef Lutfi Muhse in [22] in an unpublished master's thesis "Information Security Management In Palestinian Banking". The main objective in his research Checking and reviewing the current status management of information security in Palestinian banks, and Measuring the degree of implementation of security controls and issues related to risks and governance. The factors studied are as follows: people, processes, technology, external parties or partners, budget and data, the study Recommendations, Palestinian banks must follow international information security management standards, Palestinian banks should follow the development of technology and work to keep up with it to reduce the weakness of the technologies used in
banks. One of the advantages of this study is that it studied the budget factor devoted to information security, which was absent from most studies.

The researchers in [23] designed suggested Web-based Analytic Hierarchy (AHP) risk assessment model depend on the standard ISO27001:2013 in order to evaluate and weigh the importance of each element of the standard which Divided into five sections: Organization, Policies and Procedures, Assessments of Risk, Awareness and Training for user and Compliance for legal legislation.

The results weighed the importance of each element, which are as follows: efficiency of organization, consistent policy, training, education and legal legislation.

The researchers in [24] combines ISO 27001 with Zachman’s framework to design a framework that companies can use to manage information security. The framework consists of three aspects: technical, process and human, and provides guidance for the implementation of information security and operations management on the basis of ISO /IEC 27001. The authors considered that policy, processes and procedures were critical factors for the successful implementation of security management information, but the framework did not make any practical proposal to support its implementation by practitioners and did not address the budget allocated to information security.

The researchers in [25] proposed a High level self sustaining information security management framework. The framework was designed to adapt the most important security standards and best practices and Distinguishing the ISM framework from others a wide list of stakeholders was added in order to present the wide area of information security assurance and different type stakeholders' incorporation into the enterprise operations. Also The study carried out a comparative analysis of other ISM frameworks based on multiple factors while the other authors define evaluation criteria individually. As well the ISM framework was adapted for usage in a small and medium enterprise – self-assessment sheet with associated information security maintenance, modeling and evaluation tools accompanied the framework.

M Ula et al. in [26] A model was proposed for evaluating an initial framework for information security governance in the banking system, the framework was categorized into three level the technical level, Managerial level and Governance level and every level have sublevels see Fig[5]. Within this framework the weighting factor was measured for all component of the information security governing (ISG) in the banking environment and The researcher found the most critical components for ISG implementation in the banking system are: Strategy for Information Security, Information Security Policies, Guidelines and procedures, Monitor and auditing, plan for Business continuity and Disaster recovery plan, but The proposed framework does not measured weighting factor such as budget, access control and the external party.

The researchers in [27] suggested the ISMS framework specifically for the data center to management the confidentiality, integration and availability of information security. A framework that consisting three aspects the people, processes (Policies and Procedure) and technology To manage and protect security of information in the data center. This framework was developed in accordance with ISO 27001 standard and cover 21 information security controls as the fig.[25], and They were focused in the framework on the people factor, which they considered an important factor and depend on the concept plan -do-check -act Which supports continuous improvement. but The proposed framework doesn’t focus on others important factor, such as budget.
Zhao et al. in [28] proposed framework that provides a comprehensive view in information security management system and provide guidance to Security organizations and the practitioners who need to effectively implementation their information systems security management. The framework consists from five factors: Information security management system, organizational, human security, planning, strategic, and security policies. but This study is conducted on non-technical security issues only from an organizational perspective and not at the individual level and considers the commitment of top management and the security structure to be an important resource for the organization’s security.

Singh et al. in [29] proposed the framework for Governance the information Technology for the Indian Banking Industry. The framework combines the quality of service and information security, the quality of service involved in reliability, warranty, tangible objects, empathy and responsiveness combined with three critical factors in the information security, i.e. confidentiality, integrity and availability (CIA) to create a conceptual framework for IT governance in Indian banking. The researcher’s recommendations for Indian banks to adopt a comprehensive and strong framework such as COBIT for IT governance, must provide the necessary training for bank employees, and banks must work to improve the client’s perception of service quality and information security within the framework of work if the researcher focuses on the quality of information security service.

The researchers in [30] design Conceptual framework to compares multiple information security governance (ISG) frameworks XYZ in gas company in Indonesia’s with the (ISO 17799 framework, COSO, and the IT Risk Framework) depending in four factors People, Risk Management, Process And Business Dependency and identify the success and inhibiting factors for implementing ISG frameworks. From Three aspect human aspects, organization aspects, and technology aspects. Based on the evaluation results, it was found that the multiple ISG framework XYZ strategy has better effectiveness compared to the adoption of a single ISG framework. The results of the evaluation of the ISG framework implementation maturity level show a significant gap between the current maturity level and the expected maturity level, there are five factors that determine the successful implementation of ISG Management support factors, implementation of Information Security Policy (ISP), division of job responsibilities and compliance with information security standard and guidelines are all supporting factors for ISG implementation. Risk estimation is an inhibiting factor for the implementation of ISG in organizational aspects. Risk estimation is an inhibiting factor because this business is still reactive, marked by the absence of information classification and critical asset data collection. In the technological aspect, the complexity of information systems and applications as well as mobility and distribution access are inhibiting factors for ISG implementation. In this framework the data
collect from interview only and the multiple ISG framework XYZ not compare with COBIT framework to evolution.

![Fig. 6: The Conceptual Framework ISG Assessment and Evaluation](image)

### Table 2: Show Comparison of Information Security Management Frameworks:

<table>
<thead>
<tr>
<th>Authors/ year</th>
<th>Main objectives</th>
<th>Standards or frameworks</th>
<th>Factors of study</th>
<th>cons and pros of framework</th>
<th>Results of study</th>
</tr>
</thead>
</table>
| Z. Ismail et al. (2010) | Assesses the compliance to ISMS                                                | MyMIS ISO/IEC 27001, COBIT and COSO | information security policy, management of risk, access control, training and awareness programs and compliance, | pros: framework is more comprehensive  
cons: not mention budget | Building a framework for information security management in the Malaysian academic environment |
| Munirul Ula(2011)      | Development of guidelines and Implementation of security controls to protect the bank’s assets from threats | FFIEC, COBIT, ISO 27002 and PCI | Strategic, tactical, operational and technical                                    | pros: framework focused on employee culture and behavior  
cons: need additional components might be required like external parties and budget | A framework for information security governance |
| Kazemi et al(2012)     | - Identify the most important success factors that contribute to the implementation of an effective security management system Organization. | No a standard               | Top management, information security policy, job responsibilities, motivation of employee, training, compliance, consultants for external information security | Pros: Determine the most important success factors for implementing information security management  
Cons: it did not include all factors like | A model whose components are the most important success factors for implementing an information security management system |
<table>
<thead>
<tr>
<th>Authors/ year</th>
<th>Main objectives</th>
<th>Standards or frameworks</th>
<th>Factors of study</th>
<th>cons and pros of framework</th>
<th>Results of study</th>
</tr>
</thead>
<tbody>
<tr>
<td>H. Susanto (2012)</td>
<td>Help stakeholders assess the readiness to comply with ISO27001</td>
<td>ISO27001</td>
<td>The Organization, the Stakeholder, Tools &amp; Technology, Policy, Culture and Knowledge</td>
<td>Pros: Helping stakeholders understand the security control or invoke them by compliance parameters, Cons: did not address the environmental and physical</td>
<td>Framework to the development ISMS called I-SolFramework</td>
</tr>
<tr>
<td>Mahsa Mohseni (2015)</td>
<td>• assesses the compliance with ISMS, • implementation of information security; management of information security of Commercial Banks</td>
<td>NIST 800-66, COBIT 4.011, ITIL, ISO27001, ISO/IEC 27001:2013</td>
<td>Business Continuity Management, Compliance with Police, Access Control, Physical and Environmental Security, Communication Security, Organization, Management for Asset, Human security and Training</td>
<td>Pros: It was a comprehensive study based on several standards, Cons: not study budget Other impact factors such as external party and budget</td>
<td>A model to identify gaps between the requirements of security standards and the reality of ISMS implementatio n.</td>
</tr>
<tr>
<td>Shiann Ming Wu (2016)</td>
<td>• Design framework which can be used to manage the information security, • Ensuring that threat cannot affect company’s business</td>
<td>ISO 27001</td>
<td>All controls of ISO27001:2013 into the 5 parts; Organization, Infrastructure, Risk Assessments, User Awareness and Training, Compliance</td>
<td>Pros: Use with the proposed framework of concept Plan, Do, Check, Act (PDCA), Cons: Not study budget</td>
<td>Framework is Formed To Enhancing ISMS</td>
</tr>
<tr>
<td>Authors/ Year</td>
<td>Main Objectives</td>
<td>Standards or Frameworks</td>
<td>Factors of Study</td>
<td>Cons and Pros of Framework</td>
<td>Results of Study</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| W Fuadi et al. (2017) | • Evaluate governing the information security in banking system                 |                         | Technical factor, Managerial factor And Governance factor | Pros: Focusing to important factors and components that are assigned to banking corporate governance  
Cons: not study budget | framework for the governing information security |
| L. Kauspadiene (2017) | It aims to provide a comprehensive approach to an architectural reference model of the cooperative information security management framework. | No a standard           | Stakeholders                                        | Pros: Suitable for any type of organization  
Cons: Not comprehensive, focus on stakeholders only | framework serve the practitioners for guidelines to developing a comprehensive information security plan or the program in their organizations |
Cons: framework doesn't focus on others important factor such as budget | proposed ISMS framework Developing ISMS for Data Center |
| G. Zhao et al. (2019) | • Provide guidance to organizations and practitioners who need to effectively implement their information systems security management | No a standard           | Information system security management, organizational, human, strategic planning, and security policies  
Pros: It provides an integrated framework that provides a comprehensive view in managing effective information systems security  
Cons: This study is conducted on non-technical security issues | framework that provide guidance to Security organizations and practitioners who need to effectively implement their information systems security management, |
V. CONCLUSION

Through previous literature, it has been shown that effective management of information security is a systematic process to effectively deal with the threats and risks of information systems security in the organization. Technology is not sufficient to adopt successful management of information security. Therefore, there are many factors, recommended by organizations, that have to be integrated with technology to form a more comprehensive approach to information security management. Such factors are the commitment of Top management to the vision of information security, security structure, training for staff and security awareness, the establishment of a security culture in the organization, and the implementation of technologies competent, establishing strategic plans, developing comprehensive security policies, organizing and controlling, and protecting information assets and achieving all business objectives. Through this analysis of the frameworks, it was found that the best framework is that includes all factors and inputs that affect the improvement of information security, which includes people, technology and organizational processes. Although it is important to allocate a budget for information security, many researchers have not addressed it.

VI. REFERENCES


