INFORMATION SECURITY GOVERNANCE FRAMEWORKS IN CLOUD COMPUTING AN OVERVIEW

Muhaned Al-hashimi[1], Marini Othman[2], Hidayah Sulaiman[3], A. A. Zaidan[4]

[1] Department of Basic Science Branch, College of Dentistry, Tikrit University, Salah Al Din Governorate, Iraq

[2,3] Information Systems Department, College of Information Technology, Universiti Tenaga Nasional, Malaysia

[4] Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Malaysia

muhaned@tu.edu.iq, marini@uniten.edu.my, hidayah@uniten.edu.my, aws.alaa@gmail.com

ISSN (Printed): 2314-7350
ISSN (Online): 2231-8852

ABSTRACT

Although cloud computing creates new opportunities, it also creates new risks. Key to the successful adoption and transition of information systems to cloud is the implementation of a strategic proactive information security management and governance framework. Information security governance framework can help inform agency leaders, information security professionals, and information security governance participants on how to move into cloud environment without excessive information security risk or potential legal and regulatory compliance failures. However, very few sound ISG frameworks exist that can effectively guide most organizations in their ISG endeavors. This paper provides an overview of current information security governance frameworks in cloud computing, and demonstrates the stages and activities of a security governance framework. The paper also introduces the current efforts of evaluating these frameworks.

Key words: Cloud computing, Information security governance, Governance framework

1. Introduction

The term information security governance (ISG) describes the process of how information security is addressed at an executive level and a part of an organization's overall corporate governance responsibilities. Information security governance is considered to be a facet of an organization's broader corporate governance strategy, which itself commences at board level (Posthumus and Von Solms, 2004). Information Security Governance is now accepted as an integral part of good IT and Corporate Governance (Von Solms, 2005). Corporate governance is a set of responsibilities and practices exercised by organization board and executive management provide strategic direction, ensure that objectives are achieved, ascertain that risks are managed appropriately and verify that the enterprise's resources are used responsibly (Becker and Bailey, 2014). Security governance, as part of the company's corporate governance, is the most suitable path by which to gain control of security processes and guarantee an alignment with business strategies (Rebollo et al., 2015).

Information security governance is a subset of organizations' overall (corporate) governance program (Von Solms and Von Solms, 2006). Information security governance (ISG) consists of the leadership, organizational structures and processes that safeguard information inside an organization. ISG is the process of developing a framework and supporting management structure and processes to provide assignment of responsibility, all in an effort to manage risk. It also aims to provide assurance that information security strategies are aligned with and support business objectives and consistent with applicable laws and regulations through adherence to policies and internal controls (Rebollo et al., 2012).

Information security governance is the mechanism through which organizations can ensure effective management of information security. It is a critical component of a successful transition to the cloud (Miller et al., 2009). Moving into the cloud needs to develop a clear governance strategy and management plan by organization (Rebollo et al., 2012). Governance in the cloud requires defining policies and implementing an organizational structure with well-defined roles for the responsibility of information technology management, business processes, and applications as these elements are moved out of the traditional IT environment and into the cloud (Becker and Bailey, 2014). Typical governance activities such as goal setting, policy and standard development, defining roles and responsibilities, and managing risks must include special considerations when dealing with cloud technology and its providers (ISACA, 2009; Rebollo et al., 2012). Without a sound governance strategy that applies to both the organization and the cloud service provider, organizations risk ineffectiveness, loss of control and potential harm to their reputation from negative legal or regulatory

action (Ernst and Young, 2012).

Although cloud computing creates new opportunities, it also creates new risks. The nature of cloud deployment and service models presents new information security risks and introduces complications to compliance with legal, regulatory, and contractual security requirements for cloud consumers. Key to the successful adoption and transition of information systems to cloud is the implementation of a strategic proactive information security management and governance framework (Miller et al., 2009). Cloud providers and clients must work collaboratively to provide an assurance framework. Many respected IT organizations and standards setting bodies have established frameworks to identify the "risks and mitigation strategies with the evolving cloud computing paradigm. While no one framework or model encompasses all of the possible IT controls, collectively they cover the "what, how, and scope" of IT Governance with some duplication and overlap. To avoid potential pitfalls of extending governance to the cloud paradigm, organizations should put in place and sustain a practical governance framework to ensure cloud infrastructure and operations are as secure as traditional IT governance approaches (Becker and Bailey, 2014). The ever-changing environment of cloud computing leads to a need for a suitable assurance framework which deals with the different levels of security and against which the cloud model can be secured (Sloan 2009; Kavitha 2011). This paper provides an overview of information security governance, and on current information security governance frameworks in cloud computing, and the current efforts of evaluating these frameworks.

2. Cloud Computing Information Security Governance Framework

It is important to firstly establish understanding on the two important keywords: Cloud Computing and Information Security Governance.

The research team at the UC Berkeley RAD Lab clarifies the term Cloud Computing as referring to "both the application delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services." And," it is enabled by the construction and operation of extremely large scale commodity-computer datacenters" (Armbrust,2009). In keeping the information secure, mechanisms of monitoring and controlling must be in place. Information security governance (ISG) is an important integral of this mechanism.

The term information security governance (ISG) describes the process of how information security is addressed at an executive level and a part of an organization's overall corporate governance responsibilities. Information security governance is considered to be a facet of an organization's broader corporate governance strategy, which itself commences at board level (Subashini,2011) . Information Security Governance is now accepted as an integral part of good IT and Corporate Governance (Posthumus,2004). Corporate governance is a set of responsibilities and practices exercised by organization board and executive management provide strategic direction, ensure that objectives are achieved, ascertain that risks are managed appropriately and verify that the

enterprise's resources are used responsibly (Bailey,2014). Security governance, as part of the company's corporate governance, is the most suitable path by which to gain control of security processes and guarantee an alignment with business strategies (Rebollo,2012).

Information security governance is a subset of organizations' overall (corporate) governance program (Rebollo,2015) . Information security governance (ISG) consists of the leadership, organizational structures and processes that safeguard information inside an organization. ISG is the process of developing a framework and supporting management structure and processes to provide assignment of responsibility, all in an effort to manage risk. It also aims to provide assurance that information security strategies are aligned with and support business objectives and consistent with applicable laws and regulations through adherence to policies and internal controls (Rebollo,2011).

Information security governance is the mechanism through which organizations can ensure effective management of information security. It is a critical component of a successful transition to the cloud (Miller,2009). Moving into the cloud needs to develop a clear governance strategy and management plan by organization (Rebollo,2011). Governance in the cloud requires defining policies and implementing an organizational structure with well-defined roles for the responsibility of information technology management, business processes, and applications as these elements are moved out of the traditional IT environment and into the cloud (Bailey,2014). Commonplace governance exercises, for example, objective setting, policy and standard advancement, characterizing roles and duties, and overseeing risks must incorporate unique contemplations when managing cloud innovation and its providers ((Isaca et al., 2009; Rebollo,2012). Without a sound governance procedure that applies to both the organization and the cloud provider, organizations risk ineffectualness, loss of control and possible damage to their reputation from negative legitimate or administrative activity (Ernst & Young, 2012).

ISG cloud framework is a process oriented in view of an activities set, which give a structured method of building up a security governance structure supporting a cloud computing service. ISG cloud offers an exact depiction of activities that that ought to be surpassed to ensure cloud service security governance. ISG cloud's tasks also incorporate various references to existing direction and support of security principles that may be utilized as a part of request to encourage its usage and performance (Rebollo,2015) . Normal ISG activities such as objective setting, policy and standard advancement, roles and responsibilities definition and management of risk must involve special considerations when managing cloud technology and its providers (Rebollo,2012)

Information security governance framework has the ability to inform agency leaders, professionals of information security, and participants of information security governance on how to benefit of the benefits from Cloud Computing Environment (CCE) without compromising their mission to high information security risk or possible legal and regulatory compliance defect (Miller,2009) . However, few robust ISG frameworks exist that can efficiently direct most organizations in their ISG (Posthumus & Von Solms, 2004). Research by (Rebollo et al., 2011b)

conducted a comparative analysis through reviewing different ISG frameworks in the light of corporate governance, information security domains, and information technology governance. The analysis results revealed that although each framework tries to deal with ISG in a through way, some aspects are addressed more than others. Issues such as strategic alignment, process management, and risk management are addressed in adequate details by nearly all proposals, however, other issues such as value delivery through IT or control and responsibility are addressed less frequently. When transferring these security frameworks to be deployed in cloud, the same vigilances must be taken. More significantly, the control loss which is inherent in cloud should be compensated with further security controls to mitigate vulnerability.

3. Important aspects in Cloud Computing ISG

The review has noted consistent aspects highlighted by researchers pertaining to governance of security in cloud computing: close attentions to aspects involved during deployment of the cloud; development phases and process; and actual security measures or steps at a given phase or process.

3.1 The Pillars

Rebollo (2012), Indicated that frameworks in a cloud computing deployment are supported by three pillars namely:

3.1.1 Policies and Processes Adaptation (PPA)

- Redefining the processes and evaluating security policies according to the cloud paradigm.
- Implementation of new security processes and procedures in order to achieve organization goals.

3.1.2 Control and Audit (CA)

Control these new processes, which run out of the organization's boundaries into the cloud provider. The control and audit criterion embraces the additional security controls that should be established owing to the new cloud relationship. It includes:

- Definition of new security controls
- Security metrics for evaluation information security,
- Performance management by monitoring security strategies and processes
- Provide tools to access Cloud Provider Logs
- Audit and evaluate the services provided by the cloud by monitoring its levels

3.1.3 Service Level Agreements (SLA)

This agreement reflects the commercial relationship between the cloud client and the provider. The SLA is a tool that allows customers to define the security requirements during the provision of the cloud service. Moreover, this agreement should offer a commitment to provide the security services required by the cloud provider. The SLAs should include all the security aspects that the organization wishes to control.

3.2 Management Process

Miller (2009), Developed an information security management and governance framework which is based on evolving international standards and planned evolution of the national institute of standards and technology (NIST) risk management framework. The framework includes seven management processes: strategy and planning, policy portfolio management, risk management, awareness and training, communication and outreach, compliance and performance management, and management oversight. The management processes interact in a Plan, Do, Check, Act cycle of continuous improvement to effectively manage and govern enterprise information security.

3.3 Life Cycle

Rebollo (2015), Proposed an ISG cloud framework to a real-life case study of a Spanish public organization. The framework includes six stages with different activities as shown in table 1 below:

Table 1: ISG cloud framework stages and activities

Stage	**Security Steps**
Planning/ Strategy Definition	Establish Information Security Governance structure
	Define Information Security Program
Cloud Security Analysis	Define Information Security requirements
	Cost/benefit analysis of available cloud options
	Cloud risk analysis
Cloud Security Design	Define SLAs and legal contracts
	Establish Information Security roles and responsibilities
	Specify cloud service monitoring and auditing
	Define applicable security controls
Cloud Implementation/Migration	Secure cloud implementation
	Educate and train staff
Secure Cloud Operation	Cloud security operation
	Communicate information security inside the organization
Cloud Service Termination	Cloud service termination

An empirical evaluation of the framework proves its validity and demonstrates the usefulness of the framework to the organization. The evaluation focused on cloud service security (if it is covered

by the cloud provider's solution), development of a security governance structure (Governance metrics need to be defined in order to evaluate the state of security governance inside the organization after the service deployment), and the practical applicability of ISG cloud framework (is it easy and useful).

ENISA (2015), Proposed a governmental cloud security framework based on the Plan-Do-Check-Act (PDCA) cycle. The analysis of literature indicated that main security challenges, requirements and barriers in the governmental cloud are related to: data protection and compliance, interoperability and data portability, identity and access management, auditing, adaptability and availability, as well as risk management and detailed security SLA formalization. Based on the analysis of collected data and some preliminary interviews, a logic model for a security framework for governmental clouds was developed including the specific activities and steps as shown in table 2. The framework is flexible enough to include new requirements. The frame work was applied on governmental cloud use cases in several European countries. The use cases help to define a generic security framework through the analysis of the strategies adopted by selected countries from the security perspective.

Table 2: Overview of the proposed security framework

Lifecycle Phase	Security Activity	Security Steps
PLAN This phase focuses on setting policies, a strategy for implementing controls to achieve security objectives	Risk Profiling	Identify services to "cloudify"
		Select relevant Security Dimensions
		Evaluate individual impact to dimensions
		Determine global Risk Profile
	Architectural Model	Decide on the deployment-Service Mode
	Security & Privacy requirements	Establish Security Requirements
DO This phase involves implementing and operating the controls, i.e., controls are executed in the DO Phase	Security Controls	Selection of security controls
	Implementation, Deployment & Accreditation	selected security controls Formalization and implementation
		ex ante verification of suitability of Cloud service to provide due level of assurance

		Start service execution
CHECK This phase is focused on review and evaluation of the performance (efficiency and effectiveness) of the system. Tests are performed to ensure that controls are operating as intended and meet objective	Log/Monitoring	Periodically check that security controls are in place and being followed
	Audit	Verification that the defined / contracted levels of security are fulfilled
ACT This phase involves remediation of deficiencies or gaps identified in the CHECK Phase. Changes are made where necessary to bring the system back to the planned performance	Changes Management	Implementation of remedies and improvement to the security framework / approach
	Exit Management	Contract termination, return of data to customer and data deletion

4. Current Information Security Governance Frameworks

Several cloud computing information security governance (CCISG) frameworks have been proposed by researchers, agencies and associations. A summary of existing such frameworks are introduced in table 3.

Table 3: Existing CCISG Frameworks

CCISG Frameworks			
Authors/Year	**Outcome**	**Brief description**	**Evaluation criteria**
The European Network and Information Security Agency	information assurance framework	(ENISA) has published a guide which assesses the security risks and benefits of using Cloud Computing, and provides security guidance for potential and existing	The study evaluates set of assurance criteria which are based on the controls from the ISO

(ENISA) (2009)		users. This guide reviews technical and legal risks, along with policy and organizational issues. These risks are used as a starting point for introducing an information assurance framework, which is based on the controls from the ISO 27000 family.	27000 family.
Jericho Forum (2009)	Cloud Cube Model	The model's objective is to assist in determining which cloud formation is best suited to the business' needs, along with enabling secure operation through the chosen option. The Jericho Forum's model proposes the development of a Collaboration Oriented Architecture (COA) to assure secure business in de-parameterized environments. The COA framework includes a set of guidelines with which to guarantee secure interaction between users and end systems located in different security domains.	The Jericho Forum has identified 4 criteria to differentiate cloud formations from each other and the manner of their provision.
Tim Mather, Subra Kumaraswamy and Shahed Latif (2009)	Cloud Security and Privacy	The authors address issues that affect any organization preparing to use cloud computing as an option. They propose an introductory view to a variety of security issues related to Cloud Computing, so that users can be confident of dealing with the most important concerns.	The authors highlight a set of criteria dedicated to ISG issues such as Managing identity, Defining service requirements, Monitoring service levels, and providing assurance in internal controls, managing incident response, or Developing a business continuity

			program, audit and compliance functions.
The Cloud Security Alliance (CSA) (2009)	Security Guidance for Critical Areas of Focus in Cloud Computing	CSA has published guidelines on different security issues related to Cloud Computing. The guide has a section which deals with Governing in the Cloud, whose second domain is dedicated to Governance and Enterprise Risk Management. The proposed guidelines are not compulsory and may not all be applicable to every cloud deployment, but help to identify threats in the cloud context and to choose the best options by which to mitigate vulnerabilities.	The authors identify a set of criteria in two domain governance and operations. The governance domains are broad and address strategic and policy issues within a cloud environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.
Klaus Julisch and Michael Hall (2010)	Security and Control in the Cloud	Authors propose expanding the concept of an Information Security Management System (ISMS) from ISO/IEC 27001 to virtual ISMS. An ISM includes the set of processes and policies used by an organization to implement, operate and monitor information security. The Plan-Do-Check-Act (PDCA) cycle is adapted to the virtual ISMS. They analyze public cloud's SLAs and conclude that they tend to protect cloud providers with small penalties in comparison to the risk that is	The authors adopt the iterative PDCA cycle to define, implement and review the organization's internal processes. Continuous iterations are used to refine the processes in order to achieve their control objectives.

		transferred.	
The Information Systems Audit and Control Association (ISACA) (2011)	IT Control Objectives for Cloud Computing	The (ISACA has recently published [ISACA (2011)] with the purpose of providing an understanding of Cloud Computing and identifying its related risks. This framework deals with governance, security and assurance aspects separately.	The publication Identify the related risks, controls and frameworks that can be used as a criteria to address challenges and maximize value in the cloud.
Nia Ramadianti Putri ,Medard Charles Mganga (2011)	framework that is suitable to identify information security metrics	The overall aim of this study is to identify Service Level Agreement (SLA) based information security metrics cloud computing using the COBIT framework. The author identified 41 SLA based information security metrics to aid both cloud providers and customers obtain common security performance expectations and goals	The author identify threats and security attributes applicable in cloud computing. He also selects a framework suitable for identifying information security metrics. Moreover,He identifies SLA based information security metrics in the cloud in line with the COBIT framework.
Oscar Rebollo, Daniel Mellado and Eduardo Fernández-Medina (2012)	comparative framework	This paper presents a systematic literature review whose objective is to seek existing Information Security Governance frameworks that may assist companies in defining a clear governance strategy with regard to the security of its information assets.	The author analyzed the frameworks and provided a set of comparative criteria that consider the particularities of Cloud Computing when dealing with security governance issues.
ENISA, 2015	Security Framework for Governmental Clouds	A governmental cloud security framework based on the Plan-Do-Check-Act (PDCA) cycle. The framework is flexible enough to include new requirements.	The security framework has been empirically validated through four Gov Cloud case studies: Estonia, Greece, Spain and UK.

Table 3 revealed encouraging results in the area of evaluating an Information Security governance framework and criteria that have been specifically designed for the Cloud Computing environment. However, considerable work is still needed to specify a proper selection method of a suitable and optimal CCISG framework. The task of selecting CCISG framework has become more complex and difficult among the available frameworks. This difficulty is exacerbated due to lack of technical knowledge and experience of decision makers; and continuous improvements in information technology in various environments.

5. Evaluation of Cloud Information Security Governance Framework

Most cloud users of a private or a public cloud have certain expectations for their data security. Furthermore, the owner and operator of a cloud share responsibility for ensuring that security measures are in place, and the standards and procedures are followed. A good starting point to measure the presence and effectiveness of the cloud security includes having a list of required or recommended security controls. Measuring the presence and/or effectiveness of security controls (against security requirements) is largely what security evaluations are intended to do. Security evaluations have broad value as guidance for planning or developing security and for verifying that required controls are properly implemented. But evaluations also have utility for procurement of cloud services; for instance, a CSP may choose to publish the high-level results of a third party security evaluation. Several efforts have been conducted to offer guidance for cloud security as shown in table 4 (Winkler,2011):

Table 4: Efforts for evaluating cloud computing

Committee	Efforts
Cloud Security Alliance (CSA)	- Cloud Controls Matrix (CCM) - Consensus Assessments Initiative Questionnaire - Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 - Guidance for Identity & Access Management V2.1 - Cloud Audit
European Network and Information Security Agency Leading	Cloud Computing: Information Assurance Framework
	Cloud Computing: Benefits, Risks and Recommendations for Information Security

The Federal CIO Council's	Security Assessment and Authorization for U.S. Government Cloud Computing.
The Trusted Computing Group (TCG)	Trusted Multi-Tenant Infrastructure Work Group, which aim to develop a security framework for cloud computing
The Information Systems Audit and Control Association (ISACA)	Provide a framework to understand Cloud Computing and identifying its related risks. the framework deals with governance, security and assurance aspects

The offered guidelines are not compulsory and may not all be applicable to every cloud deployment, but help to identify threats in the cloud context and to choose the best options by which to mitigate vulnerabilities (Alliance,2009).

All of these efforts are relatively are intended to serve as a starting point for more formal work toward a common framework for cloud security as much of the previous cloud computing world has not adopted security evaluation frameworks. The intent of developing a cloud security evaluation checklist is to have a uniform means to verify the security of a cloud and also to obtain assurance from a CSP about their security. One application for the checklist is that a cloud owner can use it to guide a security evaluation of their cloud. If cloud providers use such a checklist as a framework to report on the security of their clouds, then prospective tenants and users could compare the relative security of multiple clouds (Catteddu,2009; Winkler,2011).

Rebollo (2011), conductive a comparative review to analyzes existing information security frameworks that have been specifically designed for the cloud computing environment. This comparison is performed using the eleven security control clauses from the ISO/IEC 27002 standard as evaluation criteria. Some other criteria are also introduced to evaluate cloud particular conditions such as the alignment between client IT security policies and cloud provider implementation, and liability, which reflects the relationship of responsibility between the cloud customer, the provider and applicable laws. Analysis results show that cloud specific criteria and those that gather traditional security issues, which are usually related to a technical point of view, are widely taken into account in the proposals studied. Of these criteria, the following can be highlighted: access control, communications and operations management, physical and environmental security, and compliance. However, aspects related to organizational management are less frequently considered. These are security policy, asset management and human resources security.

6. Discussion

Befor moving to cloud computing organizations need to redefine their processes and re-evaluate security policies when. Therefore, It should have the ability to control these new processes, which run into the cloud out of the organization boundaries. It has been indicated that policies and processes, control and audit (CA), and service level agreement represent the most relevant criteria for differentiating ISG frameworks in a cloud computing deployment. However, the frameworks differ in their criteria, which impede the proper framework selection process. For example some of them provide guidelines and others provide recommendations or checklists, while some provide sub criteria procedure, tool, metrics or policy. Moreover some frameworks focus on policy and others on audit and control or SLA. Generally, each framework attempts to deal with ISG in a comprehensive manner even they focus on specific issues more than others. However, almost frameworks consider adequately issues such as risk management, strategic alignment or process management with less consideration on control and accountability. Furthermore, all the frameworks lack to a framework selection method, which can help organizations to select the suitable framework that meets their requirements.

7. Conclusion

Results have been achieved is encouraging in the area of evaluating information security governance frameworks and defining criteria that have been specifically designed for the cloud computing environment. However, selecting proper and efficient CCISG framework has become more complex among the available frameworks. This difficulty is exacerbated due to lack of technical knowledge and experience of decision makers; and continuous improvements in information technology in various environments. In general, a considerable work is still needed to specify a proper selection method of a suitable and optimal CCISG framework.

REFERENCES

1 Alliance, C. S., Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance, V2.1, 2009.

2 Bailey, J. D., IT Controls and Governance in Cloud Computing. AMCIS Proceedings forthcoming (hlm. 20). Savanah: Twentieth Americas Conference on Information Systems, 2014.

3 Daniele Catteddu, G. H., Cloud computing risk assessment. European Network and Information Security Agency (ENISA), 2009, 583-592.

4 ENISA., Security Framework for Governmental Clouds. European Union Agency for Network and Information Security, February 2015.

5 Martinus, I., Sharief, M., Graul, B.: Government of Iraq E-government Strategy (2007-2010). USAID. Bearing Point, Inc, 2007.

6 Jamie Miller, L. C., Information Security Governance-Government Considerations for the Cloud Computing Environment. Booz Allen Hamilton, 2009.

7 Kevin, S., Security in a virtualized world. Network Security, 2009, 15-18.

8 Michael Armbrust, A. F., Above the Clouds: A Berkeley View of Cloud Computing. Berkeley / Technical Report No. UCB/EECS-2009-28.

9 Oscar Rebollo, D. M.-M., Comparative Analysis of Information Security Governance Frameworks: A Public Sector Approach. ECEG -Proceedings of the 11th European Conference on E Government: ECEG2011 (hlm. 482 - 490). Slovenia: Academic Publishing Limited Reading UK, 2011.

10 Oscar Rebollo, D. M.-M., A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. Journal of Universal Computer Science, vol. 18, no. 6, 2012, 798-815.

11 Oscar Rebollo, D. M.-M., Empirical evaluation of a cloud computing information security governance framework. Information and Software Technology, 58, 2015, 44–57.

12 Rossouw von Solms, S., Information Security Governance: A model based on the Direct–Control Cycle. Computers & security, 25, 2006, 408–412.

13 S. Subashini, V. K., A survey on security issues in service delivery models of cloud computing. Network and Computer Applications, 2011, 1-11.

14 Shaun Posthumus, R. v., A framework for the governance of information security. Computers & Security / Elsevier, 23, 2004, 638, 646.

15 Solms, S., Information Security Governance - Compliance management vs operational management. Computers & Security, 24, 2005, 443,447.

16 Winkler, V., securing the Cloud: Cloud computer Security techniques and tactics. Elsevier Inc., 2011.

17 Young, E. a., Ready for takeoff: Preparing for your journey into the cloud. EYGM Limited, 2012.

18 Muhaned Al-Hashimi, Shakir, M., & Hammood, Address the challenges of implementing Electronic Document System in Iraq E-government – Tikrit city as a case study, Journal of Theoretical and Applied Information Technology, Vol. 95, No.15, 2017, pp. 3672-3683.