A Context Establishment Framework for Cloud Computing Information Security Risk Management Based on the STOPE View

Bader Saeed Alghamdi, Mohamed Elnamaky, Mohammed Amer Arafah, Maazen Alsabaan, Saad Haj Bakry

(Corresponding author: Mohamed Elnamaky)

College of Computer and Information Sciences, King Saud University
Riyadh, Saudi Arabia
(Email: melnamaky@ksu.edu.sa)

(Received Nov. 15, 2017; revised and accepted Apr. 21, 2018)

Abstract

A basic need for cloud computing services is to provide them with sound "Information Security Risk Management (ISRM)" solutions. The initial essential step toward providing such solutions is to identify a context that determines all security issues. This paper introduces a management framework that targets modularity and comprehensiveness. The framework is based on the structured wide-scope view of Strategy, Technology, Organization, People and Environment (STOPE); and on recent publications related to ISRM by standards, published research work. The outcome of the work would provide a useful context establishment management tool for the future development of ISRM for cloud computing.

Keywords: Cloud Computing; Information Security; Risk Management; Structured Views

1 Introduction

Cloud computing is basically a shared computing system among various users. Two reputable organizations, the International Telecommunication Union (ITU) and the National Institute of Standards and Technology (NIST), have provided the following common definition for cloud computing: *"Cloud computing is a model for enabling ubiquitous, convenient on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications & services) that can be rapidly provisioned and released with minimal management efforts or service-provider interaction"* [1, 24, 28].

Another reputable international organization, the International Standards Organization (ISO), also provided its own definition of cloud computing as follows: *"Cloud computing is a paradigm for enabling network access to a scalable & elastic pool of sharable physical or virtual resources with self-service provisioning and administration on-demand"* [20].

The two definitions reflect the fact that cloud computing drives toward making computing a public service for individuals and for organizations, removing the burden of running their computing facilities from their private facilities to somewhere else expressed as "the cloud".

Considering risk management issues, it has been viewed that information security risk management is the process in which identification and analysis of risks are integrated. This process also combines the assessment of risk impact and decision to eliminate or reduce the risk. ISRM requires an identification and evaluation of the organization's assets, impact and likelihood of security incidents, and finally a cost analysis of the investment in security protection. Risk assessment and risk treatment are the two main phases typically enclosed in the ISRM process. Risk assessment phase aims to determine whether existing protection is sufficient to protect information assets by providing information about threats and system vulnerabilities. Risk treatment phase targets the selection and implementation of security measures to reduce the risk through different approaches namely; risk avoidance, risk mitigation, risk transfer and risk acceptance [22, 31].

It has been emphasized by ISO and NIST that a systematic approach is necessary to create an effective information security management for computing systems. For this purpose, both organizations have provided recommended specific frameworks and application approaches [22, 32]. Recognizing the special security requirements of cloud computing, ISO and NIST provided special recommendations for cloud security [19, 30]. In addition, various researchers in the field have produced useful ISRM tools for computing systems and for cloud computing [3, 12, 18, 27, 38, 40, 43].

Information security in cloud computing is not a problem that could be resolved by technology alone. Security

risks are present in organization's information systems due to technical failures, system vulnerabilities, human failures, fraud or external events. Integration among IT, organization and human factors is needed to gain sufficient knowledge of an effective ISRM, which can be designed to protect the confidentiality, integrity, and availability of information assets. [12].

This paper develops a management framework for cloud computing ISRM context establishment that enjoys comprehensiveness in accommodating the various issues concerned, and modularity in the flexible organization of these issues. The framework is based on Bakry's structured view of "Strategy, Technology, Organization, People and Environment: STOPE" on the one hand [36, 39]; and on recent publications related to ISRM by organizations concerned with standards and by various researchers working in the field on the other. The paper makes the following contributions.

- It describes the basic issues of the problem including: (1) the cloud computing architecture; (2) the key ISRM sources of information and recommendations; and (3) the structure of the targeted comprehensive and modular management framework.
- It maps the key wide-scope ISRM requirements, collected from various sources, to the structure of the targeted management framework, which is based on the STOPE view.
- It delivers the targeted STOPE based management framework of ISRM context establishment, emphasizing its comprehensiveness in accommodating the various issues concerned in a well-organized and flexible modular form.
- It uses the resulting management framework as an initiation tool for the development of ISRM for cloud computing.

The rest of this paper is organized as follows: Section 2 describes the basic issues in cloud computing, and introduces the comprehensive and structured STOPE view. Section 3 presents the proposed ISRM framework. And finally, in Section 4 discusses the implications of the work and highlights future research.

2 Basic Issues and the Structuring View

This section identifies the cloud computing architecture and the recent key ISRM recommendations. It also describes the structured STOPE view used for providing the targeted cloud computing ISRM context establishment management framework.

2.1 Cloud Computing Architecture

The cloud computing architecture is developed to enjoy various needed characteristics. While NIST [28] and the ITU [24] jointly list five main characteristics, ISO [20] adds an extra one making them six. These six characteristics are summarized in Table 1. The three reputable standards organizations have considered the cloud computing architecture to provide three main types of service: (1) Infrastructure as a Service (IaaS); (2) Platform as a Service (PaaS); (3) Software as a Service (SaaS). These types of service are illustrated by Figure 1 against the layered architecture of cloud computing provided by ITU [25].

Table 1: A Summary of the main characteristics delivered by the cloud computing architecture

Providing	Computing resources for "on-demand self-service" by customers.
Enabling	Customers to access the resources through "broadband network access".
Servicing	Multi-customers through "resource pooling".
Delivering	The service with "rapid elasticity and scalability" in terms of responding to demands rapidly and with what appears to be unlimited resources.
Providing	"Measured service", with transparency to both the customer and the service provider.
Ensuring	"Multi tenancy" in terms of isolating each customer computations and data from others.

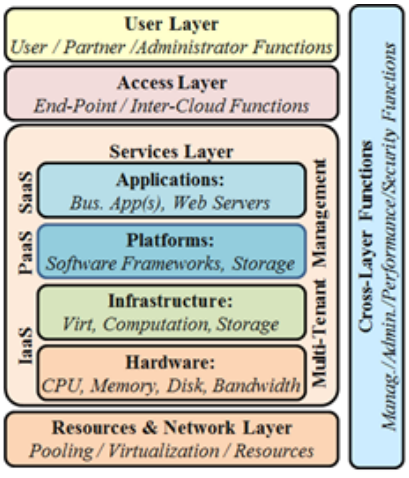

Figure 1: The ITU layered architecture of Cloud Computing Reference

2.2 Key ISRM Sources

There are two main sources for ISRM at the traditional computing systems level and at the cloud computing level.

These two sources are as follows.

- Documents on the subject issued by international and national organizations concerned with standards.
- Research papers published in refereed journals and conferences.

Key ISRM references associated with the two sources have been taken into account. Table 2 lists the main topics addressed by the various sources considered; and alongside each topic, the table shows the corresponding publication sources, and their related references. The elements of the ISRM requirements for cloud computing, addressed by these sources, will be mapped on the proposed context establishment management framework structure described in the following sections.

Table 2: Key ISRM sources of requirements related to cloud computing

Topic	Sources
Information technology - Security techniques - IS risk management [22]	ISO
Security techniques - Code of practice for IS controls based on ISO/IEC 27002 for cloud services [21].	ISO
Information security - Guide for applying the risk management framework [32]	NIST
Cloud computing security reference architecture [30]	NIST
A risk assessment framework for cloud computing [18,38]	IEEE
Security risks and their management in cloud computing [41,42]	IEEE
ISRM framework for the cloud computing [4, 26]	IEEE/ IAJC
A quantitative model for ISRM [12]	EMJ

2.3 The STOPE View

Bakry's five-domain structured view of "Strategy, Technology, Organization, People and Environment (STOPE)" has been widely used for developing comprehensive and modular views of various aspects of information technology services systems, including security and various other aspects [9, 10, 33]. Examples of these systems are given in Table 3.

Based on experience, using the STOPE view has been useful in providing two main benefits to its users. The first is comprehensiveness, where the different existing and potential issues, concerned with problems related to those of Table 3, are accommodated into its various wide-scope domains. The second is modularity, where these issues are well classified and structured per well-defined domains. These two benefits ease the management of the issues through accommodating them within a well-structured wide-scope framework on the one hand, and through grouping the related issues, and enabling flexibility in their detailed analysis.

Table 3: Examples of IT related systems, where the STOPE framework is used for their structured description

Systems	Example of references
E-Government	[10]
ISO 17799: 2005 information security management system	[34, 35]
ISO 27001 - ISMS	[39]
E-Business	[33]
Enterprise resource planning	[11, 36]
E-readiness assessment	[5, 6, 7]
Grid computing	[9]
IS Policies	[29]

Considering the experience in the STOPE view, the view would be an appropriate choice for addressing and managing ISRM context requirements for cloud computing. The STOPE view is illustrated in Figure 2 considering the main component of a security problem.

Figure 2: The STOPE framework & the security problem

The framework would support the management of the various issues of the security problem in cloud computing. The various "assets", accidental and malicious "security threats"; and the physical, administrative and technical "protection controls" can be associated with the different

TOPE domains. The framework "strategy" deals with these issues toward providing confidentiality, integrity and availability effectively and efficiently. The STOPE view will therefore be used in the next section for building the targeted management framework of cloud computing ISRM context establishment.

3 The Framework

The targeted cloud computing ISRM context establishment management framework, based on the comprehensive and modular STOPE view, is presented in this section. Figure 3 gives an illustrative view of the structure of the framework within ISO 27005 information security risk management process [22], which is based on ISO 31000 risk management principles and guidelines [23].

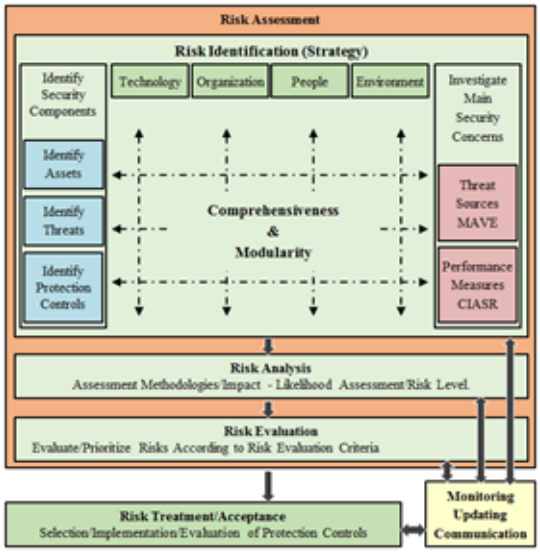

Figure 3: Structured STOPE-based Framework

The Figure has the following main components.

- The first component gives the basic structure of the targeted context establishment STOPE-based management framework which is described in the coming subsection of this main section.
- The second component is concerned with the risk analysis activity of the risk management process [8, 37], which considers the likelihood and impact of the various risks and determines the risk levels.
- The third is associated with the risk evaluation activity that considers risk evaluation criteria.
- The fourth is related to risk treatment and risk acceptance that consider all the above.

The consecutive activities of Figure 3, from the second to the fourth, receive and request information from the first, which is the context establishment. Therefore, a comprehensive and well-organized context establishment would provide great support to risk management. The targeted framework concerned with this is described in the following per the main domains of the STOPE view.

3.1 Strategy

The strategy is addressed here in terms of its security concerns, which include the following:

- The "basic principles" of the strategy, which involve its main targets.
- The various "assets" of cloud computing.
- The expected "threats", which result from "malicious actions (M); accidental events (A); vulnerabilities (V); or environmental causes (E)".
- The available "protection controls" that can be used to reduce the consequences of the threats.
- The "performance measures", which are associated with "the confidentiality of information (C); the integrity of information (I); and the availability of the services (A)". In addition, the overall safety of the cloud and its associated elements (S), and the reputation of the organization concerned (R) are also important measures.

Table 4 elaborates on these concerns and gives previous literature associated with them. Table 5 through Table 7 provides a structured view of the components of cloud computing assets, threats and protection controls per the TOPE domains.

3.2 Technology

The components of the "technology assets" associated with the cloud computing layered architecture are described in Table 8. They can be classified into four types:

- Hardware basic components.
- The infrastructure virtualization components that enable multi-users to share the cloud "IaaS".
- The system software and the essential platform services components that enable the provisioning of "PaaS" to various users.
- The application software and the essential software services components that enable the provisioning of "SaaS" to various users.

The main "threats" associated with technology are summarized in Table 9. They consider the "failure" of the various components of cloud computing technology resulting from different malicious actions, accidental events, vulnerabilities, and environmental reasons (MAVE). Such failures threaten "service availability (A)" leading to "denial of service". They also threaten the "reputation (R)"

Table 4: Strategy concerns

Issue	Concern
Basic Principles	Minimization of potential risks
	Security, integration and reliable performance are the top concerns in cloud computing
	Multi-party trust, Mutual auditability and any other considerations identified as security requirements [13]
Assets	Comprehensive ID of assets.
	Assets are associated with: "technology, organization, people and the environment".
Sources of Threats	Comprehensive identification of security incidents threats [13,14,15, 17]
	Threats result from: malicious actions (M); accidental events (A); vulnerabilities (V); and environmental reasons (E): "MAVE".
	Threats are associated with: "technology, organization, people and the environment".
Protection Controls	Comprehensive identification of investment in security protection [16].
	Protection controls are associated with: "technology, organization, people and the environment".
Performance Measures	Key performance measures are: confidentiality (C) of information; integrity (I) of information; and availability (A) of given services: "CIA". In addition, safety (S) and reputation (R) are also important targets to maintain. These five performance measures for the cloud platforms outline the STOPE-based CIASR framework.

Table 5: Assets

Type of asset	Asset	
	ID	Description
Technology	AT	All assets concerned with technology
Organization	AO	All assets concerned with the organization
People	AP	All assets concerned with people
Environment	AE	All assets concerned with the environment

Table 6: Threats

Type of threat	Threats	
	ID	Description
Technology	TT	Threats related to technology
Organization & People	TOP	Threats related to the organization / people
Environment	TE	Threats related to the environment

Table 7: Protection controls

Type of protection	Threats	
	ID	Description
Technology	PT	Protection associated with technology
Organization & People	POP	Protection associated with the organization / people
Environment	PE	Protection associated with the Environment

Table 8: Technology Assets (AT)

Type of asset	Asset	
	ID	Description
Hardware *Basic components*	AT (1)	Data processing equipment
		Transportable and Fixed equipment
		Processing peripherals
		Data and Electronic medium
		Networking Equipment
		Communications media and interfaces
Infrastructure *Virtualisation components*	AT (2)	Virtualization and customer management components
System Software *Platform services components*	AT (3)	Operating system
		Service, maintenance or administration software
		Package software or standard software
Application Software *Software services components*	AT (4)	Basic business application
		Specific business application

of the cloud computing provider, and generally the serviced customer too. In addition, threats associated with technology "destruction attacks" that may lead to various malfunctions that threaten the confidentiality (C) and the integrity (I) of information are also considered.

Table 9: Threats related to Technology (TT)

Type of threat	Threat ID	Threat Description	Source	Eff.
Hardware failures	TT (1)	Hardware	MAVE	(A) (R)
Infrastructure failure	TT (2)	Infrastructure: Virtualization		
System software failures	TT (3)	System & essential software		
Application software failure	TT (4)	Application software		
Destruction attack	TT (5)	Such as various virus attacks leading to malfunction	MV	+ (C) (I)

The "protection controls" concerned with the technology involve providing "back up" to the various technology layers of the cloud. Therefore, the service "availability" and organization "reputation" can be maintained, and "business continuity" achieved. In addition, "immunity tools" are considered to protect the cloud technology from destruction attack, and achieve confidentiality and integrity. These protection controls are summarized in Table 10.

Table 10: Protection controls concerned with Technology (PT) - The below ensures "business continuity"

Type of control	Protection controls ID	Protection controls Description	Eff.
Hardware back-up	PT (3)	Hardware protection	(A)
Infrastructure back-up	PT (4)	Infrastructure / Virtualization protection	
System software backup	PT (5)	System & essential software protection	
Application software backup	PT (6)	Application software protection	
Immunity tools / Security patches	PT (7)	Protection tools from destruction attacks such as: Firewalls & Anti-Virus	+ (C) (I)

3.3 Organization & People

The basic components of the "assets of the organization" include its business processes, information, and reputation. These are described in Table 11. For the "assets of the people", the basic components include: the people themselves; and their individual information as described in Table 12.

Table 11: Organization Assets (AO)

Type of asset	Asset ID	Asset Description
Business processes	AO (1)	Essential processes.
		Secret processes
		Processes involving proprietary technology
		Processes concerned with regulatory & contractual issues.
		Support processes
Information	AO (2)	Organization information.
		Essential management information
		Information concerned with regulatory & contractual issues.
		Information associated with external support organizations
		Information associated with cloud customer organizations
Reputation	AO (3)	The internal reputation of the organization
		The external reputation of the organization

Table 12: People Assets (AP)

Type of asset	Asset ID	Asset Description
Business processes	AO (1)	Essential processes.
		Secret processes
		Processes involving proprietary technology
		Processes concerned with regulatory & contractual issues.
		Support processes
Information	AO (2)	Organization information.
		Essential management information
		Information concerned with regulatory & contractual issues.
		Information associated with external support organizations
		Information associated with cloud customer organizations
Reputation	AO (3)	The internal reputation of the organization
		The external reputation of the organization

The threats associated with the organization and with the people include unauthorized "access" to the cloud services and information, which threatens the "confidentiality (C)" of information and the "reputation (R)" of the organization. These threats also include unauthorized "action" to the cloud services and information, which threatens the "integrity (I)" of information and the "safety (S)"

and "reputation (R)" of the organization as a whole. Both types of threats may be caused by "malicious actions (M)" and "vulnerabilities (V)". Further details are given in Table 13.

The "protection controls" concerned with the "organization and people" have three main types: management "regulations"; "awareness and training", and "user practices". Each of these types would be related to: the "rules" associated with it; the "immunity" tools concerned; "password" issues; use of "email"; use of "networks"; use of "data"; use of "encryption"; and of course, "use of the given services". These protection controls would contribute to all performance measures (C), (I), (A), (R), and (S) described in Table 14.

Table 13: Threats related to Organization & People (TOP)

Type of threat	Threat		Source	Eff.
	ID	Description		
Unauthorized access: Account penetration	TOP (1)	Access to IaaS	MV	(C) (R)
	TOP (2)	Access to PaaS		
	TOP (3)	Access to SaaS		
Unauthorized action: Account hijacking	TOP (4)	Action against IaaS	MV	(I) (S) (R)
	TOP (5)	Action against PaaS		
	TOP (6)	Action against SaaS		

Table 14: Protection concerned with Organization & People (POP)

Type of control	Protection controls		Eff.
	ID	Description	
Management regulations	POP (1)	General security rules	(C) (I) (A) (R) (S)
		Immunity tools management	
		Password rules	
		Use of email	
		Use of networks	
		Use of data	
		Use of encryption	
		Use of given services	
Awareness & training	POP (2)	General security rules	
		Immunity tools management	
		Password rules	
		Use of email	
		Use of networks	
		Use of data	
		Use of encryption	
		Use of given services	
Use practices	POP (3)	Immunity tools management	
		Password rules	
		Use of email	
		Use of networks	
		Use of data	
		Use of encryption	
		Use of given services	
		Immunity tools management	

3.4 The Environment

The "assets" associated with the environment can be viewed as the "premises" of the cloud, where the needed cloud "utilities" enabling its operation. As shown in Table 15, the premises would include the surrounding zone, the buildings, and the essential support facilities and services. The utilities would include electricity, air conditioning, cooling system, water supply, waste system, and other utilities.

The threats associated with the environment would have three main types. The first is the "destructive events" that may result from "malicious (M)", "accidental (A)" and "environmental (E)" events, leading to "availability (A)", "reputation (R)", and "safety (S)" problems. The second is "natural events" that result from the "environment (E)", leading to the same problems. The third is "radiation disturbances" that result from the "environment (E)", or from malicious "action (M)", leading also to the same problems. Table 16 provides further elaborations on these threats.

The "protection controls" concerned with the "environment" have four main types: "physical" guarding of the premises, protection from "destructive events", protection from "natural events", and protection from "ra-

Table 15: Environment Assets (AE)

Type of asset	Asset	
	ID	Description
Premises	AE (1)	Surrounding zone
		Buildings
		Essential support facilities & services
Utilities	AE (2)	Electricity
		Air-conditioning
		Cooling system
		Water supply
		Waste system
		Other utilities

Table 16: Threats related to the Environment (TE)

Type of threat	Threat ID	Threat Description	Source	Eff.
Destructive events	TE (1)	Events like: fire; failure of electricity or other utilities	MAE	(A) (R) (S)
Natural events	TE (2)	Destruction due to environmental causes like: flood; volcano; climatic phenomenon	E	
Radiation disturbance	TE (3)	Electromagnetic radiation problems	ME	
		Thermal radiation problems.		

diation disturbances". These controls would contribute to all performance measures: "(C), (I), (A), (R), and (S)". Protection from destructive, natural, and radiation disturbances events include the protection of: people, premises and utilities, in addition to all components associated with the cloud operation. These protection controls are given in Table 17.

Table 17: Protection concerned with Environment (PE)

Type of control	Protection controls ID	Protection controls Description	Eff.
Physical Protection	PE (1)	Guarding premises	(C) (I) (A) (R) (S)
Protection from destructive events	PE (2)	People	
		Premises & utilities	
		Hardware	
		IaaS Virtualization components	
		PaaS Components	
		SaaS Components	
Protection from natural events	PE (3)	People	
		Premises & utilities	
		Hardware	
		IaaS Virtualization components	
		PaaS Components	
		SaaS Components	
Protection from radiation disturbance	PE (4)	People	
		Premises & utilities	
		Hardware	
		IaaS Virtualization components	
		PaaS Components	
		SaaS Components	

4 Discussion, Conclusions & Future Work

This paper contributes to the initial stage of ISRM process for cloud computing, which is essential to all other stages of the ISRM process. It has developed a context establishment management framework based on the structure of the STOPE view. The framework derives its cloud ISRM requirements from key recent literature, including: literature developed by specialized standards organizations, and research papers published in refereed journals. The framework has two main benefits.

- It gives a comprehensive view of the targeted context enabling it to accommodate the various issues concerned with ISRM for cloud computing.

- It provides the comprehensive context with a well-organized modular construction that enables its flexible use and management by the subsequent stages of the ISRM process.

The framework is of generic nature; and it is open to different practical cloud computing context establishment cases for ISRM. It should be noted here that while full comprehensiveness for various cases is a remote target, due to the continuous development of information technology and cloud computing, the framework remains a useful dynamic tool to start ISRM process and accommodates its basic requirements, with openness to continued extensions that meet the developing requirements. This dynamism of application is supported by the clear modularity of the STOPE view of the framework.

Future work based on the framework may be associated with the following three main extensions.

- The first would be concerned with implementing the framework on the computer. This will ease establishing a structured ISRM context for various cloud case-studies; and will also enable tailoring the context to their requirements.

- The second would consider developing the above software further, following the subsequent stages of cloud ISRM process. These stages usually include: assessing the risks of the threats on the assets; considering suitable protection controls and assessing their effectiveness and efficiency; and choosing suitable controls per certain acceptable criteria. In this respect comes the idea of viewing the controls as preventive, detective or corrective, and considering them with specific priorities per their performance.

- The third would be concerned with using the outcome of the above two extensions to investigate ISRM for various clouds. This would enable building experience, and support updating and upgrading all the above.

It is hoped that both researchers and professionals in the field would make use of the framework, develop it further according to their practical requirements, and benefit from its features for better and more secure clouds in the future.

Acknowledgement

The authors thank the Deanship of Scientific Research and RSSU at King Saud University for their technical support.

References

[1] M. Ahmed, A. T. Litchfield, S. Ahmed, "A generalized threat taxonomy for cloud computing," in *25th Australasian Conference on Information Systems*, Auckland, New Zealand, 2014.

[2] A. A. AlHogail, *A Framework for the Analysis and Implementation of an Effective Information Security Culture Based on Key Human Factor Elements and Change Management Principles*, King Saud University, MSc dissertation, 2016.

[3] M. Alnuem, H. Alrumaih, H. Al-Alshaikh, "A comparison study of information security risk management frameworks in cloud computing," in *The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 103–109, 2015.

[4] M. Almorsy, J. Grundy, A. S. Ibrahim, "Collaboration-based cloud computing security management framework," in *IEEE International Conference on Cloud Computing (CLOUD'11)*, pp. 364-371, 2011.

[5] K. I. Al-Osaimi, A. Alheraish, and S. H. Bakry, "An integrated STOPE framework for e-readiness assessments," in *18th National Computer Conference, Saudi Computer Journal*, pp. 23–36, 2006.

[6] K. I. Al-Osaimi, *Mathematical Models for E-Readiness Assessment of Organizations with Intranets*, King Saud University, Unpublished Magister Thesis, 2007.

[7] K. I. Al-Osaimi, A. Alheraish, and S. H. Bakry, "STOPE-based approach for e-readiness assessment case studies," *International Journal of Network Management*, vol. 18, no. 1, pp. 65–75, 2008.

[8] A. A. A.Alrabiah, *Risk Analysis for the Development of Security-Readiness Indicators for Intranets*, King Saud University , Master thesis, 2007.

[9] M. A. Arafah, H. S. Al-Harbi, S. H. Bakry, "Grid computing: a STOPE view," *International Journal of Network Management*, vol. 17, no. 4, pp. 295–305, 2007.

[10] S. H. Bakry, "Development of e?government: A STOPE view," *International Journal of Network Management*, vol. 14, no. 5, pp. 339–350, 2004.

[11] A. H. Bakry, S. H. Bakry, "Enterprise resource planning: A review and a STOPE view," *International Journal of Network Management*, vol. 15, no. 5, pp. 363–370, 2005.

[12] R. Bojanc, B. Jerman-Blažič, "A quantitative model for information-security risk management," *Engineering Management Journal*, vol. 25, no. 2, pp. 25–37, 2013.

[13] Y. Chen, V. Paxson, R. H. Katz, *What's New About Cloud Computing Security*, University of California, Berkeley Report No. UCB/EECS-2010-5 Jan. 20, 2010.

[14] T. S. Chou, "Security threats on cloud computing vulnerabilities," *International Journal of Computer Science & Information Technology*, vol. 5, no. 3, p. 79, 2013.

[15] CSA, *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0*, Cloud Security Alliance, 2011. (`http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf`)

[16] CSA, *Cloud Controls Matrix*, Cloud Security Alliance, 2016. (`https://cloudsecurityalliance.org/group/cloud-controls-matrix/`)

[17] CSA, *The Treacherous 12, Cloud Computing Top Threats in 2016*, Cloud Security Alliance, 2016. (`https://cloudsecurityalliance.org/group/top-threats/`)

[18] K. Djemame, D. Armstrong, J. Guitart, and M. Macias, "A risk assessment framework for cloud computing," *IEEE Transactions on Cloud Computing*, vol. 1, p. 1-1, 2016.

[19] ISO, *International Standards Organization: ISO/IEC 27017:2015, Information Technology: Security Techniques - Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services*, 2015. (`https://www.iso.org/standard/43757.html`)

[20] ISO, *International Standards Organization: ISO/IEC 17788:2014, Information Technology: Cloud Computing - Overview and Vocabulary*, 2014. (`https://www.iso.org/standard/60544.html`)

[21] ISO, *International Standards Organization: ISO/IEC 27002:2013, Information Technology: Security Techniques - Code of Practice for Information Security Controls*, 2013. (`https://www.iso.org/standard/54533.html`)

[22] ISO, *International Standards Organization: ISO/IEC 27005:2011, Information Technology: Security Techniques - Information Security Risk Management*, 2011. (`https://www.iso.org/standard/56742.html`)

[23] ISO, *International Standards Organization: ISO 31000:2009, Risk Management: Principles and Guidelines*, 2009. (`https://www.iso.org/standard/43170.html`)

[24] ITU, *International Telecommunication Union, Focus Group on Cloud Computing*, Technical Report. Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements, 2012. (`https://www.itu.int/pub/T-FG-CLOUD-2012-P1/en`)

[25] ITU, *International Telecommunication Union, Focus Group on Cloud Computing*, Technical Report. Part 2: Functional requirements and reference architecture, 2012. (https://www.itu.int/pub/T-FG-CLOUD-2012-P2/en)

[26] I. Kateeb, M. Almadallah, "Risk management framework in cloud computing security in business and organizations," in *Proceedings of the 2014 IAJC/ISAM Joint International Conference*, 2014.

[27] A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security risks and their management in cloud computing," in *4th International Conference on Cloud Computing Technology and Science*, IEEE, pp. 121–128, 2012.

[28] P. Mell, and T. Grance, *National Institute of Standards and Technology, U.S. Department of Commerce, The NIST Definition of Cloud Computing*, Special Publication 800-145, 2011.

[29] F. Muhaya, S. H. Bakry, "An approach for the development of national information security policies," *International Journal of Advanced Science and Technology*, vol. 21, pp. 1–10, 2010.

[30] NIST 500-299, *National Institute of Standards and Technology, U.S. Department of Commerce, NIST Cloud Computing Security Reference Architecture*, 2013. (https://csrc.nist.gov/publications/detail/sp/500-299/draft)

[31] NIST 800 - 30, *National Institute of Standards and Technology, U.S. Department of Commerce, Information Security: Guide for Conducting Risk Assessments*, 2012. (https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)

[32] NIST 800 - 37, *National Institute of Standards and Technology, U.S. Department of Commerce, Information Security: Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, 2010. (https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final)

[33] M. S. Saleh, A. Alrabiah, and S. H. Bakry, *E-Business Diffusion Requirements: A STOPE View for Easing the Use of ISO 17799 Information Security Management Standard, Organization*, 6, pp. 16, 2005.

[34] M. S. Saleh, A. Alrabiah, and S. H. Bakry, "A STOPE model for the investigation of compliance with ISO 17799-2005," *Information Management & Computer Security*, vol. 15, no. 4, pp. 283–294, 2007.

[35] M. S. Saleh, A. Alrabiah, and S. H. Bakry, "Using ISO 17799: 2005 information security management: A STOPE view with six sigma approach," *International Journal of Network Management*, vol. 17, no. 1, pp. 85–97, 2007.

[36] M. S. Saleh, and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," *Applied Computing and Informatics*, vol. 9, no. 2, pp. 107–118, 2011.

[37] M. S. Saleh, *Analysis of Information Security Risks and Protection Management Requirements for Enterprise Networks*, University of Bradford, Doctoral dissertation, 2012.

[38] P. Saripalli, and B. Walters, "Quirc: A quantitative impact and risk assessment framework for cloud security," in *IEEE 3rd International Conference on Cloud Computing*, pp. 280–288, 2010.

[39] H. Susanto, F. Muhaya, M. N. Almunawar, "Refinement of strategy and technology domains STOPE view on ISO 27001," in *International Conference on Intelligent Computing and Control (ICOICC'10)*. Archieved by Cornell University Library, 2010.

[40] H. Takabi, J. B. Joshi, and G. J. Ahn, "SecureCloud: Towards a comprehensive security framework for cloud computing environments," in *34th Annual Computer Software and Applications Conference Workshops (COMPSACW'10)*, IEEE, pp. 393–398, 2010.

[41] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, A. Kanai, "Risk management on the security problem in cloud computing," in *First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI'11)*, IEEE, pp. 147–152, 2011.

[42] F. Xie, Y. Peng, W. Zhao, D. Chen, X. Wang, X. Huo, "A risk management framework for cloud computing," in *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, vol. 1, pp. 476–480, 2012.

[43] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments," in *IEEE 10th International Conference on Computer and Information Technology (CIT'10)*, pp. 1328–1334, 2010.

Biography

Bader Saeed Alghamdi received his B.Sc. degree in electrical engineering, electronics and telecommunications department, from Kind Saud University, Saudi Arabia in 2008. He is currently a project coordinator for telecommunications and information security projects. His current area of research interest includes information security risk management, risk assessment techniques, and cloud computing deployment.

Mohamed Elnamaky received his B.Sc. degree from Tanta University, School of Electrical Engineering, Egypt He also received the M.Sc. degree in Electronics and Telecommunication Engineering from Ajou University, South Korea. He joined King Saud University as researcher in 2009. His main areas of research interest are ASIC/FPGA modeling and simulation for wireless algorithms, Channel Estimation and Detection for mobile communications and MIMO network design.

Mohammed Amer Arafah was born in Saudi Arabia in 1965. He received the B.Sc. degree in Computer

Engineering from King Saud University, Riyadh, Saudi Arabia, and the M.Sc. and Ph.D. degrees in Computer Engineering from University of Southern California, Los Angeles, USA. He joined King Saud University as assistant professor in 1997. His main areas of research interest are computer networks modeling and simulation, wireless sensor networks, cooperative relay networks, fault tolerance, and high-speed networks.

Maazen Alsabaan received the B.Sc. degree in the electrical engineering, from King Saud University, Saudi Arabia, in 2004, the M.A.Sc. and Ph.D. degrees in Electrical and Computer Engineering from University of Waterloo, Canada, in 2007 and 2013, respectively. He is currently an Assistant Professor in the Department of Computer Engineering, King Saud University, Saudi Arabia. His current research interests include information security, vehicular networks, green communications, and intelligent transportation systems.

Saad Haj Bakry is Professor in the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, where he has been working since 1980. His main areas of research include: information networks, and knowledge society policies, including information security policies. In addition to his academic work, he provided consultations to various public and private sector organizations in Saudi Arabia including: King Abdulaziz City for Science and Technology; Commission of Information and Communication Technology; E-Government Program; and others.