



Secure migration to compliant cloud services: A case study

Fahad F. Alruwaili^{a,1,*}, T. Aaron Gulliver^b

^a College of Computing and Information Technology, Shaqra University, P.O. Box 33, Shaqra 11961 Saudi Arabia

^b Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 1700, STN CSC, Victoria, BC V8W 2Y2 Canada

ARTICLE INFO

Article history:

Available online 7 December 2017

Keywords:

Readiness assessment
Maturity level
Information security
Privacy
Compliance
Cloud computing
Service provider
Financial payment systems

ABSTRACT

Adoption of cloud computing technology in the financial sector is increasing to improve the efficiency of payment transactions, risk management, and business processes. This is occurring more rapidly in developed countries such as USA, Canada, and the UK while cloud implementation in less developed countries such as Saudi Arabia is still emerging. Implementation of cloud technologies in the financial sector requires diligent decisions such as selecting the most suitable secure cloud deployment model, service level agreement, and cloud vendor. In this paper, cloud migration using an information security, privacy, and compliance (ISPC) readiness model is presented. Several types of cloud services are available, therefore evaluating migration readiness and selecting an appropriate vendor is critical, as this will have an impact on the requirements of stakeholders such as local banks. Cloud migration decisions are obtained by analyzing ISPC requirements considering the strategic initiatives of the organization. A case study involving the Saudi Arabian central bank is presented to demonstrate the implementation of the ISPC readiness model.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

With the rapid evolution of the internet and data processing and storage capabilities, cloud computing has become a viable business model and computing paradigm. Cloud services enable powerful, scalable, cost-effective, on-demand, and efficient computing resources [1]. A variety of cloud computing service models such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) form the core cloud computing technologies. These service models are supported by different deployment models, i.e. public, private, community, and hybrid [2]. The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [3]. Further, cloud models are considered to have five essential characteristics, three service models, and four deployment models with different attributes compared to grid and distributed computing [4]. These attributes are described in Table 1. In addition, new

service models are being developed such as storage as a service (STaaS), security and data protection as a service (SDPaaS), and security operations center as a service (SOCaaS) [5].

Many organizations are considering moving some or all of their information technology (IT) capabilities to the cloud due to the advantages of cloud systems. However, migration decisions are not easily made and can require significant time, resources, and personnel to assess the feasibility and readiness of an organization to make such a move [6]. This assessment considers decisions such as the selection of suitable cloud services and deployment models. If sensitive and business critical information are involved, a careful migration analysis must be conducted to identify the risks and benefits of cloud services [7].

The rapid growth in financial industry services and payment solutions require greater agility to adopt and implement changes [8]. Cloud computing services enable organizations to quickly respond to new business requirements and can be applied to financial applications and systems [8]. In this paper, information security, privacy, and compliance (ISPC) requirements are examined via a case study of the readiness and feasibility of the Saudi Arabian central bank migrating to cloud services. The organizational and operational challenges are analyzed using the four main components of the ISPC model, i.e. cubic model, control assessment, cloud feasibility analysis, and readiness for migration. The focus is on the ISPC requirements that personnel should consider in the migration of payment systems to the cloud. In addition, commercial cloud solutions are investigated and considered in

* Corresponding author.

E-mail addresses: alruwaili@su.edu.sa (F.F. Alruwaili), agullive@uvic.ca (T.A. Gulliver).

¹ The research of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia.

Table 1
Cloud deployment and service models.

Cloud Deployment Models	Private	The cloud services are exclusively provisioned to a single organization. These services are managed by the organization or delegated to a third party.
	Community	The cloud services are provided to and shared by multiple organizations who have agreed to share similar concerns, e.g. mission, policy, security requirements, and compliance.
	Public	The cloud services are provided for public use so that multiple organizations can share cloud resources using a multi-tenancy model.
	Hybrid	The cloud services are provided as a combination of two or more of the above deployment models. These models retain their unique attributes but are bound together by standardized or proprietary technology.
Cloud Service Models	Infrastructure as a Service (IaaS)	Cloud service provider provisioning of processing instances, storage, network, and other computing infrastructure resources.
	Platform as a Service (PaaS)	Cloud service provider provisioning of middleware, programming tools, operating systems, and other tools.
	Software as a Service (SaaS)	Cloud service provider provisioning of their deployed cloud applications.

the migration assessment. These solutions are (1) threat intelligence, i.e. evidence-based knowledge including threat indicators, implications, and actionable advice about existing and emerging cyber security threats, and (2) eLearning systems, i.e. a system that administrates, documents, distributes, tracks, monitors, and reports user awareness assessments.

2. Related Work

Computing security is a major concern of organizations and government agencies considering migrating IT resources, e.g. email services, business process management, threat intelligence, security operations, training and awareness, and applications, to the cloud [9]. Migrating to the cloud can provide benefits such as flexibility and scalable on-demand IT services [10]. Further, the cost of IT operations and maintenance can be significantly reduced. However, there are few case studies that investigate the migration of IT capabilities to the cloud [11]. Moreover, the implications of cloud services from an enterprise and business perspective have not been well understood [12].

In [13], several potential benefits in moving to the cloud were identified. These benefits were viewed from a managerial perspective such as improved employee and customer satisfaction, opportunities to develop new applications, and reduced operational costs. Understanding these benefits and their associated risks are far from straightforward, so a conceptual framework was introduced to assist organizations in determining the cost, suitability, and impact of adopting cloud services. However, the challenges of cloud security and privacy were not addressed, and these have a significant influence on cloud migration [14]. Many security experts believe that organizations hosting their data and applications on the internet and/or public cloud are vulnerable to threats and cybercrime [15]. Therefore, examining the potential benefits and drawbacks of cloud services and assessing organizational readiness is a goal of this paper.

In [16], a forensic readiness model based on cloud capabilities was presented. This model allows cloud service providers to manage and deliver the data needed for digital forensic investigations. These investigations are important components of information security programs and incident response activities. A number of techniques have been designed for readiness assessment, such as the tools and models described in the WEF 2009–2010 global information technology report [17] and the Waseda University world e-government ranking [18]. However, these approaches are limited to evaluating the readiness of data for forensic analysis. A comprehensive approach is needed to address security and privacy concerns and the compliance status of cloud services.

In [33], the critical security factors that affect Saudi Arabia government agencies deciding to adopt cloud technology were examined. A framework was constructed to investigate cloud security

risks and features and analyze their influence on cloud adoption. However, this framework can only identify and confirm, via expert review, the factors that are significant to the implementation of cloud services. In [34], a similar framework was presented to identify and analyze the influence of a set of key critical success factors (CSFs) to the migration of Saudi Arabia universities to the cloud. Nevertheless, readiness assessment for migration was not considered and security and success factors were only investigated for the educational services sector which differs significantly from the financial industry. Hence the focus of this paper is on the financial sector.

A survey was conducted with 147 members of healthcare organizations from Malaysia, Saudi Arabia, and Pakistan to assess their confidence in secure cloud healthcare services as an emergent technology [35]. The results indicated that there is a direct relationship with the years of experience of the respondents to cloud security and privacy. This influences user decision to implement cloud-based healthcare systems. The results of a survey of four Saudi organizations was presented in [36] to determine the critical factors affecting cloud services adoption. It was found that 95% of the 169 respondents indicated that security is a critical factor impacting their cloud use decisions.

The study in [37] explored the impact and security significance of 70 public domains and cloud platforms in Saudi Arabia. The focus was on the application layer to ensure security safeguards throughout the entire software development life cycle (SDLC). While such work is effective in addressing application layer security issues, it cannot provide a holistic approach to assess the adoption of cloud services for payment systems, which is the subject of this work.

In [19], an ISPC readiness model was proposed to facilitate making decisions related to ISPC requirements. This model allows organizations to assess cloud risks based on the probability of threats occurring and their potential impact prior to and after migration. Both technical and non-technical issues were considered, i.e. payment technology, processes and procedures, and personnel awareness and readiness for cloud migration. In the case study presented here, an implementation of the ISPC readiness model and ISPC cubic controls [20] is used to evaluate migration readiness and the decision-making process.

3. Case Study

A case study was conducted to examine the feasibility of cloud service implementation in the financial industry. The Saudi Arabia central bank governs all electronic bill payment transactions in the region. It is dedicated to streamlining electronic billing and payment systems operations while employing the highest information security standards and risk management principles. The agency currently employs a system developed in-house for

executing payment transactions in accordance with policy requirements. While current system performance is adequate, there is an increasing need to provide customers with better real-time access and mobility. This initiative will enable the agency to develop new revenue streams and improve the efficiency of the payment system. Further, it will reduce costs and improve management and operational control over financial transactions and reporting.

Personnel in the agency department of payment systems (DPS) and senior management knowledgeable of cloud computing service models and the associated risks were interviewed. This revealed many security, privacy, and compliance issues that should be addressed in the cloud migration plan. For simplicity, only the most important factors behind these issues are considered in this study.

This case study employs the cloud security concepts presented in [19,20,22], to address actual ISPC concerns associated with migrating a financial payment system to the cloud. The methodology adopted and research motivation will first be presented, followed by the analysis of ISPC readiness for informed decision making. This is based on recent experience with the Saudi Arabia central bank and its ISPC readiness assessment. Further, the implementation and evaluation of commercial cloud security services, i.e. threat intelligence and phishing awareness services, are considered. For clarity, only critical controls in the ISPC readiness model are discussed.

3.1. Overview of the financial agency

The Saudi Arabia central bank monitors and regulates all payment transactions in the country. It has been in existence for more than a decade regulating and monitoring payment transactions through multiple electronic payment systems such as real-time settlement, bank transactions, and point-of-sale (POS). The DPS is housed in three buildings and has approximately 530 personnel in diverse areas such as marketing, customer support, project management, application development, operations, information security, and risk management. The agency has developed three distinct payment products. The first handles payment transactions and settlements to process, monitor and regulate payments between government agencies and local banks. The second promotes cashless payments by increasing the number of POS locations. It also connects all ATMs nationwide with local and international banks and billers. The third product enables online payments between customers and billers, e.g. government agencies, transportation services, and educational, financial and insurance institutions.

The DPS systems are operated and supported by the financial agency. These systems consist of a complex collection of network architectures, servers, and desktop computers with dedicated wide area network (WAN) connections and high-speed internet connectivity. The agency has made a significant investment to establish the three payment products by procuring the necessary consultants and engineers, hardware, and software.

3.2. The existing DPS

The three payment systems were developed nearly twenty years ago and require significant ongoing investments in software and hardware upgrades and maintenance. Increasing costs have made it difficult to stay within budget so that now the continuity and maintenance of these systems is a concern. For example, peak demand during month end payroll and special events, e.g. national holidays, results in system utilization near 70%, which is a critical level considering system scalability and performance. Further, there is an urgent need to redevelop the first payment system due to compatibility issues. This has been identified as a barrier to the strategic move to a unified and integrated payment system.

3.3. DPS challenges

DPS personnel are contemplating adopting cloud computing technology to reduce costs, minimize risks, improve the delivery and quality of payment systems, and address current problems. Newer technologies such as cloud services are cost effective due to their on-demand availability and pay-per-use services. Cloud services have other advantages such as scalability and accessibility from anywhere using any computing device. In addition, physical infrastructure including data center facilities, cabling, and servers can be eliminated or reduced significantly. However, while there are many benefits there are also challenges including the selection of a secure cloud deployment model.

As stated previously, cloud computing services can be categorized as one of three deployment models which differ in terms of purpose, complexity, capabilities, and costs [24]. For example, a private deployment model is appropriate when the goal is to maximize and/or optimize the use of existing in-house resources, improve data privacy, and reduce costs [25]. A public deployment model is more suitable if remote access to non-sensitive tools, e.g. advanced learning tools, must be provided in a cost-effective manner [26]. DPS personnel have determined that the chosen strategy should consider the system architecture separately from other criteria such as mission, availability, and applications, as well as data criticality, sensitivity, confidentiality, integrity, privacy, and availability. Further, consultants have been employed to assess migration readiness and assist in the decision-making process. Based on these results, the following decision controls have been identified.

- **Organization Mission and Vision:** The DPS tends to be reactive to information security and privacy incidents instead of being predictive or even proactive. DPS personnel agree that clear objectives are essential in adopting and implementing an effective information security program [23]. Further, if the mission is not adequately defined, an organization will have difficulty securing its information and enforcing ISPC policies [27]. Therefore, the business and operations processes should be strategically aligned for cloud migration.
- **Confidentiality:** A key concern when considering the adoption of cloud technology is confidentiality. DPS personnel require effective end-to-end confidentiality measures without any degradation in service functionality. As the cloud services will be executing payment systems, data encryption is essential. This includes ensuring that all payment transactions are initiated by trusted parties. Further, financial messages between parties and authentication and user information should be encrypted. Confidentiality depends on the following six essential controls.
 - *Antivirus:* There should be an online and up to date antivirus monitoring system to prevent virus and malware attacks.
 - *Authentication:* All data should be protected from unauthenticated users, and proper authentication mechanisms should be in place.
 - *Backup:* At regular intervals, online backups should be conducted to prevent data loss. DPS policy requires a reliable backup mechanism, e.g. full backups, daily incremental backups, and real-time backups.
 - *Disaster recovery:* A recovery system should be in place in case of data corruption.
 - *Encryption:* Data encryption should be employed to protect the data.
 - *Updates:* All applications should have automatic updating.
- **Integrity:** A critical component of information security is implementing controls to ensure data accuracy and consistency. It is required that integrity controls are implemented and continuously monitored across all payment systems. Therefore, a cloud service provider must provide adequate data integrity

controls such as continuous monitoring and secure hash functions, e.g. a hash-based message authentication code (HMAC) with secure hash algorithm 1 (SHA-1).

- **Availability:** It is essential that payment services always be available [28]. Thus, the cloud services should be available and accessible by all stakeholders 24/7/365, i.e. customers, banks, and billers. This is critical during peak load periods such as when monthly payroll transactions are executed. DPS personnel believe that current availability issues, e.g. downtime and lack of technical and customer support, can be resolved by adopting cloud technology.
- **Training, Awareness, and Education:** To deal with changes in cloud services and security, continuous training, awareness and education programs for DPS personnel must be provided. It is well-known that personnel are the greatest security threat with many incidents originating within the organization [29]. Thus, ongoing education and training programs are essential to achieving information security, privacy, and compliance program targets.
- **Management Support:** Senior DPS personnel are typically not information security experts. Thus, they must be provided with appropriate security awareness training to understand the importance and criticality of ISPC. This will ensure proper support and resources for secure cloud migration.
- **Information Security, Privacy, and Compliance Policy:** The creation of an information security policy is a key step in determining the required direction and support for secure cloud migration. This policy identifies the critical assets of the payment systems and determines the control objectives and practices, e.g. the acceptable use of cloud services to maintain security, privacy, and compliance. In addition, information security incident management is required to enforce compliance, protection, and recovery from malicious activities.

In the existing DPS systems, some networks are physically segregated from the internet to minimize cyber threats. However, this incurs additional expenses such as maintaining an isolated data center, cabling, communication lines, networking components, servers and workstations, licensing, and maintenance contracts. As a consequence, the services and infrastructure are not fully utilized as there are many situations when the equipment and personnel are idle, i.e. after business hours and during weekends. This

is inefficient and costly, so DPS personnel are considering migrating these systems to the cloud. There are issues associated with ISPC requirements, for example, violations of these requirements in a public cloud are more likely than with a private cloud, but the use of cloud technologies can provide significant cost savings.

Due to the complexity of the security issues, it is difficult for DPS personnel to make a decision regarding the most appropriate secure cloud deployment model for the payment systems. Consequently, a detailed list of ISPC controls based on the approaches in [19,20,22] was developed and used to assess the readiness for migrating to a secure cloud model. A summary of the main ISPC controls is presented in Table 2.

3.4. Research motivation and methodology

In Saudi Arabia, cloud computing services is in its infancy stage and is not been widely adopted [33]. A key challenge to migrating IT systems to the cloud and to its acceptance and success is the social and technological security risks [33–35]. Therefore, a comprehensive approach to address the cloud information security, compliance, and risk management concerns of DPS is presented in this paper. This includes payment systems and their security programs such as security awareness and cyber security threat awareness and intelligence.

Further, this case study examines the issues surrounding the migration of payment system to the cloud [30] and considers how DPS personnel select and implement a secure, private, and compliant cloud service, and which vendor should be chosen [31]. This will improve the readiness and success for secure migration of central bank systems and similar financial services to the cloud.

4. Readiness assessment and decision methodology

In this study, the ISPC readiness model in [19] is used to provide a detailed analysis in order to select the most appropriate cloud environment. This model provides guidelines for evaluating the readiness of the agency to migrate to a secure, private, and compliant cloud technology. Further, the required steps are given to select an appropriate cloud deployment model. These are used by the agency to make an informed decision on the suitability of cloud technology for their payment systems. In particular, the ISPC

Table 2
Summary of the Information Security, Privacy, and Compliance Controls.

	ID	Control Family	Sub ID	Sub Control	Example
Non-Technical Measures (Strategies, Policies, Plans, Procedures, and Guidelines)	OMV	Department of Payment Systems (DPS) Objectives, Mission, and Vision	ISS	<i>Information Security Strategy</i>	The development of long-term, e.g. 3-5 year, security objectives aligned with the agency business objectives. These objectives are based on a cloud ISPC readiness assessment.
			ISMF	<i>Information Security Risk Management Framework</i>	Aligned with the agency enterprise-wide framework, formal risk assessments shall be performed at planned intervals (at least annually), to determine the likelihood and impact of all identified cloud risks.
			ISG	<i>Information Security Governance</i>	The DPS leadership shall review the information security policy at planned intervals or as a result of agency changes to ensure continuing alignment with the cloud security strategy, effectiveness, accuracy, relevance, and applicability to ISPC requirements or regulatory compliance obligations.
			ISC	<i>Information Security Compliance</i>	Cloud auditing activities and plans focusing on payment data, systems access, and data boundary limitations shall be designed to minimize the risk of payment system disruption. Audit activities must be planned and agreed upon in advance by cloud

(continued on next page)

Table 2
(continued)

ID	Control Family	Sub ID	Sub Control	Example
ISPC	Information Security, Privacy, and Compliance Policy			stakeholders, i.e. the agency, customers, banks, and cloud service provider.
		MS	<i>Management Support</i>	The agency senior and line management shall take formal actions to support cloud migration and operations of payment systems through clearly-documented directions and commitments, and ensure that these actions are assigned.
		NS	<i>Network Security Policy</i>	Cloud network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted agency connections. This must be reviewed at regular intervals, and supported by documented business justification for the use of all services, protocols, and ports allowed. Network architecture diagrams must also clearly identify risks and data flows that may have an impact on legal, statutory, and regulatory compliance.
		AS	<i>Application Security Policy</i>	Payment applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with ISPC requirements and accepted industry standards, e.g. OWASP for web applications.
		SS	<i>Server Security Policy</i>	Secure and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, a network segregated from production-level networks will be used for this migration.
		AU	<i>Acceptable Use Policy</i>	DPS policies and procedures shall be established, and supporting payment processes and technical ISPC measures implemented, for defining allowances and conditions for permitting access to agency-owned or managed user end-point devices, e.g. desktops, laptops, and mobile devices.
		ESP	<i>Email Security Policy</i>	In addition to the AU policy above, a detailed email security policy shall be created to enforce cloud email Phishing and SPAM protection. Sensitive emails must always be encrypted. Email archiving must also be checked and reviewed with the cloud service provider.
		PPP	<i>Password Protection Policy</i>	Password policies applicable to DPS systems shall be documented and enforced through ISPC technical controls on all agency devices or devices approved for mobile use, and shall prohibit any changes in password/PIN lengths and authentication requirements.
		PCI	<i>PCI DSS Compliance Policy</i>	The agency must adhere to the minimum mandatory PCI DSS requirements that need to be applied to all DPS and cloud service provider personnel, and other stakeholders tasked with handling credit and debit cards, credit and debit card data, and processing systems and services.
		BCP	<i>Contingency, Business Continuity, and Disaster Recovery Planning Policy</i>	The DPS shall establish a consistent and unified framework for business continuity and disaster recovery planning. All business and payment continuity plans must be consistent with the priorities for DPS payment system testing, maintenance, and ISPC requirements.
		TAP	<i>Training and Awareness Policy</i>	A security awareness training program shall be established for all agency employees, contractors, and

(continued on next page)

Table 2
(continued)

	ID	Control Family	Sub ID	Sub Control	Example
Technical Measures					third-party users, and mandated as appropriate. All individuals with access to the agency payment systems and payment data shall receive appropriate awareness training and regular updates on the agency ISPC procedures, processes, and policies related to their positions.
	C	Confidentiality	CC	<i>Cryptography Controls</i>	Cloud service providers shall demonstrate compliance with confidentiality requirements. For instance, preserving restrictions on access and disclosure for DPS systems in the cloud. Further, DPS system classification should be implemented and monitored at regular intervals.
			ISC	<i>Information Sharing Controls</i>	The DPS should enable information sharing for decision support. Controls must be in place to enable access only by authorized DPS users.
			ISRC	<i>Information in a Shared Resource Controls</i>	The cloud multi-tenant agency owned or managed (physical and virtual) applications, and infrastructure and network components, shall be designed, developed, deployed and configured such that cloud service provider user access is appropriately segmented from other tenant users, based on the following considerations: <ul style="list-style-type: none"> • established resource sharing policies and procedures, and • isolation of DPS critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance.
			TMAC	<i>Transmission Medium Access Controls</i>	The DPS and cloud service provider must implement access control management between the DPS, cloud service provider and other connected stakeholders such as two-factor authentication, physical security monitoring, and login attempt monitoring.
			TCC	<i>Transmission Confidentiality Controls</i>	Encryption techniques must be used to protect DPS system transmissions, user authentication and other confidential information sent over the internet or other public networks. In addition, the DPS and cloud service provider must apply defense-in-depth techniques (e.g. deep packet analysis, traffic throttling, and packet black-holing), for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns, e.g. MAC spoofing and ARP poisoning attacks and/or denial-of-service (DoS) attacks.
			DLC	<i>Data Leakage Controls</i>	The DPS and cloud service provider shall implement security mechanisms to prevent data leakage, e.g. data encryption, classification, and access log monitoring.
			SSC	<i>Storage Security Controls</i>	The DPS and cloud service provider shall implement restrictive and monitored access controls for offline storage, backup data, systems, and media.
VSC	<i>Virtualization (Hypervisor) Security Controls</i>	Access to all hypervisor management functions or administrative accounts for virtualized DPS system hosting shall be restricted to personnel based on the principle of least privilege and supported through technical controls, e.g. two-factor authentication, audit trails, IP address filtering, and firewalls. Moreover, data exchanged between hypervisor sessions should be classified and protected.			

(continued on next page)

Table 2
(continued)

ID	Control Family	Sub ID	Sub Control	Example	
	I	Integrity	SFIC	Software, Firmware, and Information Integrity Controls	The DPS shall review the cloud service provider cryptographic mechanisms for integrity protection, e.g. use of digital signatures to sign hashes using asymmetric cryptography, protecting the confidentiality of keys used to generate hashes, and use of public keys to verify hash information.
			IIVC	Information Input Validation Controls	The cloud service provider and DPS shall inspect, account for, and correct data quality errors and inherited risks. Checking the valid syntax and semantics of DPS payment system inputs (e.g., character set, length, numerical range, and acceptable values), verifies that inputs match specified definitions for format and content. The DPS should periodically check the cloud service provider prescreening measures for inputs prior to passing them to interpreters to prevent content from being interpreted and modified. DPS and the cloud provider should perform input validation to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and injection attacks.
			CARC	Change and Access Restriction Controls	The DPS and cloud service provider must ensure that changes to the hardware, software, and firmware of the DPS systems and their cloud services are restricted to only authorized individuals and processes. These changes should be permitted only through change management controls.
			TIC	Transmission Integrity Controls	The communication paths outside of or between the DPS, cloud service provider and stakeholder premises are exposed to the possibility of modification. Therefore, the DPS and cloud provider shall apply cryptographic hash functions, e.g. digital signatures, checksums, and message authentication codes. Further, the use of digital signatures must be applied to all traffic for which nonrepudiation is required.
	A	Availability	AAC	Accountability and Auditing Controls	The DPS and cloud service provider must be able to audit DPS system events, time stamps, and records, and provide digital signature receipts for nonrepudiation.
			TAC	Transmission Availability Controls	The communication paths outside of or between the DPS, cloud service provider and stakeholder premises are exposed to the possibility of service interruption. Therefore, the DPS and cloud provider shall develop primary and alternate communications service agreements that contain priority-of-service provisions in accordance with DPS availability requirements (including recovery time objectives).
			RC	Redundancy Controls	The DPS must ensure that the cloud service provider implements adequate redundancy controls across all DPS system levels, e.g. network, server, and capacity. This can reduce the susceptibility to denial of service (DoS) attacks.
			CPMC	Capacity Provisioning and Monitoring Controls	The DPS must ensure that the cloud service provider implements appropriate CPU, memory, hardware, and software resource capacity monitoring to address any future or immediate scalability requirements.
			BRC	Backup and Restoration Controls	The DPS must conduct regular user-level, system-level, and hardware-level backups of all DPS systems hosted

(continued on next page)

Table 2
(continued)

ID	Control Family	Sub ID	Sub Control	Example	
				in the cloud. Restoration backups should also be available when needed.	
		DOSC	Denial of Service (DoS) Controls	The DPS must ensure that the cloud service provider protects against or limits the effects of DoS attacks. In addition, the cloud provider should employ protection devices to filter traffic and be able to increase capacity and bandwidth as per DPS requests.	
	P	Privacy	PIIC	Inventory of Personally Identifiable Information (PII) Controls	The DPS and cloud service provider shall take due care in updating inventories by identifying and linking any PII data, e.g. social security numbers, addresses, and credit card information. To reduce disclosure risks and PII sensitivity, the DPS and cloud service provider, where feasible and within the limits of cloud service provider technology, locate and remove specified PII data and/or use anonymization and de-identification techniques.
			PIRC	Privacy Incident Response Controls	The DPS must ensure the cloud service provider implements proper incident response techniques and procedures to respond to privacy incidents. This includes automated controls for immediate response, e.g., email notification of involved individuals on the incident status and expected resolution time.
			PMAC	Privacy Monitoring and Auditing Controls	The DPS and cloud service provider shall implement systems to audit the security, appropriate use, and loss of PII. Further, regular assessments must be conducted, e.g. risk assessment to identify and address gaps in privacy compliance and the associated controls.
			DRC	Data Retention Controls	The DPS and cloud service provider shall only retain PII for the purposes specified by notices or regulations, e.g. the PCI DSS cardholder data retention period. Storage and archiving controls are used for DRC.
			SDDC	Secure Disposal of Data Controls	The DPS and cloud service provider shall implement secure disposal and complete removal controls for data from all cloud storage media, ensuring that it is not recoverable by any forensic means.
			C	Compliance	CPCM
	CCM	Compliance by Control Monitoring			The DPS and cloud service provider shall perform ISPC compliance checks on cloud components prior to implementing the DPS cloud migration plan. Automated controls should be enforced to detect compliance violations, e.g. a change in the hypervisor encryption protocol triggers a violation of ISPC controls unless a change request was permitted.
	SLA	Compliance by Service Level Agreement (SLA) Monitoring Controls			The cloud service provider SLA monitoring logs shall be reviewed by the DPS for SLA assurance. This will reveal service interruptions, threats to cloud network availability, and other evidence to support the DPS in the case of an SLA violation.
LMR	Logging, Monitoring, and Reporting	PCI DSS requirement 10 requires that the DPS tracks and monitors all access to network resources and cardholder data. The DPS shall ensure that proper change management, incident response, system			
				performance, system security, and account management solutions are employed by cloud service provider.	

Table 3
Cloud ISPC Readiness Levels.

Maturity Level	Maturity Definition	Explanation	Control Readiness
0	Non-Existent	Cloud ISPC control is neither implemented or present.	Not Ready
1	Initial	Cloud ISPC control is present but partially implemented and not well documented.	Ad-hoc Readiness
2	Repeatable	Cloud ISPC control is present but inconsistently implemented and partially documented.	Reactive Readiness
3	Defined	Cloud ISPC control is present, fully implemented, and documented.	Proactive Readiness
4	Managed	Cloud ISPC control is present, fully implemented, and documented. Performance metrics for each ISPC control are defined and communicated.	Predictive Readiness
5	Optimized	Cloud ISPC control is aligned with the agency business processes and continuously improved. The control performance metrics are measured and monitored.	Optimum Readiness

model provides DPS personnel with analysis results to make informed decisions.

For **data analysis**, DPS personnel must create a data catalog, data classification, data event, and report logs to identify past and emerging threats and risks facing the agency. Further, an evaluation of cloud risks to the financial sector, in particular to payment systems, must be undertaken to determine cloud behavior against such risks and the response and recovery procedures employed.

For effective **decision-making**, the ISPC model requires that DPS personnel perform regular reviews and updates to the risk control strategies. Further, they should address the risks associated with migrating to a cloud environment. Cloud risk assessment should be an integral part of the DPS enterprise risk management framework. If they are within the acceptable risk tolerance, then migration is feasible.

The ISPC flowchart [19] details the methodology for evaluating current requirements and selecting the applicable cloud technology. The four main components of the ISPC model are discussed in the following steps.

4.1. STEP 1: ISPC cubic model

The first step is to define the problem, determine the objectives and alternatives, and identify the important ISPC elements. The cloud cubic model [20] was used as a mapping tool between security policies, attributes, and controls. It provides a 3D structure for identifying ISPC controls to ensure visibility. For simplicity and also to maintain agency privacy, only the most important controls are summarized in Table 2.

4.2. STEP 2: ISPC control assessment

The second step is to assess the current and desired states for the ISPC controls. The results from step 1 are examined using the systems security engineering capability maturity model (SSE-CMM) [19,21]. Table 3 presents the relative maturity on a scale from 0 to 5 based on this model. An example of the final readiness assessment findings for the current and desired control states is shown in Tables 4 and 5, respectively. Table 5 indicates that DPS personnel would like to improve the current ISPC controls to a higher

maturity/readiness. In the next section, the feasibility of migrating DPS systems with either the current or desired ISPC readiness is discussed.

4.3. STEP 3: Cloud feasibility analysis

The third step is to determine if cloud services are feasible and applicable to the agency payment systems ISPC requirements. In addition, this step uses the assessment results obtained from the previous step to address not only the current state of ISPC controls but also the desired state. The feasibility analysis (FA) consists of two parts as described below.

4.3.1. Technical feasibility

Technical controls and sub-controls in the DPS are addressed in terms of cloud feasibility to maintain or improve the technical operations of the agency payment systems. The DPS was advised to consider the following points.

- Compatibility with the selected cloud services. For example, payment applications should be tested using the private cloud deployment model and IaaS. The test results should indicate that there are no issues in running payment applications on an IaaS cloud instance.
- Adequate resources are assigned for the implementation of current and desired ISPC controls and sub-controls.
- Documentation for cloud migration and maintaining payment systems operations is compiled during the study including migration timelines, manpower, and cloud facilities.
- Response plan for any issues reported during the migration and proposals for alternative and/or compensative solutions.

4.3.2. Non-Technical feasibility

Here, the economic factors and associated strategies, frameworks, policies and procedures of payment systems are considered. The DPS should ensure that the cost of ISPC migration is justified and the migration conforms to ISPC policy requirements. In addition, the ISPC policy should reflect new changes such as the inclusion of secure cloud service level agreements in support of payment systems operational performance and availability.

Table 4
Current ISPC Readiness.

Control	Current Readiness Level					
	0	1	2	3	4	5
Department of Payment Systems (DPS) Objectives, Mission, and Vision	2	1	1	0	0	0
Information Security, Privacy, and Compliance Policy	0	2	2	0	0	0
Confidentiality	0	0	3	3	0	0
Integrity	0	0	4	0	0	0
Availability	0	0	1	3	0	0
Privacy	0	3	2	0	0	0
Compliance	0	0	1	3	0	0
Current Readiness	2	6	14	9	0	0

Table 5
Desired ISPC Readiness.

Control	Desired Readiness Level					
	0	1	2	3	4	5
Department of Payment Systems (DPS) Objectives, Mission, and Vision	0	0	0	4	0	0
Information Security, Privacy, and Compliance Policy	0	0	0	4	0	0
Confidentiality	0	0	0	3	3	0
Integrity	0	0	0	1	3	0
Availability	0	0	0	0	4	0
Privacy	0	0	0	3	2	0
Compliance	0	0	0	1	3	0
Desired Readiness	0	0	0	16	15	0

4.4. STEP 4: Readiness for migration

The last step is to compile and organize all results from the previous steps so the DPS can make an appropriate migration decision. Further, DPS personnel should develop a detailed migration plan or roadmap when selecting the most ISPC compliant cloud provider. The DPS is advised to do the following.

- Obtain management support and commitment to DPS cloud migration, i.e. make the decision to migrate.
- Create, audit, and update the migration plan according to the decisions made.
- Review the migration plan and ensure it meets the agency strategic goals and objectives.
- Perform testing to detect unforeseen limitations, e.g. missing components, lack of resources and trained personnel, and compatibility issues.
- Create a list of secure and suitable cloud service providers, for example, cloud service providers A, B, C, and D in Table 6. Note that these are actual service providers, but due to confidentiality their names cannot be disclosed.

5. Results and discussion

From the tables in the previous section, it is clear that the DPS personnel would like to migrate to cloud technology. This is evident from the feasibility analysis and migration readiness i.e. steps 3 and 4. Further, cloud service provider B is the most suitable and secure service provider as it meets the minimum requirements

for a private cloud deployment, and ranks first in the feasibility analysis. Further, they oppose a public or community cloud deployment as this would risk payment transactions data violating ISPC policy and compliance requirements. For example, this data would be vulnerable to hacking attacks, data leakage, and loss of confidentiality compared to other cloud deployment models, i.e. private and hybrid. As mentioned previously, DPS personnel believe that their payment systems and the required resources such as software should be available as and when required, and hence, availability issues can be resolved when moving to the cloud. Further, even though cloud technology may be elastic, scalable, private and available, if the confidentiality, integrity, and compliance are not adequately addressed, migration would not be advantageous. Therefore, the corresponding controls were key in the selection of a secure cloud deployment model by DPS personnel. The decisions may be different for financial sectors in different jurisdictions due to the corresponding security, privacy, and compliance legislation.

5.1. Managerial relevance

The results presented in this paper have some key conclusions for practitioners, which are as follows.

- Although significant technical aspects of cloud security were addressed, a managerial view was taken related to choosing a secure, private, and compliant cloud deployment model. It was demonstrated that a case study approach will benefit the financial practitioners, especially IT security and risk managers

Table 6
Department of Payment Systems (DPS) Migration Readiness.

Control Details				Cloud Service Provider Applicability and Feasibility			
ISPC Control	Control Name	Current Readiness Level	Desired Readiness Level	A	B	C	D
OMV	<i>Department of Payment Systems (DPS) Objectives, Mission, and Vision</i>						
ISS	Information Security Strategy	0	3	✓	✓	✓	✓
ISMF	Information Security Risk Management Framework	0	3	✓	X	X	✓
ISG	Information Security Governance	2	3	X	✓	X	X
ISC	Information Security Compliance	1	3	X	✓	X	X
ISPC	<i>Information Security, Privacy, and Compliance Policy</i>						
NS	Network Security Policy	2	3	✓	✓	✓	✓
AS	Application Security Policy	1	3	✓	✓	✓	✓
PCI	PCI DSS Compliance Policy	2	3	X	✓	X	X
BCP	Contingency, Business Continuity, and Disaster Recovery Planning Policy	1	3	X	✓	X	X
C	<i>Confidentiality</i>						
CC	Cryptography Controls	3	4	✓	✓	✓	✓
ISC	Information Sharing Controls	3	4	✓	✓	✓	✓
ISRC	Information in a Shared Resource Controls	3	4	✓	✓	X	X
TMAC	Transmission Medium Access Controls	2	3	X	✓	✓	✓
TCC	Transmission Confidentiality Controls	2	3	✓	✓	✓	✓
VSC	Virtualization (Hypervisor) Security Controls	2	3	✓	✓	✓	X
I	<i>Integrity</i>						
SFIC	Software, Firmware, and Information Integrity Controls	2	4	✓	X	✓	X
IIVC	Information Input Validation Controls	2	4	X	X	X	✓
CARC	Change and Access Restriction Controls	2	4	✓	X	X	✓
TIC	Transmission Integrity Controls	2	3	X	X	X	X
A	<i>Availability</i>						
AAC	Accountability and Auditing Controls	2	4	X	X	✓	X
TAC	Transmission Availability Controls	3	4	✓	✓	X	✓
CPMC	Capacity Provisioning and Monitoring Controls	3	4	✓	✓	✓	✓
DOSC	Denial of Service (DoS) Controls	3	4	X	✓	✓	✓
P	<i>Privacy</i>						
PIIC	Inventory of Personally Identifiable Information (PII) Controls	2	4	X	✓	X	X
PIRC	Privacy Incident Response Controls	2	4	✓	✓	✓	X
PMAC	Privacy Monitoring and Auditing Controls	1	3	X	✓	X	✓
RDC	Data Retention Controls	1	3	✓	✓	✓	✓
SDDC	Secure Disposal of Data Controls	1	3	✓	✓	X	X
Com	<i>Compliance</i>						
CPCM	Compliance by Policy and Clause Monitoring Controls	3	4	X	✓	✓	✓
CCM	Compliance by Control Monitoring	3	4	✓	✓	X	X
SLA	Compliance by Service Level Agreement (SLA) Monitoring Control	2	3	X	✓	✓	✓
LMR	Logging, Monitoring, and Reporting	3	4	✓	✓	✓	✓

of financial establishments, as they are likely to have similar problems.

- Prior work was utilized, i.e. the ISPC readiness model, as this allows IT security and risk personnel to make informed decisions in undertaking strategic initiatives, e.g. migrating payment systems to cloud technology.
- Controls were identified to make strategic decisions using the proposed ISPC control matrix along with detailed discussion with DPS personnel who are experienced in their domains. Hence, these controls can also be used by security and risk practitioners in the financial industry when addressing similar problems.

5.2. Implications of the decision

From the case study, cloud service provider B should be adopted by DPS personnel as it is the most secure and compliant. The next decision to be made is whether the cloud system should be created, hosted and maintained by DPS IT personnel or outsourced to a trusted third party. A study of the associated decision process is left for future study. The implications of these decisions on agency personnel are outlined below.

5.2.1. DPS personnel

Since the agency has adequate network resources, personnel can access the required cloud-hosted applications from their current locations. This should increase the productivity and performance of DPS personnel and enable mobility. Typically, security principles for remote authentication, authorization, filtering, and monitoring are applied for remote access. It is recommended that these be combined with the principles of least privilege authority and multifactor authentication, i.e. something you have, something you know, and something you are.

5.2.2. DPS IT center personnel

DPS IT center personnel currently handle maintenance requests such as upgrades, repairs, support, re-installation, and imaging. The chances of application software and hardware failure or corruption can be significantly reduced by migrating to the cloud. Moreover, the number of the DPS IT personnel can be reduced. Personnel will still be needed for customer and technical support such as maintaining access changes and creating and modifying accounts.

5.2.3. Management

The agency management recognizes the potential cost benefits in choosing private cloud technology. The cloud pay-per-use and on-demand high availability models allow for significant savings as well as proper utilization of software and applications, i.e. the payment systems. Fees for software licenses and upgrading can be eliminated, and fees for hardware resources, deployment, and implementation minimized. However, there are initial costs associated with cloud adoption. The agency has to create the necessary mechanisms to train personnel and connected customers for the new system, but the long-term benefits will outweigh these costs.

5.3. Decisions confirmed

Using the ISPC model, a decision was made by the DPS to gradually migrate to cloud services. The awareness service acquired, namely InfoShield, is a comprehensive cloud-based eLearning awareness solution recommended by the case study. In addition to InfoShield, PhishMe was also acquired for detailed awareness assessment of personnel against phishing attacks. Both products are cloud services, i.e. software as a service (SaaS). With these products, all DPS personnel will receive scheduled emails containing unique links to InfoShield and/or PhishMe. These links lead

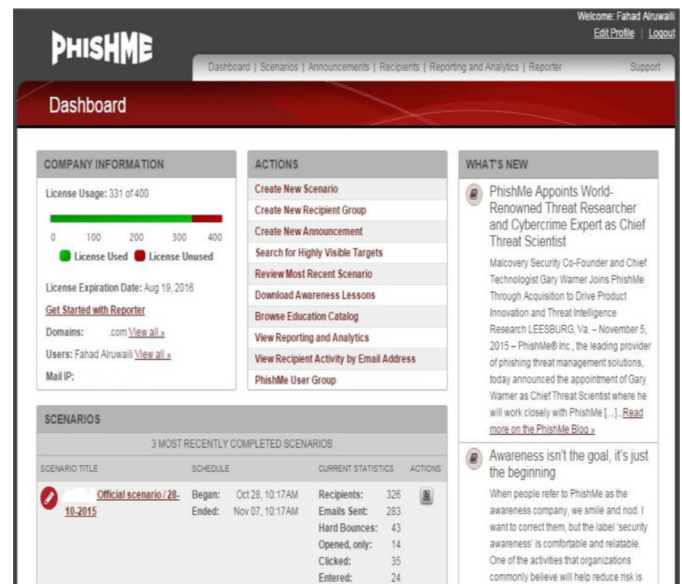


Fig. 1. PhishMe phishing awareness administrative dashboard.

Response Breakdown

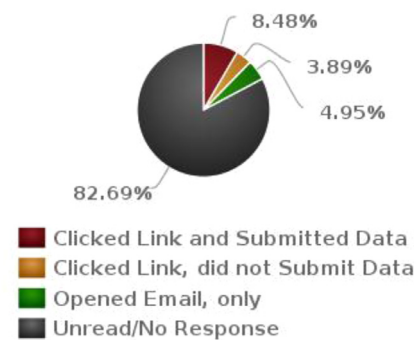


Fig. 2. Phishing awareness response results.

to assessment sessions which provide the level of awareness of personnel. For example, an employee submitting his ID or password indicates weak awareness, and hence customized content to combat this weakness will be delivered to them. The goal is to heighten the information security awareness of all personnel, educate technical, non-technical, and business users to better secure information, monitor awareness levels, and deliver customized content as per user awareness results. The first test sent phishing emails to all DPS personnel to measure their reaction and response to this attack. The results were compiled and are presented in Figs. 1–3. This shows that 17.4% of personnel are susceptible to phishing attacks, and hence 49 employees need appropriate and immediate awareness training. These numbers will be compared with future results to track awareness improvements.

InfoShield and PhishMe were acquired to comply with payment compliance industry data security requirements, i.e. the payment card industry data security standard (PCI-DSS), for awareness training. PCI DSS requirement 12.6 [32] stipulates that a formal security awareness program must be in place. As the agency is responsible for processing and monitoring all payment transactions in the country, it must comply with this standard. The decision to move

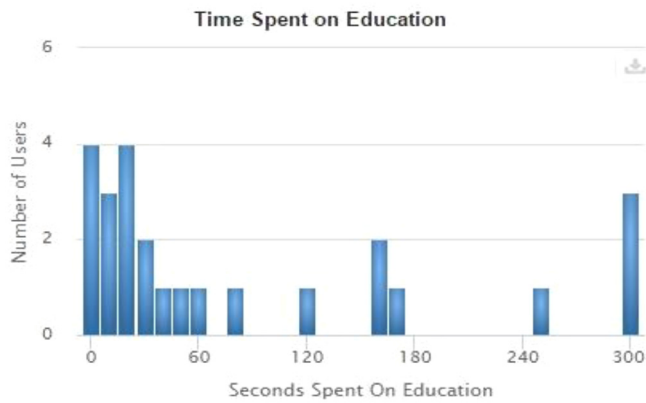


Fig. 3. Time spent on awareness content.

the DPS awareness program to the cloud is part of the overall cloud migration plan.

Cyber security threat intelligence is another DPS ISPC requirement that promotes proactive incident response and defense capabilities. Threat intelligence is a cloud security monitoring solution that provides evidence-based knowledge of emerging threats based on the targeted industry (e.g. the financial sector), technology (e.g. CISCO routers), and geography (e.g. the Middle East). DPS personnel sought to have an improved response plan and defense readiness against threats affecting their payment systems. A decision was made to acquire Symantec DeepSight, a cloud-based threat intelligence service. This service complies with multiple DPS ISPC policy requirements, i.e. incident response and mitigation policy, proactive security awareness requirements, information security risk management policy, and information security integration. The last DPS ISPC policy requirement, integration of threat intelligence, was included for automating the actionable advice obtained from DeepSight to the existing security information event management (SIEM) solution to make responses faster and proactive.

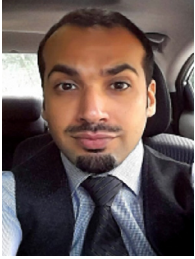
6. Conclusion

Cloud computing services are being considered by the financial sector around the world, but little has been done in Middle East countries such as Saudi Arabia. Further, existing studies on cloud adoption by the financial sector have not considered the architectures and models or examined the implementation of cloud services. The decisions associated with the adoption of secure cloud services such as the deployment models for implementing secure, private, and compliant cloud services have not been adequately examined. This paper provided a case study regarding migration of the payment systems of the Saudi Arabian central bank to the cloud using an ISPC readiness model. The requirements in this model were used to assist in making migration decisions. The impact of migrating to the cloud, in particular the deployment of secure, private, and compliant cloud services, was examined and presented to DPS personnel and management. As a result, the decision was made to migrate DPS security applications, i.e. threat intelligence and security awareness, to the cloud through the adoption of Symantec DeepSight, InfoShield, and PhishMe platforms.

References

- [1] Jouini M, Aissa AB, Rabai LBA, Mili A. Towards quantitative measures of information security: A cloud computing case study. *Int J Cyber-Secur Digital Forensics* 2012;1(3):248–62.
- [2] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. *J Netw Comput Appl* Jan. 2011;34(1):1–11.
- [3] Mell P, Grance T. The NIST Definition of Cloud Computing. National Institute of Standards Technology; 2011 <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf> Last viewed (10-11-2017).
- [4] Hossain S. Cloud computing terms, definitions, and taxonomy. IGI Global 2012.
- [5] Alruwaili FF, Gulliver TA. SOaaS: Security operations center as a service for cloud computing environments. *Int J Cloud Comput Serv Sci* 2014;3(2):87–96.
- [6] Ranjan R, Buyya R, Nepal S, Georgakopoulos D. A note on resource orchestration for cloud computing. *Concurrency Comput Jun.* 2015;27(9):2370–2372.
- [7] Khajeh-Hosseini A, Greenwood D, Sommerville I. Cloud Migration: A case study of migrating an enterprise it system to IaaS. In: *Proc. IEEE International Conference on Cloud Computing*; Jul. 2010. p. 450–7.
- [8] Shi A, Xia Y, Zhan H. Applying cloud computing in financial service industry. In: *Proc. IEEE International Conference on Intelligent Control and Information Processing*; Aug. 2010. p. 579–83.
- [9] Barron C, Yu H, Zhan J. Cloud computing security case studies and research. In: *Proc. World Congress on Engineering*, 2; Jul. 2013. p. 3–5.
- [10] Wyld DC. Moving to the cloud: an introduction to cloud computing in government. IBM Center for the Business of Government; Nov. 2009 <http://www.businessofgovernment.org> Last viewed (07-10-2017).
- [11] Hosseini AK, David G, Ian S. Cloud migration: A case study of migrating an enterprise IT system to IaaS. In: *IEEE International Conference on Cloud Computing*; Aug. 2010. p. 450–7.
- [12] Wang B, Zheng Y, Lou W, Hou YT. DDoS attack protection in the era of cloud computing and software-defined networking. *Comput Netw* 2015;81:308–319.
- [13] Hosseini AK, Greenwood D, Smith JW, Sommerville I. The cloud adoption toolkit: Supporting cloud adoption decisions in the enterprise. *Softw* 2012;42(4):447–65.
- [14] Kurdi AR, Taleb-Bendiab A, Randles M, Taylor M. E-government information systems and cloud computing (Readiness and Analysis). In: *Proc. IEEE International Conference on Developments in E-systems Engineering*; Dec. 2011. p. 404–9.
- [15] Bailey B. Cloud computing may create new venues for high-tech criminals San Jose Mercury News. Last viewed (13-10-2017) http://www.mercurynews.com/businessbreakingnews/ci_12812412?n_click_check=1.
- [16] Sibiya G, Fogwill T, Venter HS, Ngobeni S. Digital forensic readiness in a cloud environment. *Proc. IEEE AFRICON* 2013:1–5.
- [17] Dutta S, Mia I. ICT for Sustainability; 2010. *World Economic Forum on Global Information Technology Report 2009-2010*.
- [18] Obi T. Waseda University World e-Government Ranking; Jan. 2010. *Research Report of the Waseda University Institute of e-Government* <http://www.waseda.jp/eng/news10/index.html> Last viewed (11-10-2017).
- [19] Alruwaili FF, Gulliver TA. ISPC: An information security, privacy, and compliance readiness model for cloud computing services. *Int J Future Gener Distr Syst* 2014;4(4).
- [20] Alruwaili FF, Gulliver TA. SecSLA: A proactive and secure service level agreement framework for cloud services. *Int J Cloud Comput Serv Sci* 2014;3(4).
- [21] ISO and IEC. Information technology systems security engineering-capability maturity model (SSE-CMM, ISO/IEC 28127). *International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)*; 2002.
- [22] Alruwaili FF, Gulliver TA. Safeguarding the Cloud: an effective risk management framework for cloud computing services. *Int J Future Gener Distrib Syst* 2014;1(2).
- [23] Al-Awadi M, Renaud K. Success factors in information security implementation in organizations. In: *Proc. IADIS International Conference on e-Society*; Jul. 2007. p. 169–76.
- [24] Ramachandran N, Sivaprakasam P, Thangamani G, Anand G. Selecting a suitable cloud computing technology deployment model for an academic institute. *Campus-Wide Inf Syst* 2014;31(5):315–45.
- [25] Dillon T, Wu C, Chang E. Cloud computing: issues and challenges. In: *Proc. IEEE International Conference on Advanced Information Networking and Applications*; Apr. 2010. p. 27–33.
- [26] Stein S, Ware J, Laboy J, Schaffer HE. Improving K-12 pedagogy via a cloud designed for education. *Int J Inf Manage* 2013;33(1):235–41.
- [27] McKay J. Pitching the policy: implementing it security policy through awareness. SANS Institute; Jul. 2003 <http://www.giac.org/paper/gsec/3223/pitching-policy-implementing-security-policy-awareness/105199> Last viewed (09-10-2016).
- [28] Pocatilu P, Alecu F, Vetrici M. Measuring the efficiency of cloud computing for e-learning systems. *WSEAS Trans Comput* 2010;9(1):42–51.
- [29] Katz FH. The effect of a university information security survey on instruction methods in information security. In: *Proc. ACM Conference on Information Security Curriculum Development*; Sep. 2005. p. 43–8.
- [30] Baxter P, Jack S. Qualitative case study methodology: Study design and implementation for novice researchers. *Qual Report* 2008;13(4):544–59.
- [31] Yin RK. Applications of case study research. 3rd ed. London, UK: Sage Publications; Jun. 2011.
- [32] Gorge M. Data protection: Why are organisations still missing the point? *Comput Fraud Secur* 2008;2008(6):5–8.
- [33] Alassafi M, Alharthi A, Alenezi A, Walters R, Wills G. Investigating the security factors in cloud computing adoption: Towards developing an integrated framework. *J Internet Technol Secured Trans* 2016;5(2).

- [34] Alharthi A, Alassafi M, Walters R, Wills G. An exploratory study for investigating the critical success factors for cloud migration in the Saudi Arabian higher education context. *Telematics Inf* 2017;34(2):664–78.
- [35] Amin R, Inayat I, Shahzad B, Saleem K, Aijun L. An empirical study on acceptance of secure healthcare service in Malaysia, Pakistan, and Saudi Arabia: A mobile cloud computing perspective. *Ann Telecommun* 2017;72(5-6):253–64.
- [36] Alsanea M, Barth J, Griffith R. Factors affecting the adoption of cloud computing in the government sector: a case study of Saudi Arabia. *Int J Cloud Comput Serv Sci* 2014;3(4).
- [37] Rajeh W, Jin H, Zou D. Saudi cloud infrastructure: A security analysis. *Sci China Inf Sci* 2017;60(12).



Fahad F. Alruwaili is an Assistant Professor in the College of Computing and Information Technology, University of Shaqra, Saudi Arabia. He is a cyber security and risk management consultant with over thirteen years of practical experience and research development. He received the BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he received the MS degree in Computer, Information, and Network Security with first class honors from DePaul University, Chicago, IL USA, and in 2011 the MS degree in Information Systems and Technology with first class honors from Claremont Graduate University, Los Angeles, CA USA. In 2016, he received the PhD degree in Electrical Engineering from the University of Victoria, Victoria, BC Canada. His research interests are in the technical and theoretical aspects of information security and data privacy.



T. Aaron Gulliver received the PhD degree in Electrical Engineering from the University of Victoria, Victoria, BC Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.