Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Best Practices for Governance of IT Systems, Applications, and Operations in the Cloud

CAPSTONE REPORT

Susan Bowman
IT Project Management Consultant

University of Oregon
Applied Information
Management
Program

Spring 2016

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Best Practices for Governance of IT Systems, Applications, and Operations in the Cloud

Susan Bowman

IT Project Management Consultant

Abstract

This study presents literature on best practices with respect to governance in the cloud to promote an industry-wide secure cloud environment. Materials provide information on cloud computing and inherent risks associated with moving to the cloud. References pertain to the transfer of knowledge and learning to move to and use cloud-computing services. The successful transfer of IT systems from a traditional IT environment to the cloud depends on a defined governance plan.

Keywords: governance, IT governance, cloud computing, cloud-computing processes, cloud security, enterprise-wide system in the cloud, enterprise-wide cloud computing. best practices in cloud computing, best practices for IT governance, subset of corporate governance.

Table of Contents

List of Tables and Figures

Annotated Bibliography Introduction

Problem

The rate of growth and adoption of cloud computing services continues to be explosive (Rebollo, Mellado, Fernandez-Medina, & Mouratidis, 2015). Cloud computing has made end users both excited about the opportunities provided by the cloud and yet nervous about the concerns of security in the cloud (Parekh & Sridaran, 2013, p. 44). Garg, Versteeg, and Buyya (2012) assert that even with the number of cloud services available, it is difficult for cloud customers to select a cloud service that will best meet their organizational requirements (Garg et al., 2012, p. 1022). Cloud computing is defined by the National Institute of Standards and Technology (NIST) (2011a) 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" (NIST, 2011a, p. 2). Baun (2011) similarly defines cloud computing as "foster[ing] the provision and use of IT infrastructure, platforms, and applications of any kind in the form of services that are electronically available on the Web" (p. 1012). Bond (2015) suggests that cloud services are not a revolutionary shift, but rather "an evolution of information technology enabling a new style of IT services at a faster pace than in the past" (p. 2).

When organizations transition data, applications, and infrastructure to a cloud-computing environment, security becomes a key concern (NIST, 2011b). Bond (2015) asserts that when transitioning to a cloud-computing environment, the very first consideration that should be given is to define who will establish security, policies, and system accreditation (Bond, 2015, p. 231). In a report on ten steps for enhancing security in cloud computing, the Cloud Standards

Customer Council (CSCC) (2015) suggests that as organizations transition to the cloud, at a minimum, the same level of security that must be maintained for their assets in the cloud as exists in their traditional IT environments (p. 7). Security risks are inherent when moving to cloud computing (Robinson, 2011, p. 41). When considering a move to the cloud, customers need to clearly understand the security benefits and risks and communicate realistic expectations with the cloud provider (CSCC, 2015, p. 4). Security risks in the cloud include: (a) potential misuse of data when organizations share cloud resources and (b) data breaches caused by malicious user(s) accessing data stored in the cloud to which they are not authorized (Rao & Selvamani, 2015). Other breaches occur with unauthorized access from the Internet due to the lack of strong authentication processes in place by a cloud service provider (CSCC, 2015).

Some organizations are finding challenges in affording the most secure cloud solutions. Private clouds, data segregation, and different levels of security offer alternatives from traditional public cloud security levels, but tend to be more expensive (Bond, 2015). Bond (2015) asserts "experience and industry trends show that customers have a preference for the economics provided by public clouds, [but] it is private clouds that offer more flexibility with customized features and security" (p.17). A private cloud is defined as a cloud infrastructure that manages and operates as a single organization or third party, and can be hosted on premises or by a third-party datacenter. Private clouds tend to be more flexible and customizable because they are owned by one customer organization (Bond, 2015, p. 466). Private clouds also offer better security than public clouds because they segregate data for their customers (Bond, 2015).

Small businesses can more quickly adopt hosted applications at startup because there is typically little or no infrastructure in place for a small business at inception (Bond, 2015), but these hosted solutions often do not offer data segregation for their customers, meaning that one

customer's data may be hosted on the same servers as the data of other customers (Bond, 2015). Customer data that is hosted on the same servers as other customers cause security concerns because one customer's data and resources can also accidentally be exposed to other customers, or access to a customer's own resources may be unwittingly blocked (NIST, 2011b). Some public cloud providers have entered virtual private, community, and private cloud service markets to provide greater data segregation and customization for their customers. Data segregation occurs when a solution is offered in response to security concerns from customers who do not want their data and services offered on the same servers as other customers (Bond, 2015). "Some cloud providers offer higher government-level security upgrades" (Bond, 2015, p. 18), such as an isolated and dedicated network infrastructure for customers purchasing government-compliant high-security cloud options (Bond, 2015). Prigge (2011) asserts that one common thread that should run through every level of infrastructure is to keep it separated (p. 1); it will ensure the ability to deliver "solid security, performance, and efficiency" (p. 3).

Security concerns arise with the loss of governance rights when a customer gives control to the cloud service provider for issues that could impact security, but the cloud service provider fails to deliver resolutions to the issues, thus creating gaps in security defenses (CSCC, 2015). One way in which security concerns can be addressed is to implement a security governance framework that will "manage all risks that can appear and establish a set of rules for dealing with security issues and compliance of the organization's cloud environment" (Suicimezov & Georgescu, 2014, p. 833). Robert S. Seiner (2014) defines data governance as "the formal execution and enforcement of authority over the management of data and data related assets" (p. 2). The term "cloud governance" is used to refer to the paradigm extending traditional IT governance to cloud computing (Brandis, Dzombeta & Haufe, 2013, p. 275).

Though cloud computing has been the target for recent security attacks, having a strong governance framework can provide security in the cloud (Suicimezov & Georgescu, 2014). Bond (2015) asserts that governance is a significant part of successful cloud brokering and that the level of governance responsibility depends on customer needs (p. 315). Cloud brokering refers to "the role that an organization or cloud provider can take in delivering to customers a variety of cloud services from multiple providers" (Bond, 2015, p. 342). Bond identifies governance functions as: (a) security accreditation of the cloud broker, (b) operational procedures, (c) contracts and procurement, (d) service level agreements (SLAs), and selection of XaaS cloud service provider, meaning anything that is offered as a service in the cloud (p. 330-331).

Common issues associated with moving to the cloud without a governance structure include: (a) loss of governance due to lack of clarity between customer-owned and shared responsibilities with the service provider (Hill, Hirsch, Lake, & Moshiri, 2013); (b) security concerns as data continues to grow, becoming inflexible and not easy to move and thus a target for online security attacks (Suicimezov & Georgescu, 2014, p. 833); (c) lack of information when cloud service providers do not inform their customers of security breaches (Bond, p. 247); and (d) the fact that customers have lost direct control of the security of their data while maintaining the liability for the security of that data (Bond, p. 323). Loss of governance is "one of the biggest single risks for cloud adopters" (Hill et al., 2013, p. 233).

Purpose Statement

The purpose of this annotated bibliography is to present literature that addresses the establishment of best practices for data governance in the cloud to address security concerns. "Neither academic literature nor the security industry has provided a security governance framework that is suitable for cloud computing services" (Rebollo, Mellado, Fernández-Medina, & Mouratidis, 2015, p. 56). Literature is provided on background of cloud-computing services, security risks and challenges with cloud computing, and best practices for governance in the cloud.

Audience Description

The audience for this research includes Chief Cloud Officers (CCOs), Cloud Service Managers (CSMs), and the Cloud Management Committee (CMC). The main role of the CCO is to mimic the organization's Chief Technology Officer (CTO), but with specific "expertise in the cloud computing services and logistics" (Prasad et al., 2014, p. 344). The CCO also participates in "the coordination of the cloud computing services-based technological efforts between the business units and the corporate goals to ensure synergy and economics of scale" (Prasad et al., 2014, p. 344). The CSM is the principal resource within the IT cloud governance structure, and is responsible for monitoring, facilitating, and making decisions relating to cloud computing services (Prasad et al., 2014, p. 345). "The CSM will deal with the economics of [the] cloud" (Prasad et al., 2014, p. 346). The CMC provides cloud computing expertise and oversight to various levels of management and stakeholders regarding cloud-computing services (Prasad et al., 2014, p. 344).

The audience also includes all knowledge workers using cloud computing services as a source for accessing company data and information, such as IT project managers (PMs)

"responsible for guiding the implementation of new initiatives, upgrades to existing systems, [and] security best practices" (Pruitt, 2013, p. 1). Security and compliance teams provide input for cloud provider systems and staff, data classification and lifecycle management, and "compliance and audit of data and access to critical data and systems that are mostly virtual" (Shackleford, 2010, p.5). All of these stakeholders can benefit from a study that provides information on the best practices for addressing data security concerns in the cloud with a cloud data governance plan.

Research Question

What are best practices for data governance in the cloud to promote a secure cloud-computing environment?

Search Report

Search strategy. The search strategy involves the use of Google to help narrow the list of keywords. This is accomplished by entering the phrases *IT governance in the cloud*, *cloud computing*, *cloud computing processes*, *cloud security*, *enterprise-wide system in the cloud*, *enterprise-wide cloud computing*, *best practices in cloud computing*, and *best practices for IT governance* into the Google search engine, as well as the University of Oregon Library. Similar words or phrases show up in the results, which are identified as the keywords for this study.

There is limited peer-reviewed content regarding the topic *best practices for governance in cloud computing*. There is a broader selection of peer-reviewed content that expands beyond the topic that includes *data governance in the cloud* and *security governance in the cloud*. Because cloud computing technology and applications are changing rapidly, research data are filtered to show only peer-reviewed journals, articles, and books in full-text literature from the

year 2011 forward. Using these parameters results in a very short list of research material on the topic.

Keywords. The research focus is on various keywords in order to retrieve specific and relevant articles. The keywords used are as follows:

- best practices for IT governance;
- best practices in cloud computing;
- cloud computing;
- cloud computing processes;
- cloud security;
- cloud security and governance;
- data governance;
- data governance in the cloud;
- data in the cloud;
- definition of cloud computing;
- enterprise architecture management;
- enterprise-wide cloud computing;
- enterprise-wide system in the cloud;
- governance;
- IT governance;
- National Institute of Standards and Technology (NIST); and
- sustainable cloud computing.

Search engines and databases. The keywords are used to perform searches in the University of Oregon Libraries' databases. The majority of searches are performed within the

University of Oregon Libraries' site. The assumption is that using the University of Oregon Libraries' databases provides a better chance of retrieving more recent peer-reviewed articles and journals. The University of Oregon Libraries' site also provides books for downloading. If the book is not available, searching Google or Amazon can sometimes provide a few full-version ebook versions that can be downloaded onto a Kindle tablet.

Google Scholar is also used to search for literature. However, some of the results from Google Scholar are either not applicable for this study or are duplicate articles from the University of Oregon Libraries' site. Additionally, the Google search engine is used, but only as a tool to generate keywords. The University of Oregon Libraries' databases include the following:

- UO Library Databases A-Z/Subject;
- UO Library Information Technology;
- UO Library Academic Search Premier;
- UO Library Computer Source;
- Science Direct;
- Google Scholar;
- ACM Digital Library, and
- JSTOR.

Documentation approach. Zotero is used to save articles into specified folders. Zotero provides the ability in some cases to create references in American Psychological Association (APA) format. Because Zotero does not always populate the references in APA format, the University of Oregon Libraries provides the ability to create references in APA format.

Additionally, the Purdue Online Writing Lab (OWL) and APA Style Guide (6th ed.) are available online to provide guidance on the correct APA citation formats.

A folder is created using Microsoft Excel specifically for references that include the citation in APA format, the abstract, the search terms and the database used in locating the source. This information provides the ability to retrieve the document should the electronic file get deleted. It also provides a way in which to sort by author, title, and category. Each reference is placed into categories based on content: (a) background on cloud computing services, (b) security risks and challenges with cloud computing, and (c) best practices for governance in the cloud. The Excel files are saved locally and backed up on an external USB drive.

Reference evaluation criteria. References are evaluated using the following criteria based on the University of Florida's Center for Public Issues Education (2014), *Evaluating Information Sources*:

***Authority*.** The reference material is evaluated by examining an author's credentials, including educational history and employment. Authors with advanced degrees or multiple published books and articles are generally more credible. Authors who are associated with a reputable organization or who have been cited multiple times by other authors have credibility. Authority can also be determined by examining the publisher or trade organization for evidence of peer reviews and other signs of a strict editing process.

***Timeliness*.** For the topic of governance in the cloud, the author of this study restricted sources to those published in 2011 or later. This time period was selected because cloud computing is evolving rapidly and the risk is that the information may not be current.

Quality. Sources are validated to determine if the grammar, spelling, and punctuation are accurate. The sources are also evaluated to ensure that the organization, clarity, flow, and structure of the information are accurate and logical.

Relevancy. Sources are evaluated to ensure that the content is appropriate for the purposes of providing strong documentation for best practices for data governance in the cloud. The scholarly sources selected are relevant to the categories identified in the annotated bibliography in support of security for IT governance in the cloud.

Bias. Sources are evaluated to determine if the author has ties or a relationship, directly or otherwise, with any vendor, product, service, organization, or institution that would degrade the impartiality of the information provided. Authors who demonstrate multiple sources for their reported information and perspectives are also indicative of a lack of bias. Finally, sources are validated to ensure that the author's arguments and conclusions are supported by credible and cited sources.

Annotated Bibliography

The references selected for the Annotated Bibliography relate to the topic of best practices in data governance in the cloud to promote a secure cloud-computing environment. Each annotation includes (a) the complete bibliographic citation; (b) the published abstract provided by the author(s); and (c) a summary describing the relevance to this study. The selected references are organized into the following categories: (a) background on cloud computing services, (b) security risks and challenges with cloud computing, and (c) best practices for governance in the cloud.

Each annotation consists of three elements: (a) the full bibliographic citation, (b) an abstract, and (c) a summary. The summaries present an overview of the background on cloud computing services, security risks and challenges, and best practices for governance in cloud computing.

Category 1: Background on cloud computing services

Baun, C. (2011). *Cloud computing web-based dynamic IT services*. New York, NY: Springer. ISBN: 978-3-642-20916-1, e-ISBN: 978-3-642-20917-8. doi: 10.1007/978-3-642-20917-8

Description. Cloud computing is a buzzword in today's information technology (IT) that nobody can escape. But what is really behind it? There are many interpretations of this term, but no standardized or even uniform definition. Instead, as a result of the multi-faceted viewpoints and the diverse interests expressed by the various stakeholders, cloud computing is perceived as a rather fuzzy concept. With this book, the authors deliver an overview of cloud computing architecture, services, and applications. Their aim is to bring readers up to date on this technology and thus to provide a common basis for

discussion, new research, and novel application scenarios. They first introduce the foundation of cloud computing with its basic technologies, such as virtualization and Web services. After that they discuss the cloud architecture and its service modules. The following chapters then cover selected commercial cloud offerings (including Amazon Web Services and Google App Engine) and management tools, and present current related open-source developments (including Hadoop, Eucalyptus, and Open CirrusTM). Next, economic considerations (cost and business models) are discussed, and an evaluation of the cloud market situation is given. Finally, the appendix contains some practical examples of how to use cloud resources or cloud applications, and a glossary provides concise definitions of key terms.

Summary. This book focuses on cloud computing and the cloud models available based on organizational strategies and objectives. Cloud computing offers cloud services that are: (a) web-based, (b) scalable, (c) delivered electronically, (d) pay as you go, and (e) on-demand. The services usually provide multi-tenancy architecture in a utility services environment that provides flexibility in services and savings to its users.

The author introduces the National Institute of Standards and Technology (NIST) cloud computing framework that includes: service models, deployment models, and characteristics of cloud computing. In cloud computing, virtualized IT infrastructures, platforms, and complete applications are implemented in a service-oriented architecture (SOA) environment.

The author suggests that cloud computing depends on technologies, such as: (a) visualization, (b) service-oriented architecture (SOA), and (c) web-based services. Cloud computing deployment models identified are: (a) public, (b) private, and (c) hybrid. The

four service models identified are: (a) Humans as a Service (HuaaS), which identifies with crowdsourcing; (b) Software as a Service (SaaS), which includes applications and services; (c) Platform as a Service (PaaS), which provides an integrated development environment; and (d) Infrastructure as a Service (IaaS), which provides an abstract view of hardware, including networks and data storage. The characteristics of cloud computing are: (a) on-demand, (b) self-service, (c) broad network access, (d) resource pooling, and (e) elasticity. There are many special services provided by cloud computing that typically rely on a distributed infrastructure managed by a centralized environment owned by the provider.

Baun concludes that cloud computing remains exciting and promising as a strong and competitive market trend for the IT industry. Cloud computing can be disruptive, but Baun asserts that taking the opportunity to fundamentally leverage and provision IT services can result in a more secure and sustainable cloud environment. Baun recommends that IT managers consider moving to the cloud, aligning with their organizations' long-term strategies and objectives.

Garg, S., Versteeg, S., & Buyya, R. (2012). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, *29*(4) doi: 10.1016/j.future.2012.06.006

Abstract. Cloud computing is revolutionizing the IT industry by enabling them to offer access to their infrastructure and application services on a subscription basis. As a result, several enterprises including IBM, Microsoft, Google, and Amazon have started to offer different Cloud services to their customers. Due to the vast diversity in the available Cloud services, from the customer's point of view, it has become difficult to decide whose services they should use and what is the basis for their selection. Currently, there

is no framework that can allow customers to evaluate Cloud offerings and rank them based on their ability to meet the user's Quality of Service (QoS) requirements. In this work, we propose a framework and a mechanism that measure the quality and prioritize Cloud services. Such a framework can make a significant impact and will create healthy competition among Cloud providers to satisfy their Service Level Agreement (SLA) and improve their QoS. We have shown the applicability of the ranking framework using a case study.

Summary. This article focuses on cloud computing and its ability to provide on-demand customer service. The expansion of cloud computing is making it difficult for organizations to choose the cloud service that best fits their quality of service (QoS) requirements. This article identifies a framework that ranks key cloud service attributes, enabling customers to select the service provider based on best fit for their organizations. There are two components that users must consider when evaluating QoS to rank cloud providers: (a) Service measurement index (SMI) provides key performance indicators (KPIs), measuring pertinent business services, and (b) cloud computing services are ranked based on attributes.

This article concludes that cloud computing is an integral part of IT resourcing in organizations, and notes that although there are many cloud services to select from, challenges can occur when trying to meet organizational QoS requirements. This article supports SMIcloud framework, which provides those considering moving to the cloud with a solution to assist in ranking cloud service providers based on the following: (a) accountability; (b) agility in provisioning business needs; (c) assurance of service, which refers to the likeliness that the cloud provider will deliver the service as promised; (d)

cost; (e) performance; (f) security and privacy; and (g) usability that allows users to accomplish their goals effectively and efficiently.

NIST Information Technology Laboratory (2011, October 25). *Final Version of NIST Cloud Computing Definition Published.* NIST (Publication No. 800-145). doi: 10.6028/NIST.SP.800-145

Description. Cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The defined service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

Summary. This publication identifies a cloud-computing paradigm that describes a model for providing recurrent and on-demand access. It shares a network of computing resources that can be configured, quickly implemented, and deployed with little effort.

This publication identifies four cloud models and three cloud service models and strategies to consider when deploying to cloud computing. The four cloud deployment models are: (a) Private cloud infrastructure provisioned for specific use by a single user; (b) community cloud provisioned for specific use by the community of shared services; (c) public cloud provisioned for open use; (d) hybrid cloud consists of two or more infrastructures (on premise, private cloud as well as community and/or public) that maintain individuality but are connected by standardization or proprietary technology.

This publication also identifies four cloud service models: (a) Humans as a Service (HuaaS) is restricted to IT services; however, it can also include human resources, (b) Infrastructure as a Service (IaaS) provides customers with the resources necessary to configure and deploy software applications and operating systems, (c) Platform as a Service (PaaS) that allows applications to be configured and processed by the consumer, and (d) Software as a Service (SaaS) allows the consumer to use service provider applications in the cloud. These cloud deployment models and service models provide essential characteristics that help organizations select a cloud provider that best aligns with their strategic goals and objectives.

Rai, R., Sahoo, G., & Mehfuz, S. (2015). Exploring the factors influencing the cloud computing adoption: A systematic study on cloud migration. *SpringerPlus, 4*, 197. doi: 10.1186/s40064-015-0962-2

Abstract. Today, most of the organizations trust on their age old legacy applications, to support their business-critical systems. However, there are several critical concerns, as maintainability and scalability issues, associated with the legacy system. In this background, cloud services offer a more agile and cost effective platform, to support business applications and IT infrastructure. As the adoption of cloud services has been increasing recently and so has been the academic research in cloud migration. However, there is a genuine need of secondary study to further strengthen this research. The primary objective of this paper is to scientifically and systematically identify, categorize and compare the existing research work in the area of legacy to cloud migration. The paper has also endeavored to consolidate the research on Security issues, which is prime factor hindering the adoption of cloud through classifying the studies on secure cloud

migration. SLR (Systematic Literature Review) of thirty selected papers, published from 2009 to 2014 was conducted to properly understand the nuances of the security framework. To categorize the selected studies, authors have proposed a conceptual model for cloud migration which has resulted in a resource base of existing solutions for cloud migration. This study concludes that cloud migration research is in seminal stage but simultaneously it is also evolving and maturing, with increasing participation from academics and industry alike. The paper also identifies the need for a secure migration model, which can fortify organization's trust into cloud migration and facilitate necessary tool support to automate the migration process.

Summary. This article focuses on cloud migration, security risks, and deploying a secure model to the cloud, while aligning with business applications and IT infrastructure. Because of the benefits that cloud computing offers that outdated legacy systems cannot provide, many organizations are in favor of adapting to this new technology. However, cloud security and migration issues are hindering adaptability.

This article presents a survey on secure migration processes in order to identify the key concerns surrounding the secure adoption of cloud services. These authors recommend implementing a five-phased cloud migration model that uses a waterfall methodology that incorporates both a bottom-up and top-down approach to identify key phases in a cloud migration.

These authors conclude by identifying cloud deployment and service models, tools and techniques, security risks, and an approach for migrating to the cloud using a five phase model. The challenges identified in their study for the migration process in cloud computing include: (a) business factors, such as expense and existing IT

investments, security of data, regulations and provisioning; (b) technical factors, such as security infrastructures, IT skill sets, network services and support, and service level agreements (SLAs). This article acknowledges the demand for a secure migration framework that will facilitate an efficient and secure transition to cloud computing.

Category 2: Security risks and challenges with cloud computing

Cloud Standards Customer Council (2015, March). *Security for Cloud Computing Ten Steps to Ensure Success Version 2.0*. Retrieved from: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Introduction. Failure to ensure appropriate security protection when using cloud services could ultimately result in higher costs and potential loss of business (CSCC, 2015), thus eliminating any of the potential benefits of cloud computing. The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers analyze the security implications of cloud computing on their business. The section titled “Current Cloud Security Landscape” provides an overview of the security and privacy challenges pertinent to cloud computing and points out considerations that organizations should weigh when migrating data, applications, and infrastructure to a cloud computing environment. The section titled “Cloud Security Guidance” is the heart of the guide and includes the steps that can be used as a basis for evaluation of cloud provider security. It discusses the threats, technology risks, and safeguards for cloud computing environments, and provides the insight needed to make informed IT decisions on their treatment. The section titled “Cloud Security Assessment” provides customers with an efficient method of assessing the security capabilities of

cloud providers and assessing their individual risk. Additionally, this paper highlights the role that standards play to improve cloud security and also identifies areas where future standardization could be effective.

Summary. This publication is sponsored by the Cloud Standards Customer Council (CSCC), a non-profit advocacy group working to accelerate the cloud's adoption and focused on standards, security, and interoperability issues with the cloud (CSCC, 2015). The publication focuses on the potential negative impact that cloud computing can have on organizations if security is not fully recognized and implemented. This publication recommends that organizations implement a cloud security assessment to identify risks and security capabilities when moving to the cloud. It also provides an overview of how standardization can provide greater improvements and efficiencies to cloud security.

This publication concludes information on the security risks that are inherent with cloud computing. The security risks identified are: (a) loss of governance that occurs when public cloud providers inherit issues that do not get resolved, which can create gaps in security; (b) responsibility of security may not be clearly understood between the customer and cloud provider, leaving security defenses vulnerable and exposed, depending on the model used, such as IaaS or SaaS; (c) lack of process for authenticating and authorizing users; (d) customer does not have individual cloud use due to publicly shared resources, and (e) noncompliance risk due to the inability to verify that compliance is in place with the cloud provider. The CSCC recommends that security policies be put in place and notes that an organization that is moving to the cloud has multiple cloud service models from which to choose; they are: (a) Infrastructure as a service (IaaS), (b) Platform as a service (PaaS), and (c) Software as a service (SaaS). It

further suggests possible solutions be given to cloud risks by standardizing security policies, implementing governance and best practices to address the risks, and certifying compliance in the cloud.

Parekh, D. & Sridaran, R. (2013). An analysis of security challenges in cloud computing. *International Journal of Advanced Computer Science and Applications, 4*(1) doi: http://dx.doi.org/10.14569/IJACSA.2013.040106

Abstract. Vendors offer a pool of shared resources to their users through the cloud network. Nowadays, shifting to cloud is a very optimal decision as it provides pay-as-you-go services to users. Cloud has boomed high in business and other industries for its advantages like multi-tenancy, resource pooling, storage capacity etc. In spite of its vitality, it exhibits various security flaws including loss of sensitive data, data leakage and few others related to cloning, resource pooling and so on. As far as security issues are concerned, a very wide study has been reviewed which signifies threats with service and deployment models of cloud. In order to comprehend these threats, this study is presented so as to effectively refine the crude security issues under various areas of cloud. This study also aims at revealing different security threats under the cloud models as well as network concerns to stagnate the threats within cloud, facilitating researchers, cloud providers and end users for noteworthy analysis of threats.

Summary. This article focuses on security risks and threats to cloud deployment. Cloud computing seeks to combine a fiscal utility model with evolutionary changes made to the existing landscape of computing technologies, services, applications, and infrastructure. The authors seek to incorporate solutions to security in a structured approach, performing a risk analysis in order to expose security threats from cloud deployment. Cloud

computing deployment models identified in this article are: (a) private, (b) public, and (c) hybrid cloud. The four types of service models identified are: (a) Software-as-a-Service (SaaS), (b) Database-as-a-Service, (DaaS), and (c) Infrastructure-as-a-Service (IaaS), and (d) Platform-as-a-Service (PaaS).

The authors conclude in providing suggestions for potential security solutions: (a) delete unnecessary data, such as old passwords, and perform routine system backups to prevent data risks, such as security breaches and compromised data integrity due to unauthorized users accessing data; (b) implement an encryption policy to raise data protection; and (c) compress data to eliminate user copying and uploading of data.

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science, 48*, 204-209. doi: 10.1016/j.procs.2015.04.171

Description. Cloud Computing is a rapidly increasing trend that has a technology connection with Grid Computing, Utility Computing, Distributed Computing. Cloud service providers such as Amazon IBM, Google's Application, Microsoft Azure etc., enable users to develop applications in a cloud environment and to access them from anywhere. Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. Providing security is a major concern as the data is transmitted to the remote server over an Internet channel. Before implementing Cloud Computing in an organization, security challenges needs to be addressed first. In this paper, we highlight data related security challenges in cloud based environment and solutions to overcome them.

Summary. This article provides information on cloud computing environments, the services available, cloud utility model usage, and identifies cloud security as a major

concern. The authors assert that a reduction of security risks is critical for organizations that have data that is stored and transmitted remotely. The authors also note that while there are customizable services available for users anywhere, applications that are being developed and accessed from the Internet pose a major concern for the security of data.

This article identifies three major security concerns associated with the cloud: (a) confidentiality is threatened by data being exposed to malicious users, (b) the integrity of the systems are in jeopardy by not password protecting them from unauthorized users, and (c) availability is threatened if/when there are disruptions or downtime. To improve security for cloud computing, the authors recommend authentication, authorization and access control for stored data.

The authors conclude that data protection is extremely important and recommend the following solutions to protect against potential data risks; they are: (a) implement a framework that secures the data from access by other cloud users, (b) protect the data from unauthorized access with data encryption, and (c) standardize security policies in cloud computing.

Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., & Hopkins, P. (2011). *The Cloud - Understanding the Security, Privacy and Trust Challenges. RAND Corporation.* ISBN: 9780833059604.

Description. This report discusses how policy-makers might address the challenges and risks in respect of the security, privacy and trust aspects of cloud computing that could undermine the attainment of broader economic and societal objectives across Europe.

Summary. This publication focuses on the risks identified with cloud security and privacy; they are: (a) loss of governance; (b) data lock-in when a cloud provider does not

allow cloud users to extract and move data to another service provider; (c) isolation failure, which is meant to guarantee operational confidentiality and integrity without customer interference; (d) compliance risks when providers are unable to provide evidence that they are compliant; (e) cloud data protection vulnerabilities due to lack of data verification and/or password authentication and compliance; and (f) data deletion by malicious end users.

The authors of this publication conclude that cloud computing is riddled with challenges on issues of security and privacy. Some operational tools to help manage security and privacy arising from cloud deployments may be less viable and effective due to the complexity in establishing and monitoring risk controls across all boundaries between the end users and cloud service providers. The authors assert that there is always room for improvement in providing cloud security, including implementing risk control frameworks and best practices.

Other challenges that come with establishing a cloud service arise in the areas of accountability and transparency. To successfully address these challenges, the authors assert that there should be a continuous improvement process in place that will engage all participants who have a vested interest in the successful deployment to the cloud. As a result, this potential economic benefit will address the security and privacy concerns of a cloud-computing environment.

Sood, S. (2012). A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications, 35*(6), 1831-1838. doi: 10.1016/j.jnca.2012.07.007

Abstract. Cloud computing is a forthcoming revolution in information technology (IT) industry because of its performance, accessibility, low cost and many other luxuries. It is

an approach to maximize the capacity or step up capabilities vigorously without investing in new infrastructure, nurturing new personnel or licensing new software. It provides gigantic storage for data and faster computing to customers over the internet. It essentially shifts the database and application software to the large data centers, i.e., cloud, where management of data and services may not be completely trustworthy. That is why companies are reluctant to deploy their business in the cloud even cloud computing offers a wide range of luxuries. Security of data in cloud is one of the major issues which acts as an obstacle in the implementation of cloud computing. In this paper, a frame work comprising of different techniques and specialized procedures is proposed that can efficiently protect the data from the beginning to the end, i.e., from the owner to the cloud and then to the user. We commence with the classification of data on the basis of three cryptographic parameters presented by the user, i.e., Confidentiality (C), Availability (A) and Integrity (I). The strategy followed to protect the data utilizes various measures such as the SSL (Secure Socket Layer) 128-bit encryption and can also be raised to 256-bit encryption if needed, MAC (Message Authentication Code) is used for integrity check of data, searchable encryption and division of data into three sections in cloud for storage. The division of data into three sections renders supplementary protection and simple access to the data. The user who wishes to access the data is required to provide the owner login identity and password, before admittance is given to the encrypted data in Section 1, Section 2, and Section 3.

Summary. This article focuses on data security in the cloud. The author suggests implementing procedures and techniques that address the need for data protection from inception to completion in the cloud environment. A framework addressing data security

in the cloud is divided into two phases: (a) process for moving stored data securely; and (b) secure data retrieval by identifying the requests made to access data, as well as authenticating and verifying signatures for user access.

This author suggests using Secure Socket Layer (SSL) as a method to raise encryption capabilities. It also suggests using a Message Authentication Code (MAC) to check the integrity of the data, as needed. The author concludes that implementing firewalls, virtual private networks (VPNs), and security policies is key to producing a secure cloud environment.

Category 3: Best practices for governance in the cloud

Bond, J. (2015). *The enterprise cloud: Best practices for transforming legacy IT* (First ed.). Sebastopol, CA: O'Reilly Media. ISBN-13: 978-1491907627

Description. Despite the buzz surrounding the cloud computing, only a small percentage of organizations have actually deployed this new style of IT—so far. If you're planning your long-term cloud strategy, this practical book provides insider knowledge and actionable real-world lessons regarding planning, design, operations, security, and application transformation. This book teaches business and technology managers how to transition their organization's traditional IT to cloud computing. Rather than yet another book trying to sell or convince readers on the benefits of clouds, this book provides guidance, lessons learned, and best practices on how to design, deploy, operate, and secure an enterprise cloud based on real-world experience.

Summary. This book focuses on best practices, IT governance, frameworks, and planning for deployment to a secure cloud. The five deployment models identified are: (a) public cloud, (b) virtual private cloud (VPC), (c) private cloud, (d) community cloud,

and (e) hybrid cloud. Organizations choose a service model based on business needs. Larger organizations will typically choose a private cloud because of data sensitivity, whereas small and medium-sized companies will typically choose a public cloud because they are unable to afford a private cloud. Additionally, small businesses initially adopt hosted applications because of the lack of infrastructure at inception.

This book identifies challenges that need to be addressed when moving to the cloud: (a) legacy systems and resources that need to be eliminated to save costs, (b) deploying important applications can be cost prohibitive, (c) lack of redundancy in private clouds, (d) procurement practices can stall deployment, and (e) traditional IT practices must adapt to a new cloud model. The author proposes the following recommendations: (a) replace inefficient legacy systems and resources (e.g., computers, datacenters, and servers) with faster, more powerful computers and systems; (b) evaluate the cost of investment for legacy applications versus new applications; (c) use many datacenters or cloud providers to improve services and operation; and (d) use virtual machines (VMs) launched via automation.

This book concludes that cloud computing's future trend is shifting back to virtualization and the concept of centralization that provides a single instance of software serving multiple users. Bond notes that computing continues to expand in the following areas: (a) automation of provisioning for computing and application services; (b) elasticity provides increased capacity for IT resources (e.g., memory, storage, and network services); (c) on-demand ordering and pay-as-you-go pricing; and (d) self-service management and control systems to provide a quicker, less expensive way to deploy services, allowing organizations to focus on their core business functions.

Brandis, K., Dzombeta, S., & Haufe, K. (2013). Towards a framework for governance architecture management in cloud environments: A semantic perspective. *Future Generation Computer Systems, 32,* 274-281. doi: 10.1016/j.future.2013.09.022

Abstract. This article introduces a model for cloud governance with a specific focus on its semantic aspects. It considers three dominant paradigms — the business–IT alignment paradigm, the governance paradigm, and the cloud paradigm. The model can be enhanced with specific tools to serve as a holistic framework for addressing governance of both traditional and cloud-based IT environments. The proposed consideration of semantic aspects within the model can enable a more feasible application of the model in complex architectural settings — both from the point of view of architecture assessment and architecture management.

Summary. This article suggests a cloud governance model and tools that provide a framework that focuses on both traditional and cloud-based environments. The model considers three paradigms: (a) business-IT alignment paradigm that ensures consistency between an organization's business objectives, operational goals, and IT infrastructure; (b) governance paradigm that considers data objects, requirements, roles and responsibilities (R&Rs); and (c) cloud paradigm, a cloud governance that considers possible deployment models abstracting services such as Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). These service models are becoming more the norm in a delivery system via the Internet and enable large cost advantages in IT provisioning.

The authors suggest that IT governance addresses the following areas of concern: (a) strategic alignment, (b) value delivery, (c) risk management, (d) resource

management, and (e) performance measurement. The authors identify two toolsets that extends the approach to bridging the gap between traditional business-IT alignment and IT governance; they are: (a) Information Technology Infrastructure Library (ITIL) designed to standardize practices that align with IT services to meet business requirements, and (b) Control Objectives for Information and Related Technology (COBIT) designed as a business framework to manage IT governance.

The authors note that a holistic governance framework approach allows the integration of (a) enterprise architecture management (EAM), (b) IT governance, and (c) cloud computing. The governance model offers a holistic view and builds on best practices from other areas, such as legal and technology. Data is presented from a 2011 study that shows cloud brokers are increasing provisions for governance services in cloud computing.

Hill, R., Hirsch, L., Lake, P., & Moshiri, S. (2013). *Guide to cloud computing: Principles and practice* (Computer communications and networks). Heidelberg: Springer. ISBN: 9781447146025

Introduction. Part 1. Cloud Computing Fundamentals – Introducing Cloud Computing – Business Adoption Models and Legal Aspects of the Cloud – Social, Economic and Political Aspects of the Cloud – Part 2. Technological Context – Cloud Technology – Cloud Services – Data in the Cloud – Intelligence in the Cloud – Part 3. Business Context – Cloud Economics – Enterprise Cloud Computing – Cloud Security and Governance – Developing a Cloud Roadmap – Cloud Computing Challenges and the Future.

Cloud computing platforms can allow organizations to become more efficient and more responsive to users of both internal and external systems, yet a clear understanding is

needed in order to separate the facts from the hype behind this new and rapidly expanding area. This Guide to Cloud Computing describes the landscape of cloud computing from first principles, leading the reader step-by-step through the process of building and configuring a cloud environment. The book not only considers the technologies for designing and creating cloud computing platforms, but also the business models and frameworks in real-world implementation of cloud platforms. Emphasis is placed on "learning by doing," and readers are encouraged to experiment with a range of different tools and approaches. Topics and features: Includes review questions, hands-on exercises, study activities and discussion topics throughout the text. Describes the key technologies involved in cloud computing. Explores the use of cloud computing in business environments. Demonstrates the approaches used to build cloud computing infrastructures. Reviews the social, economic, and political aspects of the on-going growth in cloud computing use. Discusses legal and security concerns in cloud computing. Examines techniques for the appraisal of financial investment into cloud computing. Identifies areas for further research within this rapidly-moving field.

Summary. This book focuses on cloud computing and the benefits it offers for business opportunities. One of the most important contributions of cloud computing is creating a network system for cloud users and providers. Cloud security is being addressed by adopting a risk-based approach by prioritizing controls based on the level of damage. Infrastructural framework and best practices are creating a unique and active platform for collaboration and innovation. The authors believe that as systems and networks mature, this effect will contribute to an increasing intellectual collaborative environment, generating value to organizations. The authors provide information about the Cloud

Security Alliance (CSA) that promotes: (a) security planning and deployment to the cloud, (b) implementing best practices for cloud security, and (c) educating potential users on the use of cloud computing.

This book provides a published report by the European Network and Information Security Agency (ENISA) (2009) that suggests security risks must be a priority for cloud architecture. It suggests that a loss of governance happens when the responsibilities between the cloud provider and customer have not been clearly defined. Cloud customers are not able to move to another service provider easily, which creates higher costs for the customer. Security vulnerabilities happen when the number of risks is not reduced. Lack of compliance, incomplete data deletion, and compromises in the cloud can all lead to security risks.

The authors of this book conclude that there are challenges inherent with moving to the cloud and new risks increase the learning curve for organizations across the entire cloud computing environment. Several cloud tools and techniques are identified but they may not meet every business need; therefore, it is important to consider the potential impact on the organization when moving to cloud computing. A few traditional tools and techniques available for cloud development are: (a) SWOT analysis evaluates the strengths, weaknesses, opportunities, and threats for each existing system; (b) critical success factors (CSF) analysis that promotes successful outcomes when transitioning to the cloud; (c) Porter's value chain analysis that measures the impact of the cloud on value and supply chain; (d) governance, risk, and compliance (GRC) analysis that allows organizations to meet objectives; and (e) capability maturity model (CMM) analysis that supports improvement of existing processes.

Prasad, A., Green, P., & Heales, J. (2014). On governance structures for the cloud computing services and assessing their effectiveness. *International Journal of Accounting Information Systems, 15*(4), 335-356. doi: 10.1016/j.accinf.2014.05.005

Abstract. This research suggests information technology (IT) governance structures to manage the cloud computing services. The interest in acquiring IT resources as a utility from the cloud computing environment is gaining momentum. The cloud computing services present organizations with opportunities to manage their IT expenditure on an ongoing basis, and access to modern IT resources to innovate and manage their continuity. However, the cloud computing services are no silver bullet. Organizations would need to have appropriate governance structures and policies in place to manage the cloud computing services. The subsequent decisions from these governance structures will ensure the effective management of the cloud computing services. This management will facilitate a better fit of the cloud computing services into organizations' existing processes to achieve the business (process-level) and the financial (firm-level) objectives. Using a triangulation approach, we suggest four governance structures for managing cloud services. These structures are a chief cloud officer, a cloud management committee, a cloud service facilitation centre, and a cloud relationship centre. We also propose that these governance structures would relate directly to organizations' cloud computing services-related business objectives, and indirectly to cloud computing services-related financial objectives. Perceptive field survey data from actual and prospective cloud computing service adopters suggest that the suggested governance structures would contribute directly to cloud computing-related business objectives and indirectly to cloud computing-related financial objectives.

Summary. This article focuses on IT governance structures in a cloud environment. Cloud computing is a service model that provides on-demand delivery via a network system. IT governance structures are presented to identify appropriate cloud services management to align with organizational objectives. The authors state that the most important goal is for cloud governance structures to provide an opportunity to encourage sustainable relationships between cloud service providers and customers.

This article identifies the challenges and solutions that come with the opportunity to acquire and source IT services as a utility in order to manage IT costs. Organizations face the challenge of adopting and transitioning to cloud services as they determine what governance structure best fits their organizational needs. Sourcing cloud services as a utility leverages governing efforts. A potential solution includes developing metrics to evaluate cloud-based performances.

The authors introduce four potential governance structures to manage the cloud: (a) Chief cloud officer (CCO), (b) cloud management committee, (c) cloud facilitator, and (d) cloud relationship committee. These governance structures suggest a holistic approach to managing cloud services from inception through completion in meeting organizational IT needs. IT services is responsible for (a) managing cloud computing services, (b) ensuring sources fit existing business processes, and (c) considering the appropriate governance structures to manage cloud services.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*, 44-57. doi: 10.1016/j.infsof.2014.10.003

Abstract. *Context:* Cloud computing is a thriving paradigm that supports an efficient way to provide IT services by introducing on-demand services and flexible computing resources. However, significant adoption of cloud services is being hindered by security issues that are inherent to this new paradigm. In previous work, we have proposed ISGcloud, a security governance framework to tackle cloud security matters in a comprehensive manner whilst being aligned with an enterprise's strategy.

Objective: Although a significant body of literature has started to build up related to security aspects of cloud computing, the literature fails to report on evidence and real applications of security governance frameworks designed for cloud computing environments. This paper introduces a detailed application of ISGCloud into a real life case study of a Spanish public organization, which utilizes a cloud storage service in a critical security deployment.

Method: The empirical evaluation has followed a formal process, which includes the definition of research questions previously to the framework's application. We describe ISGcloud process and attempt to answer these questions gathering results through direct observation and from interviews with related personnel.

Results: The novelty of the paper is twofold: on the one hand, it presents one of the first applications, in the literature, of a cloud security governance framework to a real-life case study along with an empirical evaluation of the framework that proves its validity; on the other hand, it demonstrates the usefulness of the framework and its impact to the organization.

Conclusion: As discussed on the paper, the application of ISGCloud has resulted in the organization in question achieving its security governance objectives, minimizing the security risks of its storage service and increasing security awareness among its users.

Summary. This article focuses on security governance frameworks in cloud computing. The empirical evaluation identifies three main pillars of the security governance framework: (a) cloud service security is a key factor to governance success in raising security awareness within the organization; (b) deploying security governance structure defines metrics to evaluate the service deployment by comparing previous governance, and (c) ISGCloud framework's practical applicability executes tasks being deployed guaranteeing service governance structure is viable.

These authors focus on Information Security Group Cloud (ISGCloud), which is a security governance framework that nurtures cloud adoption and enables security deployment. The ISGCloud executes tasks parallel to internal tasks being deployed, guaranteeing that the service governance structure is viable and all security risks are considered. These authors provide information about ISGcloud's performance and design based on industry-wide standards and best practices. They propose ISGcloud framework as an approach to drive the process of developing security governance in support of a cloud service. These authors note the challenge involved in putting a framework like ISGcloud into practice. Though there is awareness of the importance of introducing cloud service security in governance structures, the authors maintain that there is no structured approach available. The ISGcloud framework provides steps for developing a security governance structure for cloud deployment based on the cloud service lifecycle.

Suicimezov, N. & Georgescu, M. (2014). IT Governance in Cloud. *Procedia Economics and Finance, 15,* 830-835. doi: 10.1016/S2212-5671(14)00531-0

Abstract. The evolution of the IT sector influences the development of other systems related to this, and the present trend seems to be the cloud concept. As information and corporate knowledge are directly involved in these processes, they represent major risks and require a high security in fields like usage or control, and IT governance establishes a solid best practice set of rules for companies. The next generation of IT governance will migrate towards Cloud computing, the data lifecycle, social media as models and will integrate existing data in multiple sources, in which security, privacy and control remain critical, vital subjects. Traditional security issues could no longer be effectively solved in the cloud, and as a result other solutions were developed to focus on Governance in the Cloud. IT governance can best manage and ensure the efficiency and effectiveness of IT as a corporate resource, but on the other hand the rapid transition to cloud technologies has fuelled some critical issues in accomplishing success for information systems, communications and security. IT governance offers visibility and IT control, therefore the efforts in corporate governance can reduce operational risks, can establish compliance and protect the invested value. As a consequence, the paper aims to recognize the importance and impact of best practices for IT governance in the evolution of IT systems and to emphasize the importance of Governance in Cloud Computing at the business level.

Summary. This article focuses on IT governance when transitioning to a cloud computing business model. It presents the importance of IT governance, particularly at the business level. It also points out the importance of adapting to cloud services while

focusing on issues inherent with cloud computing: (a) security risks, (b) lack of customer control, and (c) insufficient space control and inability to retain data.

These authors recommend adopting a best practice that uses various IT service models; they are: (a) Complete IT services (XaaS-X), which indicates use of all service models; (b) Infrastructure as a Service (IaaS), which provides flexibility and an open architecture; (c) Software as a Service (SaaS), which provides applications and services; (d) Platform as a Service (PaaS), which allows the setup and scalability of relational databases; and (e) Application as a Service, which provides digital flexibility and scalability that aligns with core business objectives.

Conclusion

The analysis of selected literature identifies the opportunities and concerns for best practices for governance of IT systems, applications, and operations in the cloud. The growth in cloud computing continues to be explosive (Rebollo, Mellado, Fernandez-Medina, & Mouratidis, 2015, p. 44). However, many organizations are still nervous about the security risks and threats that are inherent when moving to the cloud (Parekh & Sridaran, 2013, p. 44). At a minimum, the same level of security should be maintained for assets in the cloud as exists in the traditional IT environment (CSCC, 2015, p. 7). Some common security risks for applications in the cloud include the misuse of data, unauthorized data access, and data breaches caused from malicious users (Rao & Selvamani, 2015, p. 206). Implementing a well-defined governance framework provides the opportunity to define who will establish security measures, policies, and system accreditation, which are all integral to maintaining a secure and safe cloud environment (Bond, 2015, p. 231). As a result, those who operate in the cloud can have more faith that the environment is compliant, ethical, and manageable (Shackleford, 2010, p. 5).

Common ideas and techniques are identified during the analysis of the selected references presented in the Annotated Bibliography section of this literature study. The Annotated Bibliography includes source material and citations, abstracts, and summaries. The intent is to help IT and business managers determine whether their organizations will benefit by deploying to a cloud computing service. The sources identified are categorized as follows: (a) cloud computing services background, (b) security risks and challenges, and (c) best practices for governance in the cloud.

Cloud computing services background

Cloud computing is revolutionizing the IT industry; it remains explosive and promising (Baun, 2011; Garg, Versteeg, & Buyya, 2012; NIST, 2011). There is general agreement that cloud computing can be defined as an Internet-based provider service that offers on-demand network access and shared resources (NIST, 2011; Garg, Versteeg, & Buyya, 2012; NIST, 2011). Baun (2011) asserts that there are many interpretations of cloud computing, that there is no standard definition making it fall into a gray area of ambiguity. He does go on to say however that cloud computing nurtures provisioning of electronic services via the Internet provider (Baun, p. 1).

Cloud computing is typically multi-tenancy and shares resources (Baun, 2011; NIST, 2011; Bond, 2015; Parekh, 2013). Organizations can benefit from cloud computing because of the agility of the platform that supports business applications and IT infrastructure and the cost savings that result (Baun, 2011; Garg, Versteeg, & Buyya, 2012; Rai, Sahoo, & Mehfuz, 2015). Because outdated legacy systems are not able to provide the benefits that cloud computing can, many organizations are adapting to the new cloud technology (Rai, Sahoo, & Mehfuz, 2015).

Cloud computing frameworks consist of cloud characteristics that include: (a) on-demand, (b) self-service, (c) broad network access, (d) resource pooling, and (e) elasticity (Baun, 2011). In addition, cloud computing frameworks include cloud deployment models and cloud service models (see Table 1) (Baun, 2011; Bond, 2015; Brandis, Dzombeta, & Haufe, 2013; CSCC, 2015; Garg, Versteeg, & Buyya, 2012; NIST, 2011; Parekh, 2013). There are "five essential characteristics of cloud computing, three different service models, and four different deployment models" (Baun, 2011, p. 3; NIST, 2011, p. 1). The five characteristics are defined as: (a) on-demand self-service, (b) broad network access, (c) resource pooling, (d) rapid elasticity,

and (e) measured service (Baun, 2011; NIST,2011, p. 2). "The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation" (NIST, 2015, p. 1). Table 1 depicts five cloud deployment models offered by cloud providers and includes descriptions of the environments represented by each deployment model. Also depicted are five cloud service models and descriptions of the associated services offered with each service model.

Table 1

Cloud Deployment Models and Cloud Service Models

Cloud Deployment and Service Models (Multiple Sources)	
Baun, 2011; Bond, 2015; Brandis, Dzombeta, & Haufe, 2013; Garg, Versteeg, & Buyya, 2012; NIST, 2011; Parekh, 2013	
Cloud Deployment Models	**Description / /Definition**
Private Cloud	Infrastructure provisions for specific use by a single user.
Community Cloud	Provisions specific use by the community concerned with shared services.
Public Cloud	Provisioned for open use, multi-tenancy with shared resources.
Hybrid Cloud	Consists of two or more infrastructures bound by standard or proprietary technology enabling data and application portability.
Virtual Private Cloud VPC	Basically a public cloud provider that offers a unique compartment and subnetwork environment. A private subcloud within a larger cloud can provide greater security and some customization (Bond, p. 123-24).

(Baun, 2011; Bond, 2015; Brandis, Dzombeta, & Haufe, 2013; CSCC, 2015; Garg, Versteeg, & Buyya, 2012; NIST, 2011; Parekh, 2013)	
Cloud Service Models	**Description / /Definition**
Humans-as-a-Service (HuaaS)	Crowdsourcing: A group of human resources use the Internet to perform tasks of varying complexity and scope for a customer.
Infrastructure-as-a-Service (IaaS)	Infrastructure services: Offers the highest flexibility and the customer is responsible for security. "Open cloud architectures allow [customers] to add a number of third-party services, thus forming the basis of an ecosystem of providers who offer added value, such as for cloud application monitoring and management" (Baun, p. 66-67).
Platform-as-a-Service (PaaS)	Integrated development environment: Makes it easy to set up, operate, and scale a relational database in the cloud. The PaaS components form the framework layer.
Software-as-a-Service (SaaS)	Applications and services: Components can be found on the application layer. In cloud environments, application virtualization is an important foundation.
Everything-as-a-Service (XaaS)	Everything-as-a-Service: It comprises all of the four main service models: HuaaS, IaaS, PaaS, and SaaS.

Security risks and challenges with cloud computing

Security risks and threats are inherent with cloud deployments (CSCC, 2015; Parekh & Sridaran, 2013). Reducing security risks is critical for organizations that have data stored and transmitted remotely (Rao & Selvamani, 2015). The failure of an organization to provide

security protection for resources deployed to the cloud could potentially result in increased costs and possible business losses (CSCC, 2015). Rao and Selvamani (2015) assert that data protection in the cloud is extremely important and that a framework must be in place that addresses data security by protecting data against unauthorized users. The framework should include best practices policies for data encryption and password protection and authentication (CSCC, 2015; Parekh & Sridaran, 2013; Rao & Selvamani, 2015; Robinson, Valeri, Cave, Starkey, Graux, Creese, & Hopkins, 2011; Sood, 2012). Without adequate security practices unauthorized users may access sensitive data very easily (Parekh & Sridaran, 2013).

Security concerns arise with the loss of governance rights when a customer gives control to the cloud service provider for issues that could impact security, but the cloud service provider fails to deliver resolutions to the issues, thus creating gaps in security defenses (CSCC, 2015). A data lock from application and/or service provider not allowing users to extract and move data can create uncertainties in ability to switch provider, asset accountability and compliance to ensure secure controls are in place (Robinson, Valeri, Cave, Starkey, Graux, Creese, & Hopkins, 2011).

Best practices for governance in the cloud

Establishing best practices for data governance in the cloud helps to address security concerns (Bond, 2015). Best practices provide a framework for planning and deploying to a secure cloud (Bond, 2015; Brandis, Dzombeta, & Haufe, 2013; Rebollo, Mellado, Fernández-Medina, & Mouratidis, 2015). A holistic governance framework approach allows the integration of (a) enterprise architecture management (EAM), (b) IT governance, and (c) cloud computing (Brandis, Dzombeta, & Haufe, 2013). In order to capture the complexities of IT, a governance

model must take a holistic view that builds on current best practices from other areas, such as law, economics and technology (Brandis, Dzombeta, & Haufe, 2013).

There is widespread recognition of the need for data governance in the cloud to mitigate security risks (Bond, 2015; Rebollo, Mellado, Fernández-Medina, & Mouratidis, 2015; Suicimezov, & Georgescu, 2014). To address cloud security concerns, Rebollo, Mellado, Fernández-Medina, and Mouratidis (2015) propose ISGcloud, an option for a security governance framework that is built upon security guidelines and industry standards (Rebollo et al., p. 47). When implemented according to industry standards, IT governance establishes a solid set of best practices and rules for companies migrating to cloud computing (Suicimezov, & Georgescu, 2014). At a minimum, the same level of security should be maintained for assets in the cloud as exists in the traditional IT environment (CSCC, 2015, p. 7). Suicimezov and Georgescu (2014) note that a cloud computing environment can be made very secure if a strong governance framework is applied.

Table 2 depicts tools and techniques available for governance in the cloud.

Table 2

Tools and Techniques for Governance in the Cloud

Best Practices for Governance in the Cloud	
(Hill, Hirsch, Lake, & Moshiri, 2013)	
Tools and Techniques	**Description / Definition**
Capability Maturity Model (CMM)	Carnegie Mellon's Software Engineering Institute Capability Maturity Model (SEI-CMM) is a methodology used to measure the maturity level of an organization and refers to "optimization and continuous improvement" (Hill et al., 2013, p. 244) of

	software processes. It is one of the tools that supports the "planning process to develop a cloud roadmap" (Hill et al., 2013, p. 244) in aligning business and IT objectives (Hill et al., 2013).
Critical Success Factors (CSF) Analysis	Provides guidance for a successful outcome when deploying to the cloud.
Governance and Risk Analysis	Governance and risk analysis are techniques recommended to "assist in the planning process to develop a cloud roadmap" " (Hill et al., 2013, p. 244). According to CSCC (2015) a cloud security assessment should include a security step to "ensure effective governance, risk and compliance processes exist" (CSCC, p. 26). The assessment should include a litany of questions, such as information relating to security, privacy, compliance, regulations, and appropriate governance. Hill et al. (2013) assert that performing this analysis will ensure that the organization has met the business-IT objectives (Hill et al., p. 244).
Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis	The analysis helps to identify if the cloud should be taken serious. It helps to bring some clarity to the organization's strategic business decisions about IT investments. Using the analysis can create a matrix with cloud service and cloud deployment models that aligns with the business strategies. It is important to understand the complexity of the cloud in order to be able to meet cloud challenges.

Value Chain Analysis	Identify "if cloud could improve efficiency or effectiveness or provide competitive advantage through linkages within the internal and external value chains" (Hill et al., 2013, p. 248).

(Brandis, Dzombeta, & Haufe, 2013)	
Cloud Computing Measurements	**Description / Definition**
Information Technology Infrastructure Library (ITIL)	Designed to standardize practices that align with IT services to meet business requirements.
Control Objectives for Information and Related Technology (COBIT)	Designed as a business framework to manage IT governance.

In summary, the references included in this study define the need for cloud computing. Organizations are challenged with risks when deploying to a cloud service, including risks related to security (CSCC, 2015; Parekh & Sridaran, 2013). Implementing a well-defined governance framework provides the opportunity to define who will establish security, policies, and system accreditation, which are integral to maintaining a secure and safe cloud environment (Bond, 2015, p. 231). As a result, cloud computing becomes compliant, ethical, and manageable (Shackleford, 2010, p.5).

References

Baun, C. (2011). *Cloud computing web-based dynamic IT services*. New York, NY: Springer. ISBN: 978-3-642-20916-1, e-ISBN: 978-3-642-20917-8. doi: 10.1007/978-3-642-20917-8

Bertolucci, J. (2014, February 3). Data governance plans: Many companies don't have one. Retrieved from InformationWeek website: http://www.informationweek.com/big-data/big-data-analytics/data-governance-plans-many-companies-dont-have-one/d/d-id/1113678

Bond, J. (2015). *The enterprise cloud: Best practices for transforming legacy IT* (First ed.). Sebastopol, CA: O'Reilly Media. ISBN-13: 978-1491907627

Brandis, K., Dzombeta, S., & Haufe, K. (2013). Towards a framework for governance architecture management in cloud environments: A semantic perspective. *Future Generation Computer Systems*, *32*, 274-281. doi: 10.1016/j.future.2013.09.022

Cloud Standards Customer Council (2015, March). *Security for Cloud Computing Ten Steps to Ensure Success Version 2.0*. Retrieved from: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Creswell, J. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: SAGE Publications. ISBN-13: 978-1452226101

Garg, S., Versteeg, S., & Buyya, R. (2012). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, *29*(4). doi: 10.1016/j.future.2012.06.006

Hill, R., Hirsch, L., Lake, P., & Moshiri, S. (2013). *Guide to cloud computing: Principles and practice* (Computer communications and networks). Heidelberg: Springer. ISBN: 9781447146025

NIST Information Technology Laboratory (2011a, October 25). *Final Version of NIST Cloud Computing Definition Published.* NIST (Publication No. 800-145). doi: 10.6028/NIST.SP.800-145

NIST Information Technology Laboratory (2011b, December). *Guidelines on Security and Privacy in Public Cloud Computing.* NIST (Publication No. 800-144). doi: 10.6028/NIST.SP.800-144

Parekh, D. & Sridaran, R. (2013). An analysis of security challenges in cloud computing. *International Journal of Advanced Computer Science and Applications, 4*(1) doi: http://dx.doi.org/10.14569/IJACSA.2013.040106

Prasad, A., Green, P., & Heales, J. (2014). On governance structures for the cloud computing services and assessing their effectiveness. *International Journal of Accounting Information Systems, 15*(4), 335-356. doi: 10.1016/j.accinf.2014.05.005

Prigge, M. (Dec. 19, 2011). Information overload: Architectural rule no. 1: Segregate everything. Retrieved from *InfoWorld, Inc.* website: http://www.infoworld.com/article/2618860/infrastructure-storage/architectural-rule-no--1--segregate-everything.html

Privacy Technical Assistance Center (2011, December). Data governance and stewardship. Retrieved from *U.S. Department of Education* website: http://ptac.ed.gov/sites/default/files/issue-brief-data-governance-and-stewardship.pdf

Pruitt, M. (2013,June 18). Security best practices for IT project managers. Retrieved from *SANS Institute* website: https://www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257

Rai, R., Sahoo, G., & Mehfuz, S. (2015). Exploring the factors influencing the cloud computing adoption: A systematic study on cloud migration. *SpringerPlus, 4*, 197. doi: 10.1186/s40064-015-0962-2

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science, 48,* 204-209. doi: 10.1016/j.procs.2015.04.171

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58,* 44-57. doi: 10.1016/j.infsof.2014.10.003

Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., & Hopkins, P. (2011). *The Cloud - Understanding the Security, Privacy and Trust Challenges. RAND Corporation.* ISBN: 9780833059604.

Seiner, R. S. (2014). *Non-invasive data governance.* Basking Ridge, NJ: Technics Publications, L.L.C.

Shackleford, D. (2010, August). Cloud security and compliance: A primer. Retrieved from *SANS Institute* website: https://www.sans.org/reading-room/whitepapers/analyst/cloud-security-compliance-primer-34910

Sood, S. (2012). A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications, 35*(6), 1831-1838. doi: 10.1016/j.jnca.2012.07.007

Suicimezov, N. & Georgescu, M. (2014). IT Governance in Cloud. *Procedia Economics and Finance, 15,* 830-835. doi: 10.1016/S2212-5671(14)00531-0

University of Florida Center for Public Issues Education (2014), *Evaluating Information Sources.* Retrieved from http://ce.uoregon.edu/aim/Capstone1Perm/evaluateinfo.pdf