Securing Cloud Computing Through IT Governance

[1]Salman M. Faizi and [2]Shawon Rahman, Ph.D.

[1]Information Assurance and Cyber security Program, Capella University,
Minneapolis, Minnesota, USA
[2]Associate Professor, Dept. of Computer Science & Engineering, University of Hawaii-Hilo,
200 W. Kawili Street, Hilo, HI 96720, USA

Abstract—Lack of alignment between information technology (IT) and the business is a problem facing many organizations. Most organizations, today, fundamentally depend on IT. When IT and the business are aligned in an organization, IT delivers what the business needs and the business is able to deliver what the market needs. IT has become a strategic function for most organizations, and it is imperative that IT and business are aligned. IT governance is one of the most powerful ways to achieve IT to business alignment. Furthermore, as the use of cloud computing for delivering IT functions becomes pervasive, organizations using cloud computing must effectively apply IT governance to it. While cloud computing presents tremendous opportunities, it comes with risks as well. Information security is one of the top risks in cloud computing. Thus, IT governance must be applied to cloud computing information security to help manage the risks associated with cloud computing information security. This study advances knowledge by extending IT governance to cloud computing and information security governance.

Keywords—Business alignment, cloud computing, cloud computing security, information security, IT governance.

I.INTRODUCTION

THIS paper presents a study on implementing information technology (IT) governance policies and processes to cloud computing information security. IT governance is defined as a set of mechanisms designed to encourage behaviors that are consistent with the mission, strategy, and culture of the organization; the mechanisms address various matters related to IT such as decision processes, policies, the assignment of accountabilities, and participation rights for the stakeholder [1, 2]. From the preceding definition, it is evident that IT policies and processes such as information security fall within the domain of IT governance. IT governance also applies governance to information security. Moreover, as organizations move from on-premises computing to cloud computing, it is imperative that they adopt information security governance to the essential characteristics of cloud computing. Lack of effective IT governance is one of the barriers to cloud computing adoption [3]. It is vital that organizations consider a sound IT governance framework as they adopt cloud computing.

In organizations today, the alignment of IT operations with the business strategies and management of IT risks are imperative. IT governance is a way to accomplish IT-Business alignment; furthermore, according to the research on the subject, the most important purpose of IT governance is to align IT operations of an organization with its business strategies [4]. IT-Business alignment ensures that IT operations deliver and operate in a way that supports the business strategies and the vision of the organization. IT governance is the management of an organization's IT and business processes in such a way that IT and business are integrated; however, aligning IT operations with business strategies is not easy [4]. In addition to IT-Business alignment, the literature on information system (IS) research emphasizes management of IT-related risks. IT governance provides a structure of processes and relationships to attain the goals of an enterprise by adding value while balancing risks with a return over IT investments [5]. Thus, the two main aspects of IT governance, emphasized by researchers, are to align IT to business and to manage risk, and the alignment and risk management lead to an organization that is better positioned to serve the market needs.

IT governance must be effective. Studies have shown that the effectiveness of IT governance relies on the existence of three mechanisms: (a) an IT steering committee, (b) the involvement of senior management in IT, and (c) corporate performance measurement systems [5]. The three mechanisms of IT governance allow organizations to build effective IT governance to help realize business success through alignment of their IT operations with business strategies. Researchers have long established that IT-Business strategic alignment is key to business success [6]. One of the primary goals of IT governance should be making decisions for investment and utilization of IT functions by addressing the question of how an organization should make investments to its IT for maximum benefit to the entire organization. IT governance applies to an organization in various ways such as principle,

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

policy, process, or organization specific activities [7]. Effective IT governance is in the interest of an organization. Furthermore, IT governance driven IT-Business alignment even increases the status of the CIO. When CIOs have used IT governance to ensure alignment between business and IT, IT governance has been pivotal for the CIOs to increase their status within an organization [8]. IT governance not only helps the IT leadership gain prominence within the organization but also positively moderates business performance of the organization. Effective IT governance provides efficient mechanisms to achieve alignment between IT and business and to allocate their resources such as people, processes, and technology to IT investments.

II. BACKGROUND OF THE STUDY

One area where organizations must apply governance to allocate IT resources is the area of information security. Many organizations today find that information has grown to become their lifeblood because information is used to drive most business processes for employees of all levels [2]. Furthermore, information is not only used as an enabler but also used to gain a competitive advantage in the marketplace and to drive business value chain. Information has become an essential asset for most organizations, and similar to all other critical assets, information needs adequate protection to prevent theft or intentional or unintentional misuse of information.

Information security is not just an implementation of technology; there are other elements involved. Information security consists of technology, processes, and people [9]. Technical measures such as passwords, firewalls, network monitoring, and the likes are not enough to counter threats to information; therefore, organizations must consider a combination of measures to protect their information against theft and harm whether intentional or unintentional [9]. Processes include things like user registration, deregistration, and organizations must consider people aspects such as compliance, training, and leadership by example instead of just deploying a solution that protects information from theft, loss, or misuse. The way to achieve the security objectives of protecting information through people, process, and technology is for information security to have its governance framework.

Moreover, there are compliance reasons to adopt IT governance. Most modern corporate governance rules as well as some country laws make the Board and specifically the CEO responsible for protecting sensitive information [10, 11]. Placing such a responsibility on the board of directors and the CEO of an enterprise highlights the importance of protection of private and business-critical information. In some cases, there is a regulatory obligation to safeguard information, and the violation of the responsibility can have punitive repercussions for an organization and its executives. Consequently, the boards and the CEOs have a vested interest in using governance to efficiently protect their organization's information in both the existing and new models of delivering IT services to customers and employees.

One relatively new model for delivering IT services is cloud computing, and it needs a framework for IT governance intended to secure an organization's information when stored in the model of cloud computing. Given the maturity and development of cloud computing, public cloud computing services are a natural choice for enterprises to achieve greater cost savings and resource utilization; however, there are worries about the security of cloud computing services [12]. Moreover, enterprise data security and privacy issues have become one of the main factors that have hindered the popularity of cloud computing [12]. Thus, cloud computing will benefit from a framework of IT governance and the associated best practices.

III. CLOUD COMPUTING

Cloud computing is a relatively recent entrant onto the landscape of information technology, and it stands to fundamentally shift how organizations deliver information technology services to their employees, customers, and partners. The following diagram provides a conceptual overview of cloud computing showing its various elements.

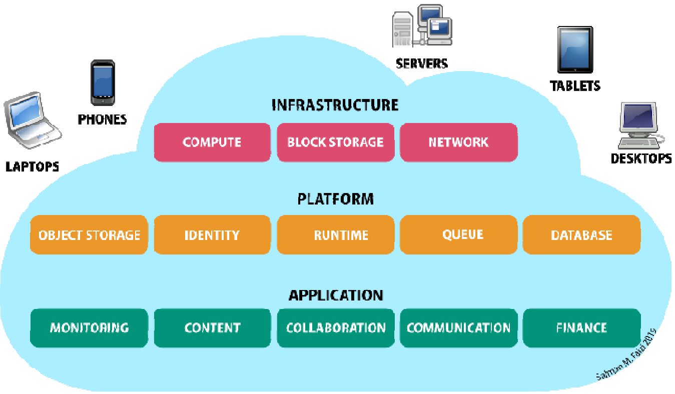


Figure 1. Cloud Computing

Today, cloud computing has become a global trend, and it has drawn attention from both the business world and the academic community [13]. Such technology provides a paradigm shift in the field of information technology. Thus, increasingly information assets will be stored, retrieved, and processed on cloud computing platforms.

Numerous surveys show that a substantial majority of organizations are either already using cloud computing or plan to adopt it in the near future[14]. The characteristics of cloud computing are already impacting IT organizations. Right Scale Inc. [15] reported that companies not only already process most of their computational workload using cloud computing, but they are planning on increasing their use of cloud computing. The report also indicated that among the respondents to its survey, public cloud adoption increased to 92% in 2018 from 89% in 2017. Such an explosive growth in the adoption of cloud computing points to its importance.

The cloud computing adoption is just as applicable to the government sector as it is to the private sector. Cloud computing has received attention at all levels of the US government since, according to the Brookings Institution, government agencies can save 25-50% by migrating to the cloud [16]. Similarly, the European Commission is promoting the use of cloud computing among the government sector in Europe as part of the "Digital Agenda for Europe" [17]. In the developing economies, cloud computing is a vehicle for the realization of electronic government or e-government [18]. Both private and public sectors are accelerating adoption of cloud computing. Consequently, cloud computing is just as important to the private sector as it is to the public sector.

A. Definition of Cloud Computing

Before proceeding further, it is helpful to define cloud computing. The cloud computing literature contains several definitions of cloud computing, and the definitions do not seem to cover all the features of the cloud. There is confusion about the definition of cloud computing [19]. It is important to define cloud computing because the definition will help contain the scope of the discussion for this paper. Efforts have been made to standardize the definition of cloud computing. One such standardized definition is from Mell and Grance [20] of the National Institute of Standards and Technology (NIST). The NIST definition of cloud computing is a reasonable definition [21]. The NIST [20] defines cloud computing as follows:

> Cloud computing is 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models. (p. 2).

B. The Essential Characteristics of Cloud Computing

The above definition of cloud computing leads to the five essential characteristics of cloud computing. These characteristics are (a) on-demand self-service, (b) broad network access, (c) resource pooling, (d) rapid elasticity, and (e) measured service. Next, we define each one of these characteristics per the definitions of Mell and Grance [20] and Stieninger and Nedbal [19].

The first characteristic is on-demand self-service which means a cloud computing consumer can solely provision computing features, such as server time and network storage, as desired automatically without needing human interaction with a cloud computing service provider. The cloud computing customers can adjust the demand of cloud computing services as their needs change. An essential characteristic of cloud computing is on-demand self-service.

The second characteristic of cloud computing is broad network access which means that cloud computing capabilities are available over the network and are accessible through standard mechanisms employed by varied thin or thick client platforms such as mobile phones, tablets, laptops, workstations, and other similar clients. Broad network access is one of the highly attractive features of cloud computing and is deemed essential.

The third characteristic of cloud computing is resource pooling which implies that the cloud computing provider's computing resources are pooled to serve multiple consumers using a multi-tenant model. Multitenancy in cloud computing refers to an architecture that allows each tenant or customer to keep his or her data separate and invisible to other tenants. In the multitenancy model different physical and virtual resources are dynamically assigned and reassigned according to consumer demand at a given moment. This aspect provides a sense of location independence such that the customer normally does not have any control or knowledge over the exact location of the cloud computing provided resources. However, when provisioning a cloud computing service, the customer may be able to specify location at a higher level of abstraction. The customer can specify country, state, region, or data center to control the general location of where the hardware and associated services will originate. Examples of cloud computing resources are storage, processing, virtual network, memory, and network bandwidth. Resource pooling is an essential characteristic of cloud computing.

The fourth characteristic of cloud computing is rapid elasticity which means that cloud computing capabilities can be dynamically provisioned and released to scale rapidly per the increasing and decreasing demand. In some cases, elasticity can occur automatically based on rules predefined by the customer. Elasticity is important because, to the cloud computing customer, the capacity available for provisioning often appears to be unlimited. The customer can allocate capacity in almost any quantity at any time. A crucial characteristic of cloud computing is fast elasticity.

The fifth and final characteristic of cloud computing is measured service which suggests that cloud computing systems use metering capabilities and associated metrics to automatically regulate and optimize resource usage at some level of abstraction appropriate to the type of service. Type of service includes storage, processing, bandwidth, and active user accounts and other similar types. The consumer can monitor, control, and obtain reports on resource usage. Such monitoring provides transparency for both the provider and consumer of the utilized service. A vital characteristic of cloud computing is measured service.

Therefore, due to the unique characteristics of cloud computing, information stored in cloud computing is susceptible to additional security threats that traditional on-premises computing does not face. The public cloud computing services have their specific security issues, which are different from traditional IT technology [12]. The organizations considering cloud computing for their IT needs must first understand the factors that lead to cloud adoption.

The literature on cloud computing reports several challenges towards the adoption of cloud computing. Stieninger, et al. [22] investigated the factors that are important contributors to the attitude towards cloud computing adoption. They found that compatibility, relative advantage, security and trust, as well as a lower level of complexity contribute positively to attitude towards cloud adoption. Additionally, Right Scale Inc. [15] found that the top challenges to cloud computing in 2018 reported by the respondents to its survey are security and spend; 77% considered security a challenge while 76% saw cloud spend a challenge, and enterprises experienced more challenges overall than small and medium businesses. Reports such as these point to the need for a structured control mechanism, such as IT governance, towards cloud computing. This paper will limit the application of IT governance to security.

Cloud Service Delivery Models. Before applying the IT governance framework, it is helpful to look at different service models that are available for cloud computing. Looking at different models allows customization of the information security governance for each model of the cloud computing service. Three service models are available for cloud computing. These models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [20, 23]. The three service models need not be orthogonal in a given deployment, and a given deployment can contain one or more of the service delivery models. Each of these service models ultimately uses cloud computing infrastructure which is a collection of hardware and software to enable the five essential characteristics discussed above [20]. The cloud infrastructure is both the physical and the abstraction layer of cloud computing where physical layer is the hardware on which cloud computing runs, and the abstraction layer consists of software that manages the cloud and its essential characteristics [20]. Understanding the service models and the infrastructure is important to implement an IT governance framework for information security. The diagram below, adopted from Schouten [24], shows the three service delivery models and the management responsibility of the customer compared to the management responsibility of the cloud vendor.

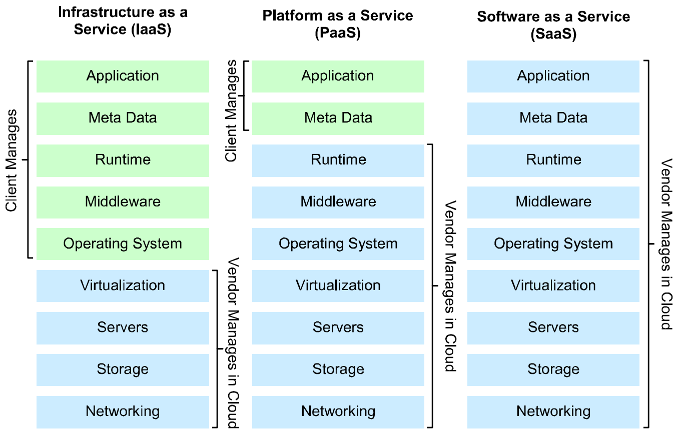


Figure 2. *Cloud Service Delivery Models*

The diagram above also shows the amount of control the client has in each cloud service delivery model. On-premises computing provides enterprises complete control over assets and information. When addressing information security in cloud computing, the main difference is an enterprise's loss of control, and therefore, loss of governance it has over assets and information [25]. Thus, governing information security to guard against the security threats in a cloud computing environment requires controlling the parts of the cloud computing environment under client control and collaboration with the cloud computing vendor to manage the parts that the vendor manages.

IV. SECURITY THREATS IN CLOUD COMPUTING

This section discusses major cloud computing security concerns. Similar to traditional on-premises computing, cloud computing presents security threats. The diagram below shows various areas from where cloud security threats can emerge.

Four categories represent the major security concerns in cloud computing: (a) software security, (b) infrastructure security, (c) storage security, and (d) network security [26]. Next, we discuss each of these categories of major security concerns.

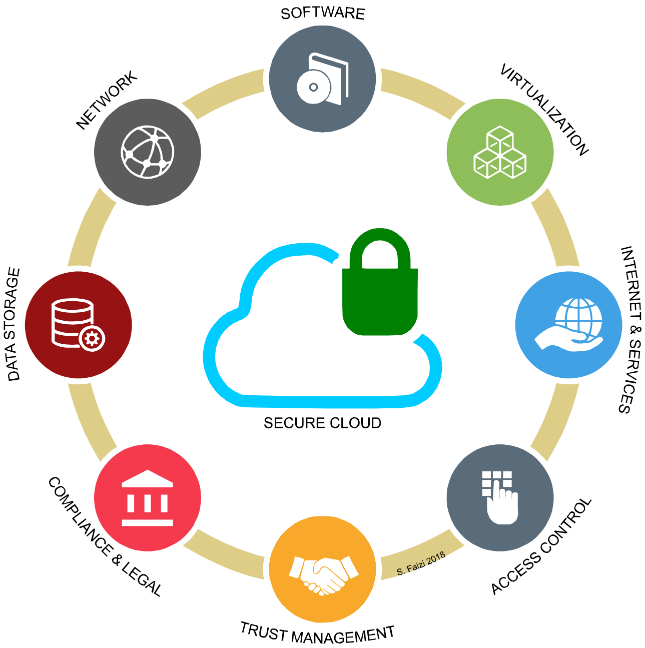


Figure 3. Cloud Computing Security Domains

A. Software Security

The software security risk is due to unaddressed security during development. Software applications face unique challenges and security threats. In 2009, a study found that cyber-attacks on internet web applications made up more than 60% of the total attacks on the internet [27]. However, things have only gotten worse in these areas. Cisco Systems [28] reported that in 2017, 64% of all denial of service attacks targeted applications. The attackers specifically target applications because the network layer has increased protection leaving less room for exploitation. The increased attacks on the applications need the increased protection of the application by removing security flaws in them.

The top ten security attacks experienced by applications include injection, broken authentication, sensitive data exposure, XML external entities (XXE), broken access control, security misconfiguration, cross-site scripting (XSS), insecure deserialization, using components with known vulnerabilities, and insufficient logging and monitoring [29]. No stage of software development is immune from exposure to security flaws. The OWASP Foundation [27] states that security flaws can be injected into the software during any stage of the software development lifecycle. Security flaws can result during security requirements definition, conceptual design creation, following poor coding practices, improperly deploying software, or introducing a security flaw during maintenance or updating. Thus, it follows that policies, processes, and procedures must cover all phases of software development for including security.

Often, software developers do not comply with secure programming practices. Many software application security flaws result due to the developer's failure to follow secure coding practices [30]. It is much more cost effective to prevent security flaws in an application than to cure them later. The view remains among software developers that security should be added after the development of the application ends. Even during training in software development curricula in universities, secure coding practices are taught as an elective towards the end of the educational program, and this practice further reinforces the view that software security is a feature that is added later [31]. A way to overcome this mentality is to provide policies, procedures, and processes for increasing secure software development. For example, a policy could require software developers to use statistic software analysis tools which can detect many vulnerabilities in the software code [30]. The management team can require software developers to use such tools and provide them training to properly configure them for effective detection of application security flaws.

B. Infrastructure Security

Infrastructure security applies to both virtual and physical infrastructure. The objective of infrastructure security to establish trust in the infrastructure [26]. Infrastructure is the foundational element in cloud computing, and it consists of physical and virtual resources. Virtual resources include virtual machines (VMs) that provide for the movement, storing, processing, and analysis of data in cloud computing. Multiple VMs can run on a single physical server to enable multitenancy. VMs are vulnerable to security risks and pose a threat to the security and privacy of cloud computing [32]. An erroneous deployment of a VM can result in a lack of isolation between other VMs on the same server leading to data leakage and cross-VMs attacks [26]. Specific VM attacks can compromise customer data. Some VM attacks include (a) a cross-VM side channel attack, which can allow a hacker to extract cryptographic keys, resource usage, and other information, (b) VM creation attacks, where malicious code is placed in VM to be replicated to other VMs at creation time, (c) VM migration and rollback attacks, where an attacker exploits VM's vulnerability during transfer between physical machines, and (d) VM scheduler based attacks occur when an attacker attempts to steal resources by exploiting the VM scheduler [33]. Additionally, attackers can exploit VM

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

monitoring tools used to monitor VMs due to their nature of being a central control point [26]. VMs are part of infrastructure security, and they pose a security risk to a cloud computing environment.

There are other security risks present in the category of infrastructure security. Electronic access control systems used to negotiate client authentication via the federation protocol of Security Assertion Mark-up Language (SAML) which contains authentication credentials [34]. In this case, an attacker can eavesdrop on a message even if it is digitally signed allowing an attacker to target random machines while masquerading as legitimate users. Furthermore, a simple network management protocol (SNMP) server, which is used to collect data from various devices, is susceptible to attacks given the cryptographic design of SNMP [26]. The vulnerabilities in the infrastructure expose cloud computing to severe security risks. Thus, it is critical that organizations using cloud computing verify that the infrastructure is secure.

C. Storage Security

Cloud computing deals extensively with data; data are transferred, processed, and stored in the cloud. Global data center traffic is growing exponentially and is expected to reach 10.4 zettabytes by 2019 with 83% of the data coming from the cloud [35]. Such data quantities in the cloud require storage security. Since cloud computing customers are physically separated from their data, they experience a lack of control [32]. Thus it is important that steps are taken to ensure storage security in cloud computing.

Additionally, cloud service providers store data in their data centers in a highly redundant fashion, and while the redundancy provides higher availability of the data, it also gives hackers an additional opportunity to steal sensitive data [19]. An attacker may steal data in several ways, but we consider two types of data storage attacks. The two data storage attacks are (a) data scavenging and (b) data deduplication [33]. Data scavenging occurs during data deletion which marks data as deleted but data are not completely removed from the physical storage devices; consequently, an attacker can steal data that is not completely removed from the physical storage devices. Chandna, et al. [36] describe symmetric key cryptography as an effective countermeasure against data scavenging. The next data storage attack is data deduplication. Data deduplication allows for minimizing storage and bandwidth requirement, and it makes it possible to identify files and their content. An attacker can create a communication channel to steal the content of the files being deduplicated. Both inside and outside adversaries can employ data deduplication as a means to mount a storage attack [35].

Insiders can cause data breaches since the cloud providers typically make data available to the insiders unencrypted, and insiders can exploit the data either erroneously or maliciously.

Microsoft Azure [37] attempts to protect data from insider adversaries by severely limiting the duration for which an insider can access data storage and by providing supervision even for the short duration of time. Additionally, data loss can occur due to faults in the data storage service; for example, in 2013 an outage at Dropbox lasted over ten hours [35]. Apart from data loss caused by the failure of cloud computing storage service, a malicious insider can cause data loss intentionally to cause harm. Thus, data storage attack can occur due to the activities of the inside adversaries.

Similar to the insider adversaries, outsiders also pose serious security threats to data storage through data deduplication procedures. Shin, et al. [35] describe several methods that outsiders use to attack data through deduplication. Attackers use side channels to identify the presence of specific data and their content. Outsiders can gain unauthorized access to the data stored in cloud computing by exploiting the hash value sent to the cloud computing storage by the client-side deduplication systems. Outsiders can abuse cloud storage service by establishing covert channels to the outside world or using a content delivery network (CDN). Additionally, outsiders can mount attacks on the cloud computing storage by data poisoning which employs the data tags sent as part of data uploaded as search strings.

Countermeasures against storage attacks help organizations keep their data safe. Encryption of data during transfer, storage, and processing is an effective countermeasure to prevent theft and unauthorized access to the data [32]. Encryption ensures the safeguarding of the data by employing encryption keys. A public cloud such as Microsoft Azure, for example, provides a secure key vault to safeguard the encryption keys [38]. Cloud computing customers can use a secure key vault to keep their keys in a safe place to prevent the keys from falling into the wrong hands. Furthermore, frameworks such as C2Detector are effective in detecting covert back-channels [39]. Other countermeasures include managing insiders' access to customer data stored within cloud computing.

D. Network Security

Cloud computing components are interconnected via a network, and access to cloud computing from the outside world is a network. Attackers can exploit the vulnerabilities of the network to steal sensitive and private data; moreover, the network attacks fall into three categories [33]. The three main

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

categories of network attacks are (a) port scanning, (b) botnets, and (c) spoofing attacks. These three categories of attacks allow an attacker to exploit a range of vulnerabilities in the cloud computing network.

The first major type of network attack, port scanning, is when an attacker scans ports on a server to target vulnerabilities in the services running on the ports [32]. Port scanning can lead to denial of service. However, intrusion detection systems and firewalls can provide some level of protection against port scanning attacks [40]. Other methods to thwart denial of service attacks include a method Microsoft Azure uses to scrub traffic at the network edge before it reaches the critical services and customer servers [37]. While it may not be possible to prevent all port scanning attacks, organizations using cloud computing must take measures to guard against such attacks.

The second major type of network attack is the botnet attack which occurs when a botnet steals data from a host machine and transfers them to a remote bot-master. Botnet creates a command and control system where the bot-master communicates with several infected machines, serving as zombies, which in turn can allow a hacker access to the network inside a firewall. Command and control servers are centralized servers that send minimally sized commands to the zombies to steal sensitive data or to cause damage [41]. The botnet attacks can cause serious harm and may even be difficult to detect. Individual machines are infected with botnet software when they access the network via Wi-Fi in public places such as coffee shops, airports, and hotels [42]. The users of the target machine may not realize that a malicious software agent was installed on their machine, and then without realizing it, they bring the infected machine inside the corporate firewall. Protecting against botnet involves tracking the bot-master by intercepting the communication between the infected machines and the bot-master. Incidents involving botnets have caused large-scale damage. For example, the Ramnit botnet, which infected 3.2 million computers, was detected and removed in February 2015 but it appeared again soon afterward to attack banks and commercial operations in Canada, Australia, the United States, and Finland [43]. Botnets pose a serious threat to cloud computing, and the organizations adopting cloud computing must take measures to protect against them.

The third major type of network attack is the spoofing attack. A spoofing attack occurs when the attacker impersonates network entities to cause harm to the network [33]. The main objective of a spoofing attack is to steal sensitive data from the authorized user to attack the network hosts to spread malware or circumvent access control [44]. Some examples of spoof attacks are provided next. A domain name server (DNS) spoofing attack may direct all traffic to a DNS server to the attacker's system. Another example of a spoofing attack involves replacing the internet protocol (IP) address with a forged IP address in a network packet. For virtual machines, an address resolution protocol (ARP) attack can cause the attacker to intercept packets to other VMs. An intrusion detection system can protect against spoofing attacks [45]. All networks attacks have a potential of causing damage to cloud computing and organizations adopting cloud computing must be particularly vigilant against these attacks.

V. IT GOVERNANCE AND CLOUD COMPUTING

Cloud computing presents several potential benefits to organizations in both the private and public sector. However, there are risks associated with cloud computing that organizations must address [14]. Organizations must implement controls, such as IT governance, to address the risks and to ensure that IT and cloud computing adds business value. When IT operations are aligned with the business strategies, IT delivers business value. Over the past three decades studies have consistently found that Business to IT alignment is a persistent problem; however, IT governance is a way to achieve such an alignment [46]. Without the Business-IT alignment, IT cannot deliver what the business needs and the business cannot deliver what the customers need. The diagram below provides a visual image showing how the governance of information security in cloud computing leads to various benefits.

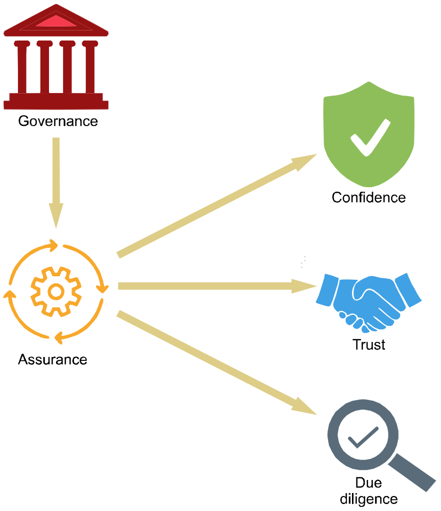


Figure 4. Cloud Computing Security Governance Outcomes

IT governance manages the risks associated with IT projects and practices [47]. Thus, in the case of cloud computing, IT governance is vital in achieving Business-IT alignment and

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

managing the traditional risks associated with the on-premises computing as well as the new risks associated with cloud computing.

IT governance plays an essential role in how organizations utilize information technology (IT). The two key objectives of IT governance are to guide the use of IT to supplement business value and to manage the risks associated with IT [14]. Traditionally, organizations applied IT governance to on-premises computing which included software that ran on computers located within the premises of the organizations. However, increasingly organizations are leveraging cloud computing for their IT needs to remain competitive and innovative [48]. Similar to on-premises computing, organizations can also apply IT governance to cloud computing since business value creation through IT and managing IT risks apply just as much to on-premises computing as it does to cloud computing.

IT governance is a complex undertaking, but, fortunately, there are guidelines developed by several IT governance bodies. Organizations can use these guidelines to supplement their existing IT governance; furthermore, the IT governance bodies have updated their guidelines to include IT governance of cloud computing because adoption of cloud computing often changes the risk profile of an organization [49]. Organizations can leverage the guidelines developed by the IT governance bodies to manage the new risk that comes with the adoption of cloud computing as well as other risks inherent to IT. Below is a list of some of the prominent IT governance bodies providing IT governance guidelines for cloud computing.

Table 1. Standards Bodies and Cloud Computing Security Governance

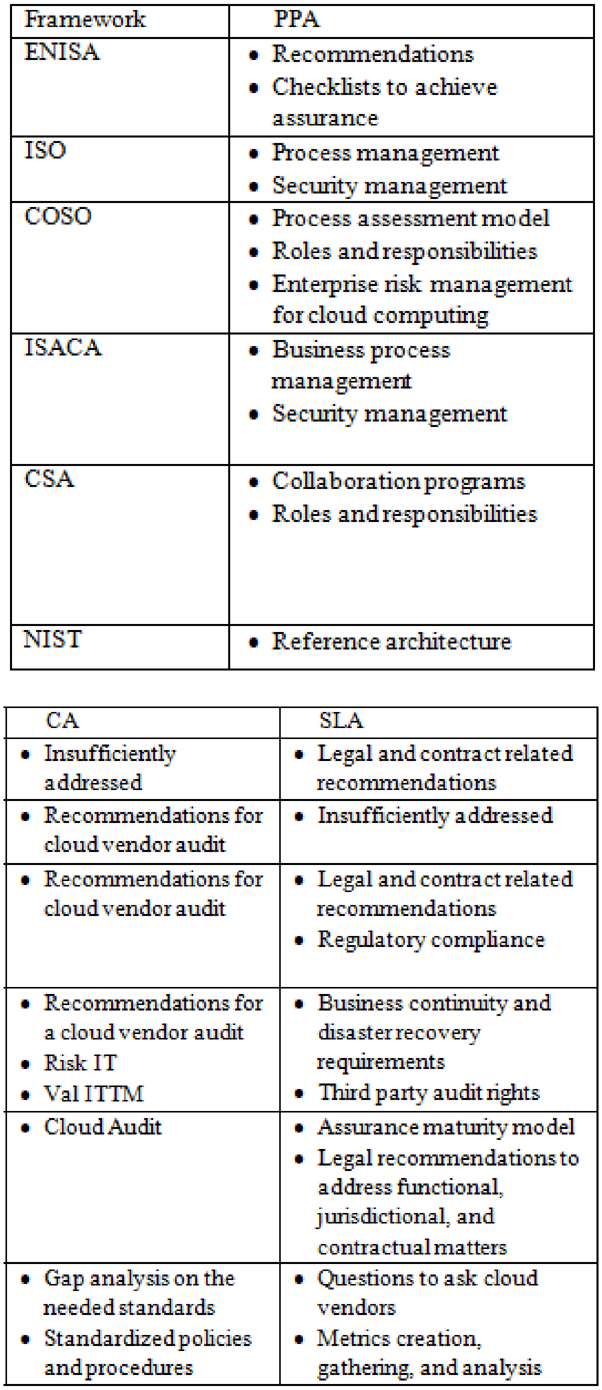
Standards Body	Description
The European Network and Information Security Agency (ENISA)	Provides a guide for assessing the security risks and benefits of using cloud computing. The risks are used as a starting point for the introduction of an information assurance framework based on the ISO 27000 family [50, 51].
International Standards Organization (ISO)	ISO provides consensus-based standards and guidelines for IT governance. Some ISO standards, such as ISO 27001, apply to cloud computing [52].
The Committee of Sponsoring Organizations of the Treadway Commission (COSO)	A combined initiative of five organizations from the private sector develops guidance that applies to IT governance [53].
Information Systems Audit and Control Association (ISACA)	Provides guidance, benchmarks, and tools for enterprises that use information systems. ISACA developed a well-known IT governance framework known as COBIT. COBIT can be applied to cloud computing [14]. ISACA [54] document "IT Control Objectives for Cloud Computing" describes the COBIT framework [14][54].
The Cloud Security Alliance (CSA)	Provides guidelines on security issues related to cloud computing including governance and enterprise risk management [55].
National Institute of Standards and Technology (NIST)	A governmental agency within the Federal government in the United States, NIST is a non-regulatory agency [56].

A comparison of the frameworks for information security governance in cloud computing, mentioned above, will help both the client and the vendor determine the right framework for them. Rebollo, et al. [25] provide guidance for comparing information security governance frameworks. They recommend that the comparison criteria should include policies and processes adoption (PPA), control and audit (CA), and service level agreement (SLA). A brief description of the three criteria is provided below.

When transitioning from on-premises computing to cloud computing, an enterprise should re-evaluate its security policies and processes in partnership with the cloud vendor. PPA represents the modifications to security policies and processes that enterprises transitioning from on-premises computing to cloud computing must make. CA represents the additional security controls that enterprises must establish to control the processes running in the cloud outside of their organizations. SLA contains the responsibilities and accountabilities between the cloud vendor and the cloud client. The table above contains a comparison of the frameworks along the criterion of Rebollo, et al. [25] and some of their data.

Since each cloud service delivery model offers a range of controls exercised by cloud clients and vendors, it is important to select the right cloud computing solutions. The CSA furnishes a method for evaluating the tolerance of cloud computing solutions for IT assets belonging to organizations [55]. ENISA [50] provides a model for selecting cloud computing solutions that are resilient and secure. ISACA [54] provides a four-step process to help decide the use of cloud computing: Service model, deployment model, and cloud provider or vendor. NIST [56] describes a decision framework for selecting a cloud computing solution which includes provisioning and managing of the cloud computing solution as well. Selecting a cloud computing solution is the first step in using cloud computing. Thus, governance models should include guidance for selecting a cloud computing solution.

Table 2. Comparison of Cloud Computing Security Governance Frameworks



Framework	PPA	CA	SLA
ENISA	• Recommendations • Checklists to achieve assurance	• Insufficiently addressed	• Legal and contract related recommendations
ISO	• Process management • Security management	• Recommendations for cloud vendor audit	• Insufficiently addressed
COSO	• Process assessment model • Roles and responsibilities • Enterprise risk management for cloud computing	• Recommendations for cloud vendor audit	• Legal and contract related recommendations • Regulatory compliance
ISACA	• Business process management • Security management	• Recommendations for a cloud vendor audit • Risk IT • Val ITTM	• Business continuity and disaster recovery requirements • Third party audit rights
CSA	• Collaboration programs • Roles and responsibilities	• Cloud Audit	• Assurance maturity model • Legal recommendations to address functional, jurisdictional, and contractual matters
NIST	• Reference architecture	• Gap analysis on the needed standards • Standardized policies and procedures	• Questions to ask cloud vendors • Metrics creation, gathering, and analysis

A. Extending Existing IT Governance to Cloud Computing

The standards bodies also provide general guidance for governance. Most of the standards bodies recommend adopting existing IT and security governance frameworks to cloud computing [14]. ISACA [54] describes the application of COBIT 4.1 to cloud computing. COSO [53] recommends applying the COSO ERM framework to cloud computing. ISO is developing a standard for cloud computing, and CSA has a reference architecture for a trusted cloud; both standards contain information security governance for cloud computing [14]. Applying the existing frameworks to cloud computing makes sense since the organizations would already be familiar with them and adding the cloud computing component would be a smaller net new addition compared to introducing a new governance framework. Thus, general guidance is to apply the existing IT and security frameworks to cloud computing.

In particular, organizations must emphasize (a) establishment of business goals for cloud computing and (b) roles and responsibilities for each level of management. First, establishing business goals and objectives for cloud computing will align cloud computing adoption with business value. ISACA [54] provides ways for organizations to come up with business goals and objectives for cloud computing. Often having an end goal provides a path to achieving that goal. Next, organizations must emphasize defining roles and responsibilities. Proper governance requires a clear definition of roles and responsibilities [14]. The roles and responsibilities can be an extension of the pre-existing roles and responsibilities that an organization uses for on-premises computing. A clear definition of roles and responsibilities will help eliminate gaps in understanding of authority, responsibilities, and accountabilities. COSO [53] provides a list of responsibilities for various managers, the board of directors, the chief executive officer, chief information officer, chief legal officer, and chief internal auditors. Additionally, COSO provides a list of considerations for managers and the board of directors when transitioning to cloud computing. Thus, a clear definition of roles and responsibilities adds to the effectiveness of information security governance of cloud computing.

B. Risk Management

The next general governance guideline is regarding risk management. Since cloud computing introduces additional risks for organizations, they must implement a risk management system [57]. The cloud computing governance standards provide several methods for capturing risk. ENISA [50] describes using SWOT analysis and a standards-based risk assessment process for evaluating risks associated with cloud computing security. CSA [55] has a framework to identify and evaluate risks in cloud computing that an organization faces. CSA has recommendations consisting of thirteen different domains for managing cloud computing risks. COSO [53] provides an enterprise risk management framework to help decide a response to risks. NIST [56] describes various risks associated with cloud computing security and provides recommendations on an appropriate risk response. A risk management system will not only help organizations determine a response to risks captured for cloud computing but also develop an effective risk management capability.

C. Compliance

Organizations must ensure compliance using contracts. ENISA [50] has a list of areas for organizations to consider when evaluating agreements with cloud vendors, and it provides a method for performing legal analysis as it relates to the usage of cloud computing. These agreements could include SLAs, memoranda of understanding, and end-user agreements. ENISA provides a three-step methodology for performing legal analysis, and it provides a list of six questions regarding an organization's usage of cloud computing.

D. Controls

Organizations can employ best practices for implementing controls in cloud computing. ISACA [54] provides control objectives based on COBIT 4.1 for cloud computing. CSA [55] provides a matrix of control objectives which is helpful in dealing with various requirements as they apply to cloud computing. These requirements may include HIPAA, ISO 27001, NIST SP800-53 R3, FedRAMP Security Controls, PCI DSS v2.0, and others [14]. Based on the industry an organization operates within, these requirements can be vital to their operations. ENISA [50] developed an assurance framework for cloud computing. The framework can help achieve control objectives.

The general governance guidelines provide organizations a means to adopt cloud computing to their specific business needs. Cloud computing contains additional information security risks when compared to traditional on-premises computing. Depending on the cloud service delivery model used, a client organization will need to adjust its governance depending on the control they are allowed on cloud computing resources. For example, IaaS provides more resources that a client must manage when compared to other cloud service delivery models. Organizations considering adopting cloud computing may find it challenging to address its additional risks. Various standards bodies, as identified above, provide best practices and guidance on where to start and what to consider.

VI. BEST PRACTICES IN IT GOVERNANCE

Researchers have highlighted several best practices in implementing governance. The best practices include involvement of business management, management of data quality, combined business and IT focus, and education of users and managers [58]. The best practices also include ethical and socially responsible corporate behavior, an effective corporate communications system, and corporate performance measurement. Taking these best practices one by one, we can further analyze and evaluate them.

First, the involvement of business management is crucial in the IT governance process. After all, it is business management that is ultimately the consumer of many services delivered by IT. The involvement of business management will ensure that the business can gain a competitive advantage through its investment in IT [7]. Alignment between IT and business will ensure that IT delivers what the business needs and that IT gets its requirements unambiguously stated from the business. Therefore, it is essential that business stakeholders be involved in the IT governance process.

Second, the management of data quality is an essential element required by any organization. Today, data contain the intellectual property, operational information, contractual obligations, and employee personal information to name a few. Managing and maintaining data quality is a key initiative for most organizations. Information technology governance must ensure that this crucial area is covered adequately in its practices. Organizations must categorize data according to its sensitivity, and data that is sensitive must be protected using mechanisms such as strong encryption while being transported to cloud computing as well as during storage. Therefore, the management of data quality is an essential element of information technology governance.

Third, the combined focus on business and IT is an important best practice of information technology governance. Organizations must understand IT's role as a service provider, not a servant; therefore, they must be inclusive of their IT as a true and valued partner [59]. A servant organization will do whatever it is asked to do while a service provider will be an equal partner in a mutually beneficial arrangement. A service provider enhances the business value chain while increasing its capabilities. Moreover, just like there is a business strategy, IT must also have a service strategy. Therefore, organizations must aspire to develop a combined focus of IT and business with both sides being equal partners.

Fourth, the education of users and managers is essential. Education is necessary because when it comes to providing quality, service education and training are essential [60]. The necessity of training is evident because training the users and managers lead to better understanding, better understanding leads to better governance, better governance leads to better firm performance, and better performance is what the employees, managers and the stockholders or owners of an organization want. Thus, it is crucial, to include training and education among the best practices of information technology governance.

Fifth, organizations must promote ethics. The presence of ethics and a culture of compliance in IT increases the overall effectiveness of IT governance [5]. Therefore, organizations should promote ethics and foster a culture of compliance. Sixth, corporate communication systems support is essential. The presence of corporate communication systems support significantly improves the overall success of IT governance [5]. Such a communication system allows for critical communication to take place, for ideas to permeate, and rich discussions to ensue. Consequently, organizations should invest in effective corporate communications systems.

The sixth, and final, best practice is a corporate performance measurement system. Research has shown that a corporate performance measurement system moderates the level of effective IT governance; however, the impact could even become negative given an incorrect use of the measurement system [5]. Organizations should deploy a performance measurement system and train the users on its proper use. Employing the best practices of IT governance and applying them to information security governance, organizations can significantly improve their IT governance implementation. IT governance will help best serve the organization.

VII. INFORMATION SECURITY GOVERNANCE

Organizations need information security to protect information. Since information security contains the triad of people, process, and technology, an information security governance framework must include all three elements [9]. Organizations must utilize a comprehensive approach to information security. A comprehensive approach is where the management of an organization develops and enforces information security mechanisms, such as policies and technical security procedures with which employees interact and include in their working procedures [9]. Technology such as passwords for access control, monitoring, firewalls, logging, and other similar equipment can only prevent a limited number of security incidences. A blend of measures is required to protect information by securing systems against harm; therefore, organizations must deploy processes to handle granting the user access to computing resources, training, leadership discipline, compliance to regulations and policies about information security [9]. Increasing the reach of information has required an increased focus on people and processes of the trifecta of people, process, and technology. IT governance is a way to focus on people and processes. Therefore, to increase the security of information, the principles of IT governance must be applied to develop information security governance focused on people, process, and technology.

The focus of information security has gradually moved from technology only to technology and governance. Initially, the discipline of information technology was limited to technical experts and technical solutions; however, gradually, technical experts determined that without management support, IT operations and business strategies could not align [9]. Thus, technical protection mechanisms have continued in parallel with management involvement. Organizations now include information security and its management in their organizational structure. Organizations can only address information security risks facing them with a governance framework containing adequate controls for their executives to direct employee behavior[9]. Consequently, a framework for information security governance allows organizations to address human behavior and accountability and the implementation of processes in addition to technology-based solutions.

An information security framework should include comprehensive security for an organization's information. Moreover, researchers have identified components that make up the comprehensive security of information, and how should the organizations go about implementing them [9]. Researchers have defined components of information security as the principles that enable assessing risk, implementing technical controls, creating an information security policy, and increasing information security awareness. These mechanisms can be included in an information security governance framework where the relationship between the mechanisms is established [9]. Thus, organizations can gain an understanding of the comprehensive requirements of information security through an information security governance framework and its components.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

VIII. INFORMATION SECURITY COMPONENTS FOR IT GOVERNANCE

This paper selects information security components from various existing information security approaches. Research has listed four well-established approaches aimed at addressing all aspects of information security governance. These approaches include the ISO 17799 standard, PROTECT (an acronym for Policies, Risks, Objectives, Technology, Execute, Compliance, and Team), Capability Maturity Model, and Information Security Architecture. Researchers, using these four approaches, have derived a comprehensive list of information security components. Implementing these information security components will alter the way people conduct their day-to-day IT-related activities for any given organization.

Furthermore, an important consideration is that while organizations do not change on their own, people change, and people, in turn, change an organization [9]. Organizations must pursue change management and take steps to protect the information assets of an organization due to change. Organizations must include information security components in such a way that employees can conduct their day-to-day responsibilities while successfully incorporating the information security governance. The information security components mentioned above are the basis for a sound information security governance framework. A successful information security governance framework must include these components [9]. These information security components are listed below.

Information security needs executive sponsorship. Executive sponsor can help obtain a commitment from an organization’s board and its management team [9]. With an active commitment, responsibility, and accountability of the board and the management team, information security becomes an active discussion in meetings of the board and the management team; therefore, this brings greater involvement of the board of directors, management team, and business process owners [61]. Increasingly, the directors and the executives of an organization are expected to protect shareholder value. This accountability to protect shareholder value applies to information assets just as it does to any other asset [61]. Such an understanding to protect information at the highest level of an organization leads to a better understanding that information security is essential for the organization’s survival. Therefore, leadership and governance are key to protecting the information asset of an organization.

IX. CONCLUSION

IT governance is a critical discipline to implement for an organization because it helps achieve alignment between IT operations and business strategies. Moreover, since most organizations rely on their IT systems to perform their day-to-day tasks, it is important that they protect IT systems against information theft or loss using information security governance. Furthermore, organizations must adapt their existing IT governance to include cloud computing. However, to successfully implement IT governance and information security governance, IT organizations must display leadership to promote information security governance, overcome user resistance, and employ a sound ethical framework that assures autonomy from external coercion, nonmaleficence to prevent harm to others, beneficence for providing a net benefit, and implement justice. It is only through these measures that IT governance and information security governance will shine. It is only through practices like the ones highlighted here, can the organization protect their information assets using proven principles of IT governance of information security.

REFERENCES

[1] A. Buchwald, N. Urbach, and F. Ahlemann, "Business value through controlled IT: Toward an integrated model of IT governance success and its impact," Journal of Information Technology, vol. 29, pp. 128-147, 2014.

[2] J. E. Mbowe, S. S. Msanjila, G. S. Oreku, and K. Kalegele, "On Development of Platform for Organization Security Threat Analytics and Management (POSTAM) Using Rule-Based Approach," Journal of Software Engineering and Applications, vol. 09, no. 12, pp. 601-623, 2016.

[3] H. Gangwar and H. Date, "Critical factors of cloud computing adoption in organizations: An empirical study," Global Business Review, vol. 17, pp. 886-904, 2016.

[4] B. C. M. A. Nathan, S. Hare, and P. C. M. A. Raju, "Establishing IT governance," (in English), Strategic Finance, vol. 99, no. 8, pp. 62-63, Feb 20182018-07-02 2018.

[5] S. Ali and P. Green, "Effective information technology (IT) governance mechanisms: An IT outsourcing perspective," Information Systems Frontiers, vol. 14, pp. 179-193, 2012.

[6] J. C. F. Tai, E. T. G. Wang, and H.-Y. Yeh, "A study of IS assets, IS ambidexterity, and IS alignment: the dynamic managerial capability perspective," Information & Management, 2018.

[7] K. Jairak and P. Praneetpolgrang, "Applying IT Governance Balanced Scorecard and Importance-performance Analysis for Providing IT Governance Strategy in University," Information Management & Computer Security, vol. 21, pp. 228-249, 2013.

[8] J. Magnusson and B. Bygstad, "Why I act differently: studying patterns of legitimation among CIOs through motive talk," Inf. Technol. People, vol. 26, pp. 265-282, 2013.

[9] A. A. Ettish, S. M. El-Gazzar, and R. A. Jacob, "Integrating internal control frameworks for effective corporate information technology governance," (in English), Journal of Information Systems and Technology Management: JISTEM, vol. 14, no. 3, pp. 361-370, Sep-DecSep-Dec 20172018-02-28 2017.

[10] R. v. Solms and S. H. B. v. Solms, "Information security governance: Due care," Computers & Security, vol. 25, pp. 494-497, 2006.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[11] R. V. Aguilera, W. Q. Judge, and S. A. Terjesen, "Corporate governance deviance," Academy of Management Review, Article vol. 43, no. 1, pp. 87-109, 2018.

[12] Y. C. Zhu, P. Liu, and J. T. Wang, "Enterprise data security research in public cloud computing," Applied Mechanics and Materials, vol. 198-199, pp. 435-438, 2012.

[13] M. Bayramusta and V. A. Nasir, "A fad or future of IT?: A comprehensive literature review on the cloud computing research," International Journal of Information Management, vol. 36, pp. 635-644, 2016.

[14] R. von Solms and M. Willett, "Cloud computing assurance – a review of literature guidance," (in English), Information and Computer Security, vol. 25, no. 1, pp. 26-46, 20172018-08-29 2017.

[15] RightScale Inc. (2018). RightScale 2018 state of the cloud report uncovers cloud adoption trends. Available: https://www.rightscale.com/press-releases/rightscale-2018-state-of-the-cloud-report

[16] J. L. Schnase et al., "MERRA Analytic Services: Meeting the Big Data challenges of climate science through cloud-enabled Climate Analytics-as-a-Service," Computers, Environment and Urban Systems, vol. 61, pp. 198-211, 2017.

[17] C. Feijóo, S. Ramos, C. Armuña, A. Arenal, and J.-L. Gómez-Barroso, "A study on the deployment of high-speed broadband networks in NUTS3 regions within the framework of digital agenda for Europe," Telecommunications Policy, 2017.

[18] F. Mohammed, O. Ibrahim, and N. Ithnin, "Factors influencing cloud computing adoption for e-government implementation in developing countries," (in English), Journal of Systems and Information Technology, vol. 18, no. 3, pp. 297-327, 20162018-09-30 2016.

[19] M. Stieninger and D. Nedbal, "Characteristics of Cloud Computing in the Business Context: A Systematic Literature Review," Global Journal of Flexible Systems Management, Article vol. 15, no. 1, pp. 59-68, 2014.

[20] P. Mell and T. Grance, "The NIST definition of cloud computing recommendations of the National Institute of Standards and Technology," NIST Special Publication, vol. 145, p. 7, 2011.

[21] A. Jula, E. Sundararajan, and Z. Othman, "Cloud computing service composition: A systematic literature review," Expert Systems with Applications, vol. 41, pp. 3809-3824, 2014.

[22] M. Stieninger, D. Nedbal, W. Wetzlinger, G. Wagner, and M. Erskine, "Factors influencing the organizational adoption of cloud computing: A survey among cloud workers," International Journal of Information Systems and Project Management, vol. 6, no. 1, pp. 5-23, 2018.

[23] O. Yigitbasioglu, "Modelling the intention to adopt cloud computing services: A transaction cost theory perspective," Australasian Journal of Information Systems, vol. 18, pp. 193-210, 2014.

[24] E. Schouten. (2014, 10/14/2018). Cloud computing defined: Characteristics & service levels. Available: https://www.ibm.com/blogs/cloud-computing/2014/01/31/cloud-computing-defined-characteristics-service-levels/

[25] O. Rebollo, D. Mellado, and E. Fernández-Medina, "A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment," Journal of Universal Computer Science, vol. 18, pp. 798-815, 2012.

[26] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," Journal of Network and Computer Applications, vol. 75, pp. 200-222, 2016.

[27] The OWASP Foundation, "OWASP Secure Coding Practices Quick Reference Guide," 2010.

[28] Cisco Systems, "Cisco Annual Cybersecurity Report,"Available: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

[29] The OWASP Foundation, "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks," 2017, Available: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

[30] J. Zhu, J. Xie, H. R. Lipford, and B. Chu, "Supporting secure programming in web applications through interactive static analysis," J Adv Res, vol. 5, no. 4, pp. 449-62, Jul 2014.

[31] M. Whitney, H. R. Lipford, B. Chu, and T. Thomas, "Embedding Secure Coding Instruction Into the IDE: Complementing Early and Intermediate CS Courses With ESIDE," Journal of Educational Computing Research, vol. 56, no. 3, pp. 415-438, 2017.

[32] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, pp. 88-115, 2017.

[33] M. A. A. Khan, "A survey of security issues for cloud computing," Journal of Network and Computer Applications, vol. 71, pp. 11-29, 2016.

[34] S. Iqbal et al., "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," Journal of Network and Computer Applications, vol. 74, pp. 98-120, 2016.

[35] Y. Shin, D. Koo, and J. Hur, "A survey of secure data deduplication schemes for cloud storage systems," ACM Computing Surveys, vol. 49, no. 4, pp. 1-38, 2017.

[36] S. Chandna, R. Singh, and F. Akhtar, "Data scavenging threat in cloud computing," International Journal of Advances In Computer Science and Cloud Computing, vol. 2, no. 2, pp. 106-111, 2014.

[37] Microsoft Azure. (2018, 10/6/2018). Azure DDoS Protection. Available: https://azure.microsoft.com/en-us/services/ddos-protection/

[38] D. Plastina. (2015). Azure Key Vault—Making the Cloud Safer. Available: http://blogs.technet.com/b/kv/archive/2015/01/08/azure-key-vault-making-the-cloud-safer.aspx.

[39] J. Wu, L. Ding, Y. Wu, N. Min-Allah, S. U. Khan, and Y. Wang, "C2detector: A covert channel detection framework in cloud computing," Security & Communication Networks, Article vol. 7, no. 3, pp. 544-557, 03// 2014.

[40] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: A survey," Journal of Network and Computer Applications, vol. 77, pp. 18-47, 2017.

[41] T. B. Waghela, "Botnet: Switching c & c servers using RaspberryPI," vol. 14, pp. 100-104, 2016.

[42] L. Ablon and M. Libicki, "Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data," Defense Counsel Journal, vol. 82, pp. 143-152, 2015.

[43] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," ACM Computing Surveys, Article vol. 51, no. 4, pp. 1-36, 2018.

[44] C. Jadala Vijaya, A. Tingilikar, and B. Prathusha, "Challenges and defenses for network and cloud security from risks, threats and attacks in cloud computing," (in English), International Journal of Advanced Research in Computer Science, vol. 8, no. 9, Nov 20172017-12-27 2017.

[45] M. Mavani and K. Asawa, "Modeling and analyses of IP spoofing attack in 6LoWPAN network," Computers & Security, vol. 70, pp. 95-110, 2017.

[46] J. Luftman, K. Lyytinen, and Z. Tal ben, "Enhancing the measurement of information technology (IT) business alignment and its influence on company performance," (in English), Journal of Information Technology, vol. 32, no. 1, pp. 26-46, Mar 20172018-04-24 2017.

[47] Z. Alreemy, V. Chang, R. Walters, and G. Wills, "Critical success factors (CSFs) for information technology governance (ITG)," International Journal of Information Management, vol. 36, pp. 907-916, 2016.

[48] H. Hassan, M. Herry, M. Nasir, and N. Khairudin, "Cloud computing adoption in organisations: Review of empirical literature," (in English), vol. 34, 2017 2017.

[49] A. Prasad and P. Green, "Governing cloud computing services: Reconsideration of IT governance structures," International Journal of Accounting Information Systems, vol. 19, pp. 45-58, 2015.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[50] ENISA. (2018). About ENISA. Available: https://www.enisa.europa.eu/about-enisa

[51] E. Cayirci, A. Garaga, A. Santana De Oliveira, and Y. Roudier, "A risk assessment model for selecting cloud service providers," (in English), Journal of Cloud Computing, vol. 5, no. 1, pp. 1-12, Sep 20162017-02-09 2016.

[52] ISO. (2018). About ISO. Available: www.iso.org/iso/home/about.htm

[53] COSO. (2018). Welcome to COSO. Available: www.coso.org/

[54] ISACA. (2018, 10/3/2018). What we offer & whom we serve. Available: http://www.isaca.org/About-ISACA/What-We-Offer-Whom-We-Serve/Pages/default.aspx

[55] CSA. (2018). About Cloud Security Alliance. Available: https://www.cloudsecurityalliance.org/about/

[56] NIST. (2018). NIST general information. Available: www.nist.gov/public_affairs/general_information.cfm

[57] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," Computers & Security, vol. 44, pp. 1-15, 2014.

[58] P. P. Tallon, R. V. Ramirez, and J. E. Short, "The Information artifact in IT governance: Toward a theory of information governance," Journal of Management Information Systems, vol. 30, pp. 141-178, 2013.

[59] D. Roberts, Unleashing the Power of IT: Bringing People, Business, and Technology Together, 2nd Edition [VitalSource Bookshelf version], 2014. [Online]. Available: https://bookshelf.vitalsource.com/books/9781118824528.

[60] C. Low and Y. Chen, "Criteria for the evaluation of a cloud-based hospital information system outsourcing provider," Journal of Medical Systems, vol. 36, pp. 3543-3553, 2012.

[61] M. Gerber and R. v. Solms, "Information security requirements – Interpreting the legal aspects," Computers & Security, vol. 27, pp. 124-135, 2008.