Security in Organisations: Governance, Risks and Vulnerabilities in moving to the Cloud

Authors, Madini O Alassafi, Raid K Hussain, Ghada Ghashgari, RJ Walters, GB Wills

University of Southampton, United Kingdom

Abstract

Any organisation using the internet to conduct business is vulnerable to violation of security. Currently security in most organizations relates to protection of data and the management of their business information systems. Hence, security is often defined as the protection of information, the system, and hardware; that use, store and relocates that information. Governing information and the secure use of Information Technology (IT) is essential in order to reduce the possible risks and improve an Organisation's reputation, confidence and trust with its customers. One of the importance success factors for an organization to adopt and use the cloud effectively is information security governance (ISG). As a consequence, this chapter clarifies the concept of governance and the necessity of its two factors IT governance (ITG) and ISG.

Enterprise governance is directing and controlling the organization by the board of directors and executive management in order to ensure the success of the organization. ITG and ISG are integral part of corporate governance. ITG is about the structure that links IT processes, resources and information to support organisation's objectives. IT brings several risks and threats that need to be considered. Therefore, Information security should not be considered as just a technical issue but governance challenge that needs proactive approach. ISG consists of leadership, organisational structure, processes, compliance and technology. In order to promote the adoption of cloud computing, it is important to recognize that an important and specific issue related to cloud computing is the potential and perceived security risks posed by implementing such technology. Adopting the cloud has several risks such as malicious insider threats and data breaches. An example of cloud risk is virtualization that is one of the concepts used for constructing cloud computing, which has its own security risks,

but they are not specific to the cloud. Virtualization is related to open-source shared application server, database, and middleware components. The multi-tenancy model has introduced security problems as it is based on virtualization and sharing resources (hard disk, application software, and virtual machine) on the same physical machine. This chapter will present an overview of information security governance, the risks and vulnerabilities when moving to the cloud.

1 Introduction

Cloud computing is a delivery model for information and services using existing technology like virtualization, distributed computing, utility computing and web services. Security is the key issues for cloud computing success as cloud users feel a lack of control over their data stored in cloud computing. One of the most problematic elements of cyber security is the quickly and constantly evolving nature of security attacks, risks and threats. The security issues need to be governed to ensure that the organisation can survive and thrive. Ongoing attention and countermeasures are required to protect organisational data and information assets. Governing cyber security is required for the sustainability of an organisation through effective direction and control of all the possible security risks, threats, and vulnerabilities. Since one of the key aspects of governance is mitigating security risks in the enterprise environment in general and in cloud computing in particular, cloud adoption security risks as well as security issues in virtualization layer in cloud computing have to be addressed.

Information security governance (ISG) is a sub set discipline of corporate governance. Businesses that rely on information technology (IT) to hold and process their data and information have many advantages over non-IT approaches, but it also brings cyber security threats (IT Governance Institute 2003). Consequently, for the sustainability of the organisations they should use ISG at all levels of the organisation with consideration of all the significant security risks that may influence the organisation negatively in achieving its mission, goals and objectives. As well as aligning their strategies with the organisational objectives. Several Information security governance best practice standard-based frameworks are available, but there is no fixed framework for an organisation as it depends on several factors (Calder and Moir 2009). Because Information security governance is one of the important success factors for an organisation adopting and successfully using cloud, this article clarifies the concept of governance and the necessity of its factors. The security of the cloud, associated privacy concerns, causes many organisations to "*apply the brakes*" as they think through their particular cloud computing concerns. Security concerns include physical security and simple access to facilities and equipment, as well as logical security, industry compliance requirements, auditability, and more (Pearson 2013). Furthermore, the security risks have potential influence on the acceptance of cloud computing in most of the world. One of the main problems notable by big organisations is the amount of cost on the IT infrastructure. When an organisation is considering using cloud computing, there is a need for professional's cyber security skills for designing and building a cloud (KPMG, 2011). In addition, before using cloud computing, every organisation should consider the multiple dimensionality posed by security risks (Fumei Weng and Ming-Chien Hung 2014).

Security risks affect different infrastructure layers, which are the application layer, network layer, data storage layer, virtualization layer, trust layer and authentication and access control layer. Virtualization is one of the main concepts used for constructing cloud computing. It is the foundation for sharing resources for multiple cloud users but it has related security risks for instance, virtual machine (VM) isolation, VM migration, VM drawback, VM escape, VM sprawl, and VM image sharing. Multi-tenancy is one of the characteristics of cloud computing which is used to shared Infrastructure, application and platform resources among multiple users (Abd et al. 2015). Security experts consider multi tenancy as vulnerable.

This chapter consists of three sections, security governance, cloud security risks and cloud virtualization issues. The first section provides an overview of the governance concept in an organisation and its necessity. This section begins with corporate governance followed by its two components IT and security governance including an explanation of each concept and the necessity to be implemented in an organisation. Furthermore, some of the best practises principles and standards as well as effective factors are highlighted. The second section provides an overview of the security and security risks in cloud computing and a clear definition of both considering features that related to the cloud computing adoption and cloud security risks that affect the cloud computing adoption. The third section provides an overview of virtualization and multi- tenancy starting with an explanation of each component. Then the main security risks related to virtualization security layer are illustrated.

2 Information Security Governance,

In order to examine Security Governance and its place in an organisation, we first examine the role of Corporate Governance and Information Technology Governance.

2.1 Corporate Governance (CG)

Corporate governance (CG) is *"the system by which companies are directed and controlled"* (Cadbury 1992) and it has been defined as:

"The set of relationships between a company's board, its shareholders and other stakeholders. It also provides the structure through which the objectives of the company are set, and the means of attaining those objectives, and monitoring performance are determined" (OECD 1999).

The main objective of good CG is the enhancement of the organisational value and success in the long-term view for its all stakeholders and shareholders (Müller 2003). A vital factor in economic growth, financial stability, social development, good decision-making, and successful operation in an organisation is good CG. Moreover, CG ensures security confidence by monitoring and controlling the operation of the organisation (OECD 2004).

Governance is the responsibility of the board of directors. Therefore, setting organisation's strategic and goals, supervising the management, providing leadership and reporting to shareholders that all subject to laws and regulations are their responsibility (Cadbury 1992). Governance is unlike management because boards do not manage day-to-day activity but direct and control the organisation, ensure that shareholders and stakeholders desires are met (Love et al. 2010), and create an appropriate organisational culture to achieve organisation's goals (de Oliveira Alves et al. 2006). Therefore, the organization is directed by producing the policies, standards and procedures and controlled by measuring, monitoring and reporting compliance (von Solms and Vonsolms 2006).

Corporate governance became a world-wide topic in 1980s after many corporate crises and the financial collapses in several developed economies that raised questions regarding the ethics of their CG (Lessambo 2013). There were several investigations in UK notably after the collapse of Maxwell Communication Corporation plc in 1991, in order to improve CG the Cadbury report was published in 1992, and the Greenbury report in 1995 (Jones and Pollitt 2004). Due to the powerful interest and the high quality process of Cadbury's committee investigation, Cadbury report on the Financial Aspects of Corporate Governance has been distinguished from all other reports and has been implemented internationally (Lessambo 2013).

The cadbury code of best practice was developed to strengthen the effectiveness of the board system in order to achieve high standards of corporate governance, financial reporting and auditing confidence based on compliance with disclosure, and clear understanding of responsibilities and expectations of each person involved. The code is based on three main principles, openess and information disclosure, integrity of fianancial reports and honesty, and accountability of the board and shareholders.

The Organisation for Economic Cooperation and Development (OECD) is an international corporate governance system. OECD framework is based on Cadbury code (Bouchnez 2007; Mallin 2002).The principles of the framework aim to raise the consideration of managing conflicts of interest by enhancing transparency and information disclosure. The principles encompass five main areas; shareholders rights, equitable treatment, transparency and board responsibilities (Bouchnez 2007; Mallin 2002).

There is no single universal framework of CG that fits all organisations because the actions of the boards and the frameworks are subject to their country's law and regulations (Cadbury 1992; OECD 2004).

By adopting CG framework, an organisation will have the opportunity to use their resources efficiently with accountability for its stewardship, and align the interests of individual, organisation, and society (Weill and Ross 2004a). CG is not just about complying with rules and regulations; CG is about principles (OECD 2004).

2.2 IT Governance (ITG)

Information technology (IT) is critical to enterprise success. It assists the enterprise to accomplish a competitive advantage since it increases the enterprise efficiency and productivity and reduces cost. However, IT creates different types of risks and threats such as hardware and software failure, human error, computer viruses and social engineering. Therefore, understanding of IT issues and strategy is required for secure and successful operational sustainability and extensibility of an organisation, if it is to be controlled and governed efficiently (IT Governance Institute 2003). Long-term success of an organisation requires that IT and business be strongly tied together in order to maximize the benefits of IT and reduce its uncertainty (Posthumusa and Von Solms 2005). IT governance (ITG) is the means for deciding who makes what decisions about the use of IT and the accountability framework creation that drives the desired behavior in the use of IT (Weill and Ross 2004). ITG has been defined as

"*The structure of relationships which links IT processes, IT resources and information to organisation strategies and objectives to direct and control the organisation in order to achieve the organisation's strategies and objective*" (Abu-Musa 2007).

ITG is the responsibility of the board of directors and executive management in particular because IT expectation and reality often do not match. ITG is a subset discipline of corporate governance, and should not be considered in isolation (IT Governance Institute 2003).Thus, to accomplish the objective of corporate performance, ITG should be developed based on the principles of corporate governance (Weill 2004). Ko and Fink (2010) illustrated the concept of ITG by framing its scope of functions since the concept is not yet consistent and mature because of the disconnection and the concentration between the industries, developers of the ITG best practice frameworks. Ko and Fink (2010) grouped the view of ITG into three collaborative and complimentary dimensions: structure, process and people. The structure dimension consists of the structure of the IT functions, IT decision-making authority, and the mechanism for the organisation to manage its IT. The process component includes IT activities that have to be aligned with strategic business objectives, and performance tracking for organisational improvement achievement and positive outcomes sustainability. People is the third collaborative dimension that has received less attention in literature. Leadership is one of the ITG key success factors that distinguishes the organisations with top performance from the others ones. Leadership is required to ensure that IT activities achieve the goal of the organisation. Furthermore, clear understanding of roles and responsibilities, commitment and participation with transparency, and awareness and understanding are the sub components of the dimension. As it can be seen, all of these ITG components and sub components work and cooperate with each other (Ko and Fink 2010).

ITG best practices, standard-based frameworks, have been developed by internationally recognized organisations. These frameworks are control objectives for Information and related technology (COBIT), and ISO/IEO 38500. COBIT has been developed by IT Governance Institute

(ITGI) which is part of Information systems audit and control (ISACA). Its objectives are the alignment of IT and business, maximize the benefits of the use of IT, the use of IT resource responsibly, and manage and mitigate IT risks (Ko & Fink 2010). ISO/IEO 38500 has been published by ISO organisation, and its aim is the effective, efficient, and acceptable use of IT in all organisations (Sylvester 2011). Both COBIT and ISO/IEO 38500 are principle-base and provide a high-level governance framework that focuses on what to be done rather than how, and these are the most comprehensive ITG frameworks (Sylvester 2011). The main principles of COBIT 5 are meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management (Vander Wal 2012). While ISO 38500 is based on six principles responsibility, strategy, acquisition, performance, conformance, human behavior (ISO 38500:2008).

There is no universal ITG framework or standard that has the best ITG structure and effective processes and implementation because ITG on an organisation depends on several factors (Calder and Moir 2009). Successful implementation of an ITG framework requires stakeholders' involvement from all business levels (Rau 2004). In addition to the management support and leadership from all management levels (Calder and Moir 2009).

2.3 Information Security Governance (ISG)

Data and information held on IT systems are valuable and critical to the business of the organisation because the value of a business is concentrated in the value of its information. Most organisations rely on IT to store and process information; therefore, it is essential to maintain Information Security. In the ever-changing technological environment, the threats to Information Security from viruses, hackers, criminals, and terrorists are increasing as well as the threats to information from errors, loss, misuse, or disclosure. Consequently, organisations need to incorporate effective information security program into the everyday practice performed that must be proactive, and cope with the technological changes and the growing cybersecurity risks effectively (IT Governance Institute 2006). information security includes the protection of information assets in all of its forms; digital physical and people as well as information systems in all of its situations in transit, processing or storage from attack, damage or misuse (Love et al. 2010). The main objectives of Information Security are protecting information confidentiality by ensuring that it is accessible only by authorized people and only disclosed to authorized people; preserving information integrity by safeguarding its accuracy and completeness and preventing unauthorized modification; promoting information availability by ensuring its availability when it is required by authorized people; and exchanging information with trust, authenticity and non-repudiation (IFAC 1998; IT Governance Institute 2006; ISO 17799).

For effective and successful information security, active involvement of executive and senior management is required in order to evaluate emerging security threats and the organisation's response to them, and to provide strong cyber security leadership. This involvement is the integration of Infromation Security with CG, the overall governance. Infromation Security needs to be addressed at the strategic level of the organisation, top-down process, in order to support organisational strategy and objectives. As a consequence, Infromation Security should not be considered as a solely a technical issue, but a governance challenge that involves, reporting, accountability and risk management (National Cybersecurity Summit Task Force 2004; IT Governance Institute 2006). The implementation of governance concepts and principles on the issues of Infromation Security is Infromation Security governance (ISG). Johnston and Hale (2009) confirmed empirically that the effectiveness of an infromation security program relies on the strategy the organisation uses for its information security planning. They confirmed that an organisations that address their infromation security from the bottom up, use reactive IS plans and segregate information security from their strategic directive; in other words, isolate the governance from the management of information security, have ineffective information security programs and can fall victim to internal and external cybersecurity attacks.

The ITGI (2006) has defined ISG as,

"*The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organisation's resources are used responsibly*."

Moulton and Coles (2003) defined ISG as,

"*The establishment and maintenance of a control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems*"

ISG assures that Infromation Security strategies are aligned with organisational strategy; support organisational objectives, and are consistent with the laws and regulations via policies and internal controls compliance. Compliance places responsibility and accountability for IS at all levels of the organisation to manage and reduce security risks (Bowen et al 2006).

When organisations update or apply new legal requirements, the responsibilities of management's governance can change significantly which can cause changes to the way information security is approached. The framework of ISG supports organisations to undertake requirements and manage new risks within the organisation (Moulton and Coles 2003).

ISG consists of leadership, organisational structure, processes, compliance and technology. It also requires executive management leadership to be proactive and strategic in order to ensure that the activities of information security are supported and understood at all organisational levels and aligned with organisational objectives (Love et al. 2010). Organisational structure is a rational set of arrangements and mechanisms (Weill and Ross, 2004a, p. 183) about how ISG functions are carried out, controlled and coordinated, and is dependent on the overall organisation structure (Bowen et al 2006). ISG processes are the Infromation Security activities that support organisational objectives. These main components of ISG ensure that the confidentiality, integrity and availability of organisation's electronic assets are maintained all the time and information is never compromised (Von Solms 2001). Employing ISG properly allows organisations to align Infromation Security with their strategy in order to support their objectives (strategic alignment), deliver business value to all stakeholders, ensure management of risk and resource, measure organisational performance to ensure that organisational objectives are achieved (IT Governance Institute 2006), and comply with regulation standards and agreement (ISO 27014).

Because their strategy is becoming a major issue of concern for all types of organisations around the world, an effective ISG framework is required. Task Force and Entrust (2004) confirmed that adopting a framework is an important action in assisting organisations with integrating ISG into their CG practices, securing information, improving the efficiency of organisational processes, complying with regulations, and cultivating an acceptable IS culture. In addition, ITGI (2006) clarifies that ISG is essential because it improves organisation's reputation, confidence and trust with customer relationship and with whom business is conducted, reducing operational costs by providing predictable outcomes and mitigating risks that may interrupt operations.

ISO/IEC 27014:2013 and COBIT 5 for their strategy are two ISG best practice standard-based frameworks that have been developed by internationally recognized organisations.

Similar to ITG, there is no single best ISG framework or standard because organisations are different according to their requirements and risk tolerance (Love et al. 2010).

3 Security Risks in Cloud Computing

Implementing ISG is based on understanding the security risk, within an organisation. Security is the most important challenge and it is still the biggest concern in cloud computing, this is because of the uncertainty about privacy and security of information in cloud, at every level (Avram 2014). Before using cloud computing, every organisation should consider the multiple dimensionality of security risk (Fumei Weng and Ming-Chien Hung 2014). Organisations around the world are facing the problem of protecting individual's private information and by adopting cloud computing, it is not clear whether it will provide security for such information (Alharthi et al. 2015).

ISO27001 defined the security as, "*Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved*"

Moreover, there is a list of cloud computing concerns; security is often at the top of the list (Sen 2013). Cloud computing might introduce different risks to many organisations from traditional IT and the security risks be influenced significantly by the type of cloud service and cloud deployment model.

According to Cloud Security Alliance Definition the Cloud Computing Security is

"*The set of control-based technologies and policies designed to follow to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use"* (Rashdi et al. 2013).

When an analogy is drawn between criminals and hackers, experts of cloud computing agree that cloud security is a step behind the development of technology in implementing it. There are various security issues for cloud computing as it includes several technologies including operating system, networking, virtualization, concurrency control, database and load balancing. Therefore, security issues in most of these technologies are applicable to cloud computing. For example, the network that communicates the systems in the cloud must be secure. Moreover, the virtualization model in cloud computing leads to more security concerns. Data security includes encrypting the data with securing that a suitable policy are applying for data sharing. Besides, resource allocation and memory management systems must be also secure (Sen 2013).

The full utilization of cloud based services by any organisation or by any individual depends on the security of their personal information, which is the biggest concern (von Solms & van Niekerk 2013). Irrespective of whether it is a service provider an organisation or an individual, there are security issues that concern every stakeholder in adoption of cloud. The security can be summarized into these principles: confidentiality, availability, and integrity (CIA) (Cherdantseva & Hilton 2013). Therefore, If any one of the three Confidentiality, Integrity, or Availability, can be threaten, it can have a serious significance for the organisations (Cherdantseva & Hilton 2013). CIA are important to understand the security principles and they can be defined as following:

Confidentiality: a system should ensure that only authorised user's access information.

Integrity: a system should ensure completeness, accuracy, and absence of unauthorised modifications in all its components.

Availability: a system should ensure that all system's components are available and operational when authorised users require them.

The principles of CIA are important to known set of threats, and occasionally law requires some of these principles. Despite the security benefits of cloud computing the cloud services which are applications successively anywhere in the cloud computing infrastructures by inside network or the internet and the most benefit of security in positions to cloud computing is the data securely and safely. Hence, cloud computing has important prospective to develop security and flexibility. According to European Network and Information Security Agency (ENISA), the following are the security benefits of cloud computing:

- Security and the benefits of scale
- Security as a market differentiator

- More timely and effective and efficient updates and defaults
- Rapid, smart scaling of resources
- Standardised interfaces for managed security services
- Audit and evidence-gathering
- Audit and Service Level Agreements (SLAs) force better risk management
- Benefits of resource concentration

When it comes to define the risk, it is the possible impact or result of happening on assets of an organisation. In economic positions, the risks have recognised like a value at risks that is arithmetical measure, which describes the significance of a loss via the confidence level or the chance of happening (Chang et al. 2015).

Despite all benefits of cloud computing, there are some risks that hinder government organisations or even public sectors to adopt cloud computing (Chang, V. 2013). Most of the risks on cloud computing addressed as:

- Time Risk: considered one of the most risk affecting the decision of the cloud computing. Time risks include (time to recognise and situations environment of using cloud computing, compliance with protect the data, time to explore and implementing a new solution and time to know and work in with the service level agreement (SLAs) terms) (Elena & Johnson 2015).
- Performance Risk: consumers always want confidence and transparency about the performance of the cloud system and how it succeeded as well, since the cloud dynamically offering a service, which meets performance needs and holds operating costs low (Nist 2012).
- Social or Reputational Risk: considered of the technical risks due to meet customer demand. Social risk for using cloud services is very high because of the possibility damage and loss of standing in matter of leakage of particular data and unavailability of the cloud services (Chang, V. 2013).
- Financial Risk: including prospective costs from reputational damage from the cloud provider in security data breaches. Financial risk is importance perceived security risks of cloud service because the cloud services need to show qualifications and

performances before spending money on new IT systems (Gentzoglanis 2011; Chang 2014).

- Security Risk: most of studied shows that the security risk is the most importance should considered when adopting cloud computing services in government organisations or even private sector and it typically ranked the top cloud computing adoption concerns (Elena & Johnson 2015). Security risks are the major impediment and information always comes with security and risk problems. According to the Cloud Security Alliance, the security of cloud computing is the biggest concern for the organisations. The security risks linked with each cloud delivery model are different and reliant on a varied collection of factors including the sensitivity of information possessions, cloud architectures and security control complicated in a specific cloud environment. However, the characteristics of cloud computing increased number of users of cloud poses concerns regarding security risks in cloud computing because of shared resources in the cloud (Sen 2013).

Implementing cloud computing in any organisation means that all the data is shifted to external cloud which increases the exposure of threats from hackers (Sen 2013). Therefore, before implementing cloud computing, be aware of potential security risks in the organisation is very important. Since, there are many different ways of classifying security risks. Furthermore, these classifying appropriate in a wider model of cloud associated to risks. For example Centre for Protection of National of in Infrastructure organisation (CPNI) covered the most of security risks in the practical cloud service transaction depending on thier accompanied a survey of industry experts to collect specialised judgement on the highest weaknesses within cloud computing *as Insider user, External attacker, Data Leakage, Data segregation, User access, Data quality, Change management, Denial of Service, Physical disruption and Exploiting weak recovery procedures.* Generally, the cloud computing are similar those used in further IT environments in term of security control. But, the clients give up the control to the provider of the cloud and there is connected of the risks that the CSP do not satisfactorily address the security that have to be control or even that service level agreement (SLAs) don't consist of any providing of the important security services (Pearson 2013).

These risks are reliant on the service cloud model that are used. The cloud providers have to be controlled because the further security the customers is responsible for. Consequently, the customers of infrastructure as a service wants to construct in security as they are mainly responsible to that, while in the software as a service environments security controls and its possibility as the privacy and the compliance are converted in the agreements for service. It is important that for the customers or users to understand what the cloud provider holder the issues such as configuration management and cover management when they build new operating system or upgrade it to new one likely the IT security hardware and software which the provider is consuming and how to be protected. In other case of IaaS and PaaS, the cloud providers have to be simplify the type of IT security. So, the users are expected to put into place. Moreover, by SaaS , the users is still wishes to offer access security over its own their systems, that could also being to know how management system or a local access control their applications (Pearson 2013).

The risks to information assets established in the cloud can vary according to the cloud delivery service models used by cloud user organisations. **Table 1** provides some of risks for cloud according to CIA security model and their linked to each of the cloud delivery models. Some of the security risks in cloud computing can affect the services in the cloud (IaaS, PaaS and SaaS) posing threats on the CIA of the systems in these services. However, some risks only affect two or one of the service models.

Table 1. Cloud services Security Risks on CIA

Security Principles	Risks	Cloud Service Models (SaaS, PaaS and IaaS)		
Confidentiality	Insider user	SaaS	PaaS	IaaS
	External attacker	SaaS	PaaS	
	Data Leakage	SaaS	PaaS	
Integrity	Data segregation	SaaS	PaaS	
	User access	SaaS	PaaS	IaaS
	Data quality	SaaS	PaaS	
Availability	Change management	SaaS	PaaS	IaaS
	Denial of Service	SaaS	PaaS	IaaS
	Physical disruption			IaaS
	Exploiting weak recovery procedures	SaaS	PaaS	IaaS

4 Virtualization Security Risks in Cloud Computing

The National Institute of Standards and Technology stated that security risks are the main obstacle that delays the adoption of cloud computing (Kshetri 2013). Cloud computing has some vulnerabilities that might affect the core principles of information security. Vulnerability in cloud computing refers to weaknesses in the system that might be exploited by an attacker to obtain unauthorized access to the resources. Whereas, threats refer to vulnerability being abused by an attacker to obtain unauthorised access to the resources (Hashizume et al. 2013). In the survey of the literature by Modi et al.(2013) show security issues at different layer in cloud computing and they are:

- The application level issues.
- The network level issues.
- The data storage level issues.
- Virtualization level issues.
- Authentication and access control level.
- Trust layer level issues.

Virtualization is an important component in cloud computing and it helps cloud computing to deliver its services. In the next section, virtualization is explained along with some of the security concerns in more detail.

4.1 Virtualization

Virtualization has a crucial role in cloud computing as it is helping the IT industries to lower the cost and improve the performance of their applications (Sabahi 2011). Virtualization means

"A way of making a physical computer function as if it were two or more computers where each non-physical or virtualized computer is provided with the same basic architecture as that of a generic physical computer. Virtualization technology therefore allows the installation of an operating system on hardware that does not really exist " (Carlin 2011).

In virtualization, the resources can be joint or spilt through multiple environments. These environments are called virtual machines (VMs). The virtual machine host the guest operating system(Buyya et al. 2009). A hypervisor is one of visualization components which permit the guest OS to be hosted on host computer (Sabahi 2011).

One of the characteristics of cloud computing is multi-tenancy. Shared infrastructure and partitioning virtualization are provided by multi-tenancy to facilitate better utilize computing resources (Abd et al. 2015). Multi-tenancy is defined as

" *Multi-tenancy is a property of a system where multiple customers, so-called tenants, transparently share the system's resources, such as services, applications, databases, or hardware, with the aim of lowering costs, while still being able to exclusively configure the system to the needs of the tenant*" (Kabbedijk et al. 2015).

There are two kinds of multi-tenancy: the multiple instance and native multi-tenancy. In multiple instance, each tenant served by devoted application instance from a shared OS, hardware and middleware server in a hosted environment. However, the native multi-tenancy one instance of a program can serve several tenants over many hosting resources. In a SaaS model, multi-tenancy can be applied to four different software layer: application layer, middleware layer, the virtual layer and the OS layer (Espadas et al. 2013).

While Multi-tenancy has brought significant benefit to cloud computing as it reduces cost and save energy, it has however from the perspective of security expert brought vulnerabilities as it may affect the confidentiality of the data held on the server (Aljahdali et al. 2013). Wu et al. 2010 admitted that eliminating the virtualization layer will avoid the security hazards caused by multi-tenancy but this will exclude a vital advantage for cloud service providers like VM mobility. VM mobility is very helpful in saving energy. However, normal security techniques used in Multi-tenancy cannot mitigated some threats when both attacker and victim are on the same physical machine (the server). To secure this vulnerability, it is important to understand how the attack is performed. Firstly, a target VM is identified by a network probing mechanism. The network probing mechanism is used to find the physical topology of a network that contains the servers connected to the network and the internet protocols (IP), which are used to recognise the victim. Secondly, by taking advantage of multi tenancy the attacker's VM is allocated close to victim's VM using a brute force attack. A brute force attack is a mechanism that is used by an attacker to run an attack operation multiple times until a breach is achieved. Brute force is one of the most common data breaches attack methods used by attackers. Finally, a side channel attack is generated based on the information gathered from the network probing to extract data from the victim's VM (Aljahdali et al. 2013).

In the virtualized (multi-tenancy) environment, each user is allocated a virtual machine that host a guest operating system. The virtual machines (VMs) that belong to different users can share the same physical resources that allows resource pooling. A virtual machine monitor is used to control the VMs and allow the many OS to run on the same physical hardware (Ali et al. 2015). The virtualized (multi-tenancy) environment has introduced security issues for instance VM isolation. VM isolation is the VMs that are running on the same physical hardware need to be isolated from each other. In spite of the VMs being logically isolated, they will still need to be isolated physically as they share the same physical storage and memory. Sharing the same hardware might lead to data breaches and cross VM attacks (Gonzalez et al. 2011) . Moreover, VM migration happens due to load balancing, maintenance and fault tolerance, a VM can be moved from one physical hardware to another without shutting down the VM. This process might expose the data to the network that lead to privacy and integrity concern. The migrated VM can be compromised by an attacker to relocate the VM to an infected monitor or compromised server (Zhang & Chen 2012).

Furthermore, VM rollback occurs when VM can be rollback to pervious state when it is necessarily. This facility provides flexibility to the user but it raise a security problems. Moreover, it might render VM to a vulnerability that was solved previously (Hashizume et al. 2013). In addition, VM escape: the VVM or the monitor is a software that manage the VMs and the access to hardware. The VM escape happen when the malicious user trying to escape from the control of the monitor. The VM escape can provide the attacker the ability to access other VMs in the same hardware or might bring the monitor down (Jansen 2011). Subsequently, VM sprawl: it is happen when a number of VMs are increasing on the host system and most of them are in the idle state. This situation lead to wasting the resources of the host machine in a large scale (Sunil Rao & Santhi Thilagam 2015).

Finally, VM image sharing: A user can use the VM image from the repository or can create his/her own VM image. A malicious user can upload an infected image that contains malware to be used by other users. An infected VM image can be used to monitor the users’ data and activities (Ali et al. 2015).

5 Recommendation

In this section, security governance, virtualisation and security risks subjects that affect the organisation when moving to the cloud are described and a set of recommendations related to these domains are further illustrated in **Table 2**.

Table 2, Security in organisation with recommendations

Domains	Subjects	Description and Recommendation	References
Information Security Governance	Strategic alingment	Information security should not consider just techcical issues but of strategic level governance concerns in order to align the security processes and practices with organisational strategy and support organizational goals and objectives.	National Cybersecurity Summit Task Force (2004) and IT Governance Institute (2006).
	Active involvement	Active involvement of senior management is required in order to evaluate emerging security risks and threats, and the organisation's response to them.	National Cyber Security Summit Task Force (2004), IT Governance Institute (2006) and Abu-Musa (2007)
	Management Leadership	It is important to have proactive and strategic leadership in order to ensure that the activities of information security are supported and understood at all organisational levels, and aligned with organisational objectives. In addition to that, when staff members see the management concern and attention to security, they understand the necessity and importance of security, therefore, its benefit the creation of security culture.	Love et al. (2010)
	Effective IS program	Organisations need to integrate an effective information security program into the everyday practice performed that must be proactive, and cope with technological changes and growing cybersecurity risks effectively.	IT Governance Institute (2006)

	Adoptin ISG best practice framework	Adopting ISG framework is an important action in assisting organisations with integrating ISG into their CG practices, securing information, improving the efficiency of organisational processes, complying with regulations, and cultivating an acceptable IS culture.	National Cyber Security Summit Task Force (2004) and Entrust (2004)
Cloud Security Risks	Security Principles (CIA)	If any one of the three Confidentiality, Integrity, or Availability, is threatened, it can have serious consequences for the organisations.	(Cherdantseva & Hilton 2013).
	Risks in cloud computing	In economic case, the risks have to known as a value at risks which is numerical measure, that defines the significance of a loss by the confidence level or the chance of happening.	(Chang et al. 2015)
	Risks with cloud service models	The risks are dependent on the cloud service models that are used. The cloud providers must be controlled because of the additional security the require. However, it is important that for the users to be familiar with what the cloud provider does to control issues such as configuration and cover management when they build new operating systems or upgrade them.	(Pearson 2013)
	Security Risks	Before using cloud computing, every organisation needs to consider the multiple dimensionality of security risks. For example, the network that communicates the systems in the cloud must be secure. Moreover, the security risks linked with each cloud delivery model are different and reliant on a varied collection of factors including the sensitivity of information and cloud architectures.	(Fumei Weng and Ming-Chien Hung 2014), (Sen 2013)
Security issues in virtualization layer	Security issues	Services in cloud computing are delivered through virtualization as they share the hardware amonge many users.	(Sabahi 2011)
	Multi-tenancy	Confidentiality of the data held on the server might be vulnerable as it is sharing the same hardware.	(Aljahdali et al. 2013)

6 Conclusion of this Chapter

In conclusion, the life blood of an orgnaisation is its data and information, therefore, compromising them could harm the orgnaisation. Governing the information security and aligning these strategies with organisational objectives is essential to the sustainability and the success of an organisation. Information security governance is a subset of corporate governance, and a task within the organisational structure of a company is to ensure that the organisation will survive and thrive. There is no universal governance model and there are no right or wrong governance frameworks, or standards because each organisation has its own culture, law and regulations, requirements, and risks. Security risks and virtualization in cloud computing have obtained attention from orgnasations.

Directing and controlling the use of IT in all the organizational levels is important in order to reduce all the possible risks. There are several risk triggers when adopting the cloud that need to be governed such as malicious insiders and account hijacking. Moreover, virtualization issues in cloud computing such as virtual machine image sharing is one of the most threaten issues that need to be directed and controlled. By governing the possible risks including such risks the organisation will survive and thrive.

7 References

1. Abd, S.K., Salih, R.T. & Hashim, F., 2015. Cloud Computing Security Risks with Authorization Access for Secure Multi-Tenancy Based on AAAS Protocol. *IEEE Region 10 Conference TENCON*, pp.1–5.
2. Abu-Musa, A., 2007. Exploring Information Technology Governance (ITG) in Developing Countries: AN Empirical Study. *The International Journal of Digital Accounting Research*, 7(13), pp.71–120.
3. Alharthi, A. et al., 2015. An Overview of Cloud Services Adoption Challenges in Higher Education Institutions.
4. Ali, M., Khan, S.U. & Vasilakos, A. V., 2015. Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, pp.357–383. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0020025515000638.
5. Aljahdali, H., Townend, P. & Xu, J., 2013. Enhancing multi-tenancy security in the cloud IaaS model over public deployment. *Proceedings - 2013 IEEE 7th International Symposium on Service-Oriented System Engineering, SOSE 2013*, pp.385–390.
6. Avram, M.G., 2014. Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, 12, pp.529–534. Available at: http://www.sciencedirect.com/science/article/pii/S221201731300710X.
7. Bowen, P., Hash, J. and Wilson, M., 2006. October. Information security handbook: a guide for managers. *In NIST Special Publication 800-100, National Institute of Standards and Technology.*
8. Bouchnez, L., 2007. Principles of Corporate Governance : the OECD Perspective. *European Company Law*, 4(3), pp.109–115.
9. Buyya, R. et al., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(JUNE), p.17. Available at: http://portal.acm.org/citation.cfm?id=1528937.1529211.
10. Cadbury, A., 1992. The Financial Aspects of Corporate Governance. , p.90.
11. Calder, A. & Moir, S., 2009. *IT Governance, Implementing Frameworks and Standards for the Corporate Governance of IT*,
12. Carlin, S., 2011. Cloud Computing Security. *Artificial Intelligence*, 3(March), pp.14–16.
13. Chang, V., 2014. The Business Intelligence as a Service in the Cloud. *Future Generation*

Computer Systems, 37, pp.512–534. Available at: http://dx.doi.org/10.1016/j.future.2013.12.028.

14. Chang, V., 2013. A proposed model to analyse risk and return for a large computing system adoption (Doctoral dissertation, University of Southampton).
15. Chang, V., Walters, R.J. & Wills, G.B., 2015. Organisational sustainability modelling—An emerging service and analytics model for evaluating Cloud Computing adoption with two case studies. *International Journal of Information Management*, pp.1–13. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0268401215000882.
16. Cherdantseva, Y. & Hilton, J., 2013. A Reference Model of Information Assurance & Security. *2013 International Conference on Availability, Reliability and Security*, pp.546–555.
17. Entrust, 2004. *Information security governance (ISG): An Essential Element of Corporate Governance*. Available at: http://itresearch.forbes.com/detail/RES/1082396487_702.html
18. Elena, G. & Johnson, C.W., 2015. F ACTORS INFLUENCING RISK ACCEPTANCE OF C LOUD COMPUTING SERVICES IN THE UK. , 5(2).
19. Espadas, J. et al., 2013. A tenant-based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures. *Future Generation Computer Systems*, 29(1), pp.273–286.
20. Fumei Weng and Ming-Chien Hung, 2014. Competition and Challenge on Adopting Cloud ERP. *International Journal of Innovation, Management and Technology*, 5(4), pp.309–313. Available at: http://www.ijimt.org/index.php?m=content&c=index&a=show&catid=56&id=832.
21. Gentzoglanis, A., 2011. Risk , Financial Modeling and Cloud Computing : A New Approach. *Computer*, 9, pp.147–151.
22. Gonzalez, N. et al., 2011. A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, pp.231–238.
23. Hashizume, K. et al., 2013. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(5), pp.1–13.
24. IFAC., 1998. International Information Technology Guidelines: Managing Security of Information, New York, NY.

25. IT Governance Institute, 2003. *Board Briefing on IT Governance. Second edition 2*,
26. IT Governance Institute, 2006. *Information Security Governance: Guidance for Boards of Directors and Executive Management*,
27. ISO/IEC 17799, 2005. ISO/IEC 17799:2005 *Code of practice for information security management.* Geneva. International Organization for Standardization and the International Electrotechnical Commission. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=39612
28. ISO/IEC 27014, 2013. ISO/IEC 27014 G*overnance of Information Security*. Geneva. International Organization for Standardization and the International Electrotechnical Commission. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43754
29. Jones, I. and Pollitt, M., 2004. Understanding how issues in corporate governance develop: Cadbury Report to Higgs Review. *Corporate Governance: An International Review*, 12(2), pp.162-171.
30. Jansen, W.A., 2011. Cloud hooks: Security and privacy issues in cloud computing. *Proceedings of the Annual Hawaii International Conference on System Sciences*, (iv), p.42.
31. Kabbedijk, J. et al., 2015. Defining multi-tenancy: A systematic mapping study on the academic and the industrial perspective. *Journal of Systems and Software*, 100, pp.139–148.
32. Ko, D. & Fink, D., 2010. Information technology governance: an evaluation of the theory-practice gap. *Corporate Governance*, 10(5), pp.662–674.
33. Kshetri, N., 2013. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4-5), pp.372–386.
34. Lessambo, F.I., 2013. The International Corporate Governance System. , p.488.
35. Love, P. et al., 2010. GTAG Information Security Governance. , p.134.
36. Mallin, C., 2002. The relationship between corporate governance, transparency and financial disclosure. *Corporate Governance: An International Review,* 10(4), pp.253-255.
37. Müller, K., 2003. Corporate Governance and Globalization: The Role and Responsibilities of Investors. *In Selected Issues in Corporate Governance: regional and*

country experiences, New York, Geneva. United Nations. Publication No. UNCTAD/ITE/TEB/2003/3.

38. Modi, C. et al., 2013. A survey on security issues and solutions at different layers of Cloud computing. *Journal of Supercomputing*, 63(2), pp.561–592.
39. Moulton, R. & Coles, R.S., 2003. Applying information security governance. *Computers & Security*, 22(7), pp.580–584. Available at: http://www.sciencedirect.com/science/article/pii/S0167404803007053.
40. Nist, 2012. Cloud Computing: A Review Of Features, Benefits, And Risks, And Recommendations For Secure, Efficient Implementations. *Itl*, (June).
41. National Cyber Security Summit Task Force., 2004, Information security governance: a call to action, *Corporate Governance Task Force Report*, CS1/05-0037, available at: www. technet.org/resources/InfoSecGov4_04.pdf0
42. OECD, 1999. *Principles of Corporate Governance*. Organization for Economic Co-operation and Development. Available at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=C/MIN(99)6&docLanguage=En
43. OECD, 2004. *Principles of Corporate Governance*. Organization for Economic Co-operation and Development. Available at: http://www.oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf.
44. Pearson, S., 2013. Privacy, Security and Trust in Cloud Computing. *Privacy and Security for Cloud Computing*, pp.3–42.
45. Posthumusa, S. and Von Solms, R., 2005. IT oversight: an important function of corporate governance. *Computer Fraud & Security*, 2005(6), pp.11-17.
46. Rashdi, A. Al et al., 2013. Cloud Security Standards.
47. Rau, K.G., 2004. Effective governance of IT: Design objectives, roles, and relationships. *Information Systems Management*, 21(4), pp.35-42.
48. Sabahi, F., 2011. Virtualization-level security in cloud computing. *2011 IEEE 3rd International Conference on Communication Software and Networks*, pp.250–254.
49. Sen, J., 2013. Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology*, (iv), p.42.

50. Sylvester, D., 2011. ISO 38500 —Why Another Standard?. *Cobit Focus*, 2. Available at: https://www.isaca.org/Knowledge-Center/Documents/COBIT-Focus-ISO-38500-Why-Another-Standard.pdf
51. Sunil Rao, K. & Santhi Thilagam, P., 2015. Heuristics based server consolidation with residual resource defragmentation in cloud data centers. *Future Generation Computer Systems*, 50, pp.87–98.
52. Vander Wal, K., Lainhard, J. and Tessin, P., 2012. A COBIT 5 Overview. *ISACA*. Available at: www. isaca. org.
53. Von Solms, R. & van Niekerk, J., 2013. From information security to cyber security. *Computers & Security*, 38, pp.97–102. Available at: http://www.sciencedirect.com/science/article/pii/S0167404813000801.
54. Von Solms, R. and von Solms, S.B., 2006. Information Security Governance: a model based on the direct–control cycle. *Computers & Security*, 25(6), pp.408-412.
55. Weill, P. & Ross, J.W., 2004. IT governance on one page. *Cisr Wp No 349*, (March), p.18.
56. Wu, R. et al., 2010. Information flow control in cloud computing. *2010 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, pp.1–7.
57. Weill, P., 2004. Don’t just lead, govern: How top-performing firms govern IT. *MIS Quarterly Executive*, 3(1):1-17.
58. Zhang, F. & Chen, H., 2012. Security-Preserving Live Migration of Virtual Machines in the Cloud. *Journal of Network and Systems Management*, pp.562–587.