SECURE VIRTUALIZATION
Benefits, Risks and Controls

Mariana Carroll[1,2], Paula Kotzé[1,3] and Alta van der Merwe[1,2]
[1]*Meraka Institute of the CSIR, PO Box 395, Pretoria, 0001, South Africa*
[2]*School of Computing, University of South Africa, Pretoria, South Africa*
[3]*Institute for ICT Advancement, Nelson Mandela Metropolitan University, Western Cape, South Africa*
MCarroll@csir.co.za, {paula.kotze, alta}@meraka.org.za

Keywords: Virtualization, Cloud computing, Benefits, Controls, Risks.

Abstract: Cloud computing is changing the IT delivery model to provide on-demand self-service access to a shared pool of computing resources (physical and virtual) via broad network access to offer reduced costs, scalability, flexibility, capacity utilization, higher efficiencies and mobility. In many instances cloud computing builds on the capabilities of a virtualized computing infrastructure enabling multi-tenancy, scalability and a highly abstracted cloud model. Even though cloud computing provides compelling benefits and cost-effective options for IT hosting and expansion, security of applications and data remains a number one business objective. It is therefore essential to ensure adequate security not only for cloud computing, but also for the underlying technologies enabling cloud computing. Management should understand and analyse risks in order to safeguard systems and data. The focus of this paper is on mitigation for virtualization security risks as a fundamental step towards secure cloud computing environments.

1 INTRODUCTION

In today's globalised, volatile and competitive market, organizations are forced to leverage core competencies, be agile to allow them to evolve, and ensure that business optimization strategies are met. Business has become increasingly reliant on IT to support and deliver critical services and to enable execution of strategies. The IT landscape evolved to enable business to create a competitive advantage through cost optimization, scalability, flexibility, innovation and agility. Many of these benefits are achieved through the implementation of *cloud computing and virtualization* technologies.

Cloud computing provides IT resources on-demand as a service to customers, through a networked infrastructure, on a pay per use basis, and often utilizes virtualization resources (Boss et al., 2007, Cloud Security Alliance, 2009, Mell and Grance, 2009). Cloud computing could improve the way business and IT operate. Instead of having to deal with the complexities and costs, applications can now run in a shared data warehouse. Essential cloud computing characteristics include on-demand self-service access, broad network access, resource pooling, rapid elasticity, measured service, multi-tenancy and pay as you go (Centre for the Protection of National Infrastructure (CPNI), 2010, Cloud Security Alliance, 2009, Mell and Grance, 2009). Cloud computing benefits include reduced costs, fast start-up/deployments, flexibility, scalability, agility, accessibility/mobility, increased efficiency / productivity, resiliency and improved security (Avanade, 2009, F5 Networks, 2009, Gadia, 2009, Ponemon, 2010, ISACA, 2009).

Many of these cloud computing benefits, such as reduced costs, scalability, agility, increased efficiency and better utilization, are achieved through *virtualization* (Carroll et al., 2010). Virtualization enables multiple operating systems and applications to run concurrently and in isolation on a single physical host machine. It also enables multiple virtual machines (VMs) to share the resources of the physical host machine, ensuring better utilization, optimization and resource efficiency. Virtualization allows for resources to be automatically allocated when and where needed and for dynamic provisioning and de-provisioning (C.A. Solutions, 2010). Through this functionality, virtualization is seen as an enabling technology for cloud computing (C.A. Solutions, 2010, Cloud Security Alliance, 2009, Stratus Technologies,

2009). Therefore, through virtualization and cloud computing, the following can be achieved: software-, application-, platform-, or infrastructure-as-a-service, utility computing, server consolidation, on-demand self-service, location independence, multi-tenancy, scalability, reduced costs, flexibility, better utilization, higher efficiencies and agility.

However, no technology is without risks. Inadequate risk management could affect business immensely, from financial losses to losing customer goodwill and business reputation. We live in an era of continuous change and improvement in order to achieve and maintain a competitive advantage. This leads to most businesses being technology pervasive, meaning that technology represents in many instances a valuable business asset. For organizations to protect their business, manage IT and comply with regulations and legislation, management needs to identify, understand and manage associated risks and implement appropriate controls to safeguard IT assets and operations.

Clear guidelines indicating potential benefits and risks are needed to assist management in assessing the value of implementing cloud computing and virtualization as its underlying technology against the risks. Securing the virtualization component is therefore an essential step for organizations to protect their business and to manage their cloud and IT environments effectively.

We argue that a holistic approach is required which considers counterbalances for the risks so that the full benefits of virtualization and cloud technologies can be exploited. It is of no value to have an awareness of the benefits and risks without having a way to address the risks. The focus of this paper is therefore to (1) provide an overview of the benefits of virtualization, (2) highlight potential security risks associated with virtualization, and (3) propose a set of controls that could be considered for the mitigation of virtualization security risks.

Section 2 provides background to the concept of virtualization and the research process followed in identifying the benefits, risks and mitigating controls. An overview of the virtualization benefits is provided in section 3 and the virtualization risks, with specific focus on security, are described in section 4. Security risks and considerations for mitigation are discussed in section 5 followed by the conclusion in section 6.

2 BACKGROUND

The IT landscape has evolved from physical, to virtual, to the cloud through the enablement of various technologies such as the Internet, service-oriented architecture (SOA), virtual private networks (VPN) and Web 2.0 (Centre for the Protection of National Infrastructure (CPNI), 2010). Although not required or a synonym for cloud computing, virtualization has had a significant impact on the computing environment through the consolidation of computer resources for more effective and efficient utilization.

Through virtualization technology, multiple VMs run concurrently on a single host operating system situated on a single physical machine. A virtualization layer or hypervisor runs between the physical hardware and virtual machines and is responsible for managing and hosting the virtual machines. Enhanced security is achieved by VMs functioning in total isolation or silos, and no one machine can disrupt or directly access another. IT security policy enforcement is less complex when applied per VM, and this also enhances administrative control over resources (Carroll et al., 2010).

Virtualization makes it possible for different application versions and operating systems to run simultaneously on a single physical machine, resulting in increased server utilization and optimization. This functionality, coupled with the automated provisioning or de-provisioning and dynamic allocation of resources, enables cloud computing to be extremely efficient and flexible (Boss et al., 2007).

Within the cloud environment, virtualization allows users to access power beyond their own physical IT environment and consequently leads to many risks (Harauz et al., 2009). Virtualization is therefore regarded as a core component in cloud computing.

Security risks are addressed and controls are proposed in this paper for mitigation of security risks in virtual environments, which is regarded an essential step to safeguard the cloud computing environment.

We employed a qualitative research approach in an extensive study of existing resources that refers to (or sometimes only hints at) the virtualization benefits, risks and/or consideration or mitigation of virtualization risks. The research followed an inductive reasoning approach, using representative primary and secondary resources (selecting a sample of work or texts in order to understand and conceptualise the necessary information).

The literature review included available subject databases, online library catalogues, published

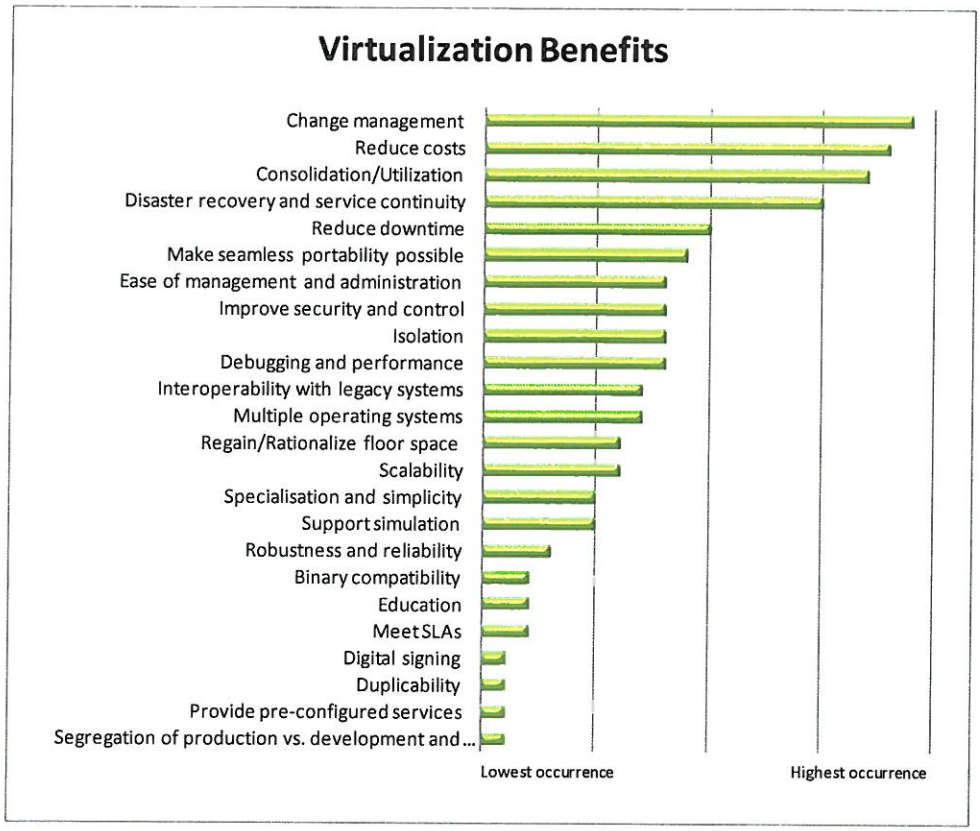

Figure 1: Virtualization benefits.

articles, relevant textbooks, industry-specific information and trusted resources from the Internet. The virtualization benefits and risks identified from the extensive literature review were also tested against primary data collected through interviews. Interviews were conducted with 15 participants, representing various South African organizations and a variety of different industries. The criteria for participation included a cloud computing and/or virtualization interest, current or planned implementing of cloud computing and/or virtualization, and currently in the role of senior management or higher. The interviews were conducted during July 2010 and October 2010. The construction research method was followed to derive, analyse and present a summary of the research findings obtained from both the literature review and the interviews.

An overview of the resulting set of virtualization benefits is provided in section 3, followed by the virtualization risks, with specific focus on security, in section 4.

3 VIRTUALIZATION BENEFITS

In the earlier part of our research, we derived a list of virtualization benefits, which we briefly summarize here (for a complete discussion on the benefits the reader is referred to Carroll et al. (2010)). The benefits are listed in Figure 1, arranged from highest occurrence (therefore cited most in the literature) to the lowest.

The *primary* benefits mentioned by most authors, when discussing virtualization, are a reduction in costs, server consolidation and utilization.

Major benefits include disaster recovery and service continuity (availability), easier or quick deployment, seamless portability and migration, increased flexibility and service agility, reduced downtime, easier and quicker developments and testing, ease of management and administration, isolation, and improved security and control.

Digital signing, duplicability, providing pre-configured services, and segregation of production versus development and test environments were also cited as *valuable* virtualization functionalities.

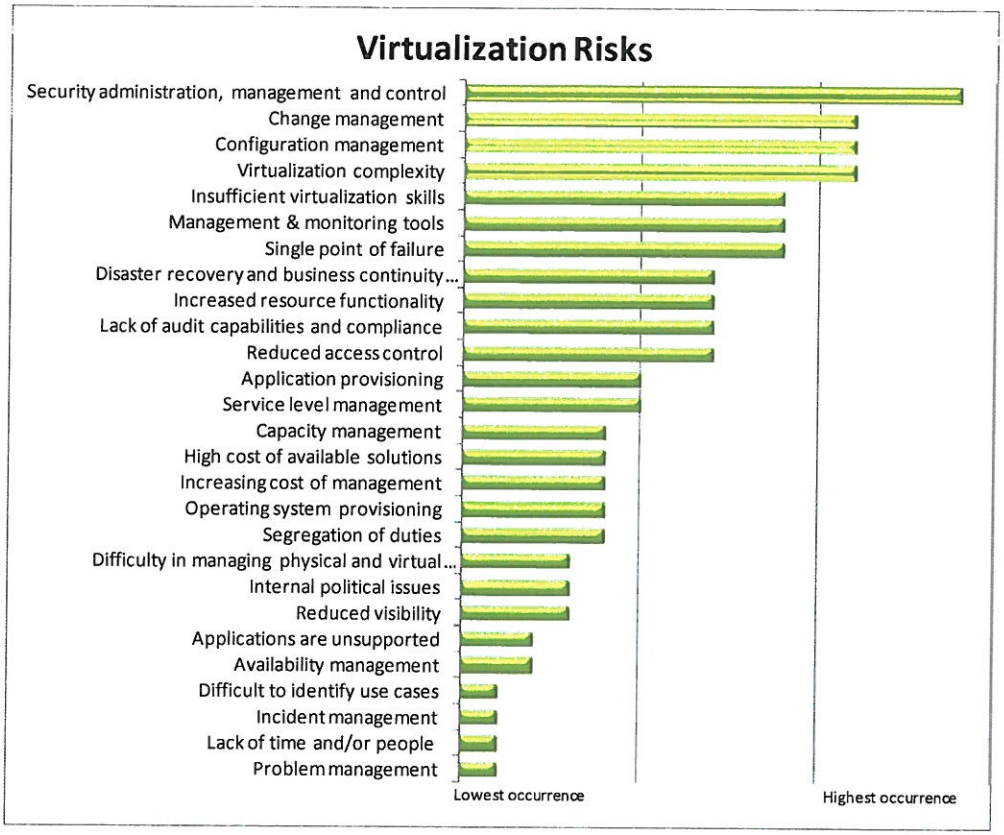

Figure 2: Virtualization risks.

4 VIRTUALIZATION RISKS

In addition to being aware of the benefits, management should also understand and analyse the risks posed by virtualization, and implement proper controls to mitigate these risks.

As described in section 2, the first step in our research was to review the published literature and to conduct an analysis to identify virtualization risks. This was followed by the 15 interviews to verify and/or enhance the data obtained from the literature review. Figure 2 presents the list of identified virtualization risks which were summarized from the literature review and which were confirmed by the data collected during the interviews.

Security risks were the *most common* risk experienced in virtual environments. Factors influencing security risks include fluctuating workloads, dynamic migration and changes, administrator skills, knowledge and training, access controls, hostile guests, the disappearance of "perimeter security", proliferation of VMs, configuration settings, hypervisor and VM monitor layer vulnerabilities, lack of visibility, lack of process management, and VM server sprawl (Barrett, 2008, Campbell and Jeronimo, 2006, Enterprise Management Associates, 2008, Hoesing, 2006, Ormandy, 2007, VMware Inc., 2006).

Other *primary* risks include change management, complexity, insufficient virtualization skills, configuration management, under-utilization of management and monitoring tools, single point of failure, disaster recovery and service continuity, the increased importance of resource functionality, reduced access control and segregation of duties, lack of audit capabilities and compliance, service level management, and application and operating system provisioning.

Difficult-to-identify use cases, incident management, lack of time and resources, and problem management were the risks mentioned *least frequently* in the literature.

As illustrated in Table 1, information security was rated by 91.7 percent of respondents to be the most critical risk area for the implementation of virtualization and cloud computing standards,

policies and controls. Disaster recovery/business continuity planning was rated the second most critical risk area, with a score of 66.7 percent. Standards, policies and controls for operations management, change management, third-party/service level management, interface management, and regulations and legislation were rated as "somewhat important" for the mitigation of risks. The findings from both the literature review and the interviews corroborate the importance of ensuring that the virtual environment is adequately protected and secure. We therefore focus primarily on security risks in the remainder of the paper.

An awareness of the risks alone would not overcome the security issues though. What is required is a set of controls that would allow management to mitigate the risks appropriately. In section 5 we will discuss the security risks in more detail and suggest examples of controls for mitigation of these risks in virtualized environments.

5 DISCUSSION OF SECURITY RISKS

It was significant during the research that in a number of instances, benefits, perceived as the main drivers for implementing virtualization, also proved to pose some of the most significant risks.

It is therefore imperative for management to analyse the benefits and risks of virtualization and to compare them in order to determine whether implementation would be feasible, practical and cost-effective. If the virtual solution is shown to be feasible and the benefit outweighs the risk, it is essential for management to implement controls, processes and procedures to ensure that virtualization risks are mitigated in the cloud environment adequately and effectively.

Through the extensive literature review, the following control objectives were identified as important for the mitigation of virtualization security risks in a cloud computing environment:

- Security, administration and control.
- Logical access.
- Network security.
- Physical security.
- Change control.
- Management and monitoring.

Each of these objectives is discussed in more detail in the following sections. The discussion of each control objective is accompanied by a table containing a summary of the risks and recommendations for possible mitigation of the risk as determined from the literature review. These recommendations form the first steps in setting up a complete framework for mitigating security risks through virtualization in cloud computing settings.

Table 1: Virtualization and cloud computing critical risk areas.

Risk area	Critical	Some-what important	Not so important
Information security	**91.7%**	8.3%	0.0%
Operations management	41.7%	**58.3%**	0.0%
Change management	41.7%	**50.0%**	8.3%
Disaster recovery/ business continuity planning	**66.7%**	33.3%	0.0%
Third-party/ service level management	41.7%	41.7%	16.7%
Interface management	8.3%	**50.0%**	41.7%
Regulations and legislation	33.3%	**41.7%**	25.0%

5.1 Security, Administration and Control

Virtualization improves security, administration and control through the ability of VMs to operate in isolation and thereby restrict security vulnerabilities to the compromised unit only. This leads to security policy enforcement being less complex and easily distributed across user interfaces. Server and hardware consolidation is further perceived to be the most generally accepted virtualization benefit. Consolidation leads to increased utilization and reduced costs. Virtualization benefits such as the ability to run different operating systems, duplicability, seamless migration and ease of deploying changes all contribute to the IT department's ability to respond promptly to organisational needs and changing environments (Bass, 2009, Campbell and Jeronimo, 2006, Enterprise Management Associates, 2008, Gardner, 2009, Hoesing, 2006, Humphreys and Grieser, 2006, Killalea, 2008, Robb, 2008, Sgallari, 2009, Sun Microsystems Inc., 2009, VMware Inc., 2006).

In direct contrast, *security administration, management and control* are also believed to constitute the biggest virtualization risks. The *security, administration, management and control* virtualization risks and the recommendations for mitigation of these risks are detailed in Table 2. The risks described in Table 2 are the dynamic migration and the seamless portability of VMs (A.1), the

duplicability of VMs (A.2), single target for attack or failure (A.3), complex or inefficient provisioning (A.4), non-compliance with licensing or service level agreements (A.5), and audit/event logging (A.6).

5.2 Logical Access

The *logical access* virtualization risks and the recommendations for mitigation of these risks are detailed in Table 3. Server and hardware consolidation lead to the collapsing of domain,

Table 2: Security, administration and control risks and mitigating controls.

Ref	Risk	Description of mitigating control
A.1	***Dynamic migration and the seamless portability of VMs between hosts*** leading to inadequate change management, lack of visibility contributing to inadequate VM tracking and an increased volume of risk exposures, software licensing violations and misconfigurations (VMware Inc., 2006, Ormandy, 2007, Hoesing, 2006, Enterprise Management Associates, 2008, Campbell and Jeronimo, 2006, Barrett, 2008).	Management reviews and approves the configuration and implementation of information security tools and techniques ensuring appropriate setup of clusters so that VMs are migrated within secure groups and between servers with the same infrastructure and security, and the implementation of monitoring and management tools proving visibility to all VMs and VM configuration (i.e. V-Tracker) (Ormandy, 2007, Gardner, 2009, Baldwin et al., 2008).
A.2	***Duplicability of VMs*** (creating copies of VMs by using templates or cloning existing VMs) leading to replication of insecure security setup based on the "templates" or cloning, increased server sprawl, misconfigurations and inappropriate access to the cloned or newly created VMs (VMware Inc., 2006, Ormandy, 2007, Hoesing, 2006, Enterprise Management Associates, 2008, Campbell and Jeronimo, 2006, Barrett, 2008).	Changes to the virtual environment should be documented, tested and approved by the appropriate level of management prior to implementation. This includes the following change scenarios: cloning or copying of VMs to ensure adequate and secure configuration, controls ensuring adequate and secure setup of VM "templates" including regular updating and patching, and unauthorized attempts to copy or clone VMs should be detected to ensure that sensitive information is not exposed outside secure and authorized environments.
A.3	If the host machine is experiencing problems or if compromised, it could have a direct impact on the virtual machine(s) being hosted. The host is perceived as a ***single target for attack or failure*** (Hoesing, 2006, Campbell and Jeronimo, 2006).	Security policies and minimum baseline security standards are implemented and processes are in place to regularly review configurations and the secure setup of the virtualization layers (hosts) (Ormandy, 2007, Gartner Executive Programs (EXP), 2010, Baldwin et al., 2008).
A.4	***Complex or inefficient provisioning*** due to manual procedures or lack of adequate tools leading to errors or misconfigurations, and possible could inhibition of the productivity of the administrators (VMware Inc., 2006, Strom, 2008, Sgallari, 2009, Senft and Gallegos, 2009, Robb, 2008, Newman, 2009, Killalea, 2008, Humphreys and Grieser, 2006, Hoesing, 2006, Hernandez, 2009, Gardner, 2009, Enterprise Management Associates, 2008, Campbell and Jeronimo, 2006, Bass, 2009).	The following controls should be in place: adequate and secure virtualization environment configuration based on approved standards and policies, adherence to change management policies and procedures for VMs and virtual environments, and independent monitoring and control mechanisms to assist with provisioning requests (Ormandy, 2007, Gardner, 2009, Baldwin et al., 2008).
A.5	Complexities such as different virtualization vendors, multiple platforms and lack of visibility and asset tracking could increase company risk of ***non-compliance with licensing or service level agreements*** (Enterprise Management Associates, 2008, Campbell and Jeronimo, 2006) as well as more difficulties concerning security, management and control (VMware Inc., 2006, Senft and Gallegos, 2009, Gardner, 2009, Enterprise Management Associates, 2008, Barrett, 2008).	Management monitors and ensures that information system service level and licensing agreements allow for all virtualization components and requirements (Campbell and Jeronimo, 2006).
A.6	***Audit/event logging*** was cited as a current barrier to virtualization implementation, providing the complexities of the virtual environment. The risk augments even further when management and monitoring tools and controls are not adequate or efficient (VMware Inc., 2006, Enterprise Management Associates, 2008).	Security tools are implemented to record security events (e.g. security violation, unauthorized attempts to access VMs) for the virtual environment. Reports are regularly reviewed and a root cause established where applicable (Baldwin et al., 2008).

Table 3: Logical access risks and mitigating controls.

Ref	Risk	Description of mitigating control
B.1	A risk conveyed through server and hardware consolidation is the ***collapsing of domain, security and network administrator roles***. The virtual administrator is now responsible for the entire virtual environment, creating possible segregation of duty problems. To further augment this risk, segregation of duty problems could also lead to human error (as a result of not being trained properly or not encompassing the required skill), the intentional or unintentional disruption of critical services, and misconfiguration of VMs (Ormandy, 2007, Hoesing, 2006, Campbell and Jeronimo, 2006).	Roles and responsibilities related to virtualization security administration are defined and privileged access limited to appropriate personnel based on approval from management. Privileged access is logged and reviewed on a regular basis (Ormandy, 2007, Hoesing, 2006, Campbell and Jeronimo, 2006, Baldwin et al., 2008).
B.2	Server and hardware consolidation lead to the ***reduction of access controls***. Should an attacker gain unauthorised access to the virtual host, access to all VMs on that host are compromised. Also, a VM image is essentially a file containing data. The data could therefore be copied and run in an unsecure environment circumventing security controls and providing a means for unauthorized access to data (Ormandy, 2007, Hoesing, 2006, Campbell and Jeronimo, 2006, Berman, 2009).	Logical security tools and techniques are implemented to restrict access to the virtualization layer, virtual hard disks, VM images, data storage, VM backups, and VM management and monitoring tools (Ormandy, 2007, Hoesing, 2006, Campbell and Jeronimo, 2006, Baldwin et al., 2008).

security and network administrator roles (B.1) and the reduction of access controls (B.2).

5.3 Network Security

Consolidating multiple physical servers onto a single virtual server hosting several VMs could lead to a number of network related risks (C.1). These *network security* virtualization risks and the recommendations for mitigation of these risks are detailed in Table 4.

5.4 Physical Security

With the disappearance of physical data centre perimeters, attackers could gain access to VMs from anywhere in the network (D.1). The *physical security* virtualization risk and the recommendation for mitigation of this risk are detailed in Table 5.

5.5 Change Control

Changes are easily distributed to end-users as a single, tested and approved virtual machine image (Bass, 2009, Campbell and Jeronimo, 2006, Enterprise Management Associates, 2008, Gardner, 2009, Hernandez, 2009, Hoesing, 2006, Humphreys and Grieser, 2006, Killalea, 2008, Newman, 2009, Robb, 2008, Senft and Gallegos, 2009, Sgallari, 2009, Strom, 2008, VMware Inc., 2006).

However, *change management* could become cumbersome when the following risks, as described in Table 6, are considered: changes to virtualization firmware affecting all VMs on a physical host, server sprawling, duplicability of VMs, inadequate planning and change management procedures, and unsupported legacy applications (E.1).

Table 4: Network security risks and mitigating controls.

Ref	Risk	Description of mitigating control
C.1	Consolidating multiple physical servers onto a single virtual server hosting several VMs could lead to a number of risks. Firewalls, intrusion detection and other protections (as known in non-virtualized environments) are eliminated within the virtual environment, implying the spreading of viruses and malicious software between VMs on the same VLAN. There is also little or no visibility to detect these viruses or malicious software. Unsecure or compromised VMs can further serve as backdoors to the whole virtual environment (VMware Inc., 2006, Ormandy, 2007, Hoesing, 2006, Enterprise Management Associates, 2008, Campbell and Jeronimo, 2006, Barrett, 2008).	Network controls are in place to secure systems and prevent unauthorised use, disclosure, damage or loss of data. Traffic between VMs is monitored to detect any malicious software or viruses.

Table 5: Physical security risks and mitigating controls.

Ref	Risk	Description of mitigating control
D.1	***Physical perimeters pertaining to data centers*** become extinct in virtual environments. Attackers could gain access to VMs from anywhere in the network (Ormandy, 2007, Hoesing, 2006, Campbell and Jeronimo, 2006, Baldwin et al., 2008).	Network level security (see *C.1* above). Network communication between guest VMs should be isolated (example of a tool to use: vShield zone from VMware).

Table 6: Change management risks and mitigating controls.

Ref	Risk	Description of mitigating control
E.1	Changes to ***virtualization firmware*** could affect all VMs running on a physical host. ***Server sprawling*** could lead to reduced visibility of VMs, therefore increasing the risk of VMs not being patched or updated appropriately and in a timely manner to guard against exploits and known vulnerabilities. The easy ***duplication of VMs*** to serve as testing and development environments could pose an easy target to obtain sensitive information as stringent security policies are not always applied to these environments. The simplistic nature of applying changes in a virtual environment could mean that ***proper planning*** does not take place and ***change management procedures*** are not adhered to, leading to insecure setup and misconfiguration. Inadequate patching or updating of the host machine could affect multiple VMs residing on the host (VMware Inc., 2006, Millard, 2008, Enterprise Management Associates, 2008, Campbell and Jeronimo, 2006, Barrett, 2008). Most of the time ***legacy applications*** are ***not supported*** by any vendor, and since patches or upgrades are not produced for known vulnerabilities it therefore also increases security-related risks (Enterprise Management Associates, 2008).	All changes to the virtual environment (virtualization layer, host, resources, VMs) are appropriately managed to minimize the likelihood of disruption, unauthorized changes, or errors (i.e. buy-in from stakeholders, compliance with policies and standards, validation and testing of changes in separate development and testing environments, formal approval and acceptance of changes, and adequate security around migration to production) (Ormandy, 2007).

Table 7: Management and monitoring risks and mitigating controls.

Ref	Risk	Description of mitigating control
F.1	Risks include ***complexity*** (monitoring each layer in the virtual configuration), ***single point of failure***, ***segregation of duties***, ***dynamic environment*** leading to poor visibility, virtualization layer ***abstracting rapidly*** and ***reduced supervision***. An added difficulty is also how to ***manage and administer*** both ***physical and virtual environments*** simultaneously since virtualization creates an extra layer inside the IT infrastructure. IP address, for instance, is not regarded as a reliable VM identifier in a highly dynamic environment (Humphreys and Grieser, 2006, Enterprise Management Associates, 2008, Campbell and Jeronimo, 2006, Barrett, 2008).	Independent management and monitoring tools are implemented and provide for strong control and compliance reporting. Management tools should be located in isolation, separate from the virtual environment, to limit the risk of unauthorized access to administration functionality (an example of such a tool is vSphefer (VMware) which includes monitoring of the hypervisors and VMs) (Baldwin et al., 2008).

5.6 Management and Monitoring

Management and administration of the virtual environment is made easier through consolidation (reducing the number of servers to maintain and monitor), higher availability, easier and quicker deployment, flexibility and service agility, seamless duplication, portability and migration, effective development and testing, and powerful debugging and performance monitoring capabilities (Campbell and Jeronimo, 2006, Gardner, 2009, Humphreys and Grieser, 2006, Strom, 2008, VMware Inc., 2006).

However, risks augment if management and monitoring tools are not used properly and regularly. The *management and monitoring* virtualization risks and the recommendations for mitigation of these risks are detailed in Table 7. Such risks are complexity, single point of failure, segregation of duties, poor visibility, virtualization layer abstracting, rapidly and reduced supervision, and managing and administer both physical and virtual environments (F.1).

6 CONCLUSIONS

Cloud computing and virtualization will continue to have an important role and increasing impact on the IT landscape. Cloud computing predictions for growth indicate substantial developments for and implementations of cloud computing services. Virtualization is regarded, in many instances, as a core component for the enablement of cloud computing.

In this paper, we provided an overview of virtualization benefits and security risks as a general guideline to assist management in the implementation of virtualization processes, procedures and controls. The fact that virtualization makes it possible to consolidate multiple operating systems and applications onto a single server has given rise to significant benefits, including hardware and server utilization, and the reduction of hardware, administration and management, energy efficiency, software costs and the enablement of services through cloud computing.

Because of the importance of virtualization in cloud computing environments, adequate and effective management and control around virtualization security risks are imperative to ensure the safeguarding of IT resources and data. Consideration should be given to risks to ensure completeness, integrity and availability of applications and data.

In this paper, we suggested a number of controls that could be considered for the mitigation of virtualization security risks. The controls included those related to security administration and control, logical access, network security, physical security, change control, and management and monitoring.

Further research focuses on the development of a complete risk and control framework for cloud computing and virtualization to provide management with guidelines and control standards to deal with cloud computing and virtualization risks coherently.

REFERENCES

Avanade. (2009). *2009 Global Survey of Cloud Computing*. Available: http://avanade.dk/_uploaded/pdf/avanadethoughtleadershipcloudsurveyexecutivesummary833173.pdf [Accessed 15 June 2010].

Baldwin, A., Shiu, S. & Beres, Y. (2008). *Auditing in shared virtualized environments*. Palo Alto: Hewlett Packard Development Company, L.P. Available: http://www.hpl.hp.com/ [Accessed 12 February 2009].

Barrett, L. (2008). Virtualization Craze Brings the Bad with the Good. *What to Expect With Virtualization.* Jupitermedia Corp.

Bass, R. (2009). Windows Virtualization - Get Started With Hyper-V. *Getting Started with Virtualization.* Jupitermedia Corp.

Berman, M. (2009). *Virtualization Audit 101: The top 5*

risks and recommendations for protecting your virtual IT. Catbird. Available: http://www.wwpi.com/ [Accessed 4 February 2009].

Boss, G., Malladi, P., Quan, D., Legregni, L. & Hall, H. (2007). *Cloud Computing.* IBM Corporation. Available: http://www.ibm.com/developerworks/ websphere/hipods/ [Accessed 20 June 2010].

C.A. Solutions. (2010). *Unleasing the power of virtualization 2010: Cloud computing and the perceptions of European Business.* Islandia, N.Y.: CA. Available: http://www.ca.com/Files/SupportingPieces/ ca_virtualisatn_survey_report_228900.pdf [Accessed 30 April 2010].

Campbell, S. & Jeronimo, M. (2006). Applied Virtualization Technology: Usage Models for IT Professionals and Software Developers. Intel Press.

Carroll, M., Kotze, P. & Van Der Merwe, A. (2010). GOING VIRTUAL - Popular Trend or Real Prospect for Enterprise Information Systems. *ICEIS 2010: Proceedings of the 12th International Conference on Enterprise Information Systems.* Funchal, Madeira, Portugal: 2010 SciTePress – Science and Technology Publications.

Centre for the Protection of National Infrastructure (Cpni). (2010). *Information Security Briefing 01/2010*

Cloud Computing. CPNI. Available: http:// www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf [Accessed 20 June 2010].

Cloud Security Alliance. (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.* Cloud Security Alliance. Available: www. cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf [Accessed 20 May 2010].

Enterprise Management Associates. (2008). Virtualization and Management: Trends, Forecasts, and Recommendations. Colorado: Enterprise Management Associates, Inc.

F5 Networks. (2009). *Cloud Computing Survey: June - July 2009.* Available: www.f5.com/pdf/reports/cloud-computing-survey-results-2009.pdf [Accessed 8 August 2010].

Gadia, S. (2009). Cloud Computing: An Autditor's Perspective. *ISACA Journal,* 6.

Gardner, B. (2009). Planning Data Protection Into Your Virtual Infrastructure. *Getting Started with Virtualization.* Jupitermedia Corp.

Gartner Executive Programs (Exp). (2010). *Gartner EXP Worldwide Survey of Nearly 1,600 CIOs Shows IT Budgets in 2010 to be at 2005 Levels.* Gartner, Inc. Available: www.gartner.com/exp [Accessed 20 August 2010].

Harauz, J., Kaufman, L. M. & Potter, B. (2009). Data Security: The world of cloud computing. *IEEE Security and Privacy,* 61-64.

Hernandez, R. (2009). For Starters: The Virtualization Performance Quandary. *Getting Started with Virtualization.* Jupitermedia Corp.

Hoesing, M. (2006). Virtualization Usage, Risks and Audit Tools. *Information Systems Control Journal,* 3, 1-2.

Humphreys, J. & Grieser, T. (2006). *Mainstreaming Server Virtualization: The Intel Approach.* Framingham: IDC Information and Data. Available: http://i.i.com.com/ [Accessed 3 July 2009].

Isaca. (2009). *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives.* ISACA. Available: http://www.isaca. org/AMTemplate.cfm?Section=Deliverables&Templat e=/ContentManagement/ContentDisplay.cfm&Content ID=53044 [Accessed 15 April 2010].

Killalea, T. (2008). Meet the Virts. *ACM Queue,* 6, 14-18.

Mell, P. & Grance, T. (2009). The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Information Technology Laboratory.

Millard, E. (2008). Virtualization's Challenges & Benefits. *Processor,* 30, 28.

Newman, A. (2009). Build a Solid Virtual Foundation. *Getting Started with Virtualization.* Jupitermedia Corp.

Ormandy, T. (2007). *An empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments.* Google, Inc. Available: http://taviso.decsystem.org/ [Accessed 10 February 2010].

Ponemon, L. (2010). *Security of Cloud Computing Users: A Study of Practitioners in the US & Europe.* Ponemon Institute. Available: http:// www.ca.com/~/media/Files/IndustryResearch/security -cloud-computing-users_235659.pdf [Accessed 29 September 2010].

Robb, D. (2008). Virtualization Enters the SMB World. *What to Expect With Virtualization.* Jupitermedia Corp.

Senft, S. & Gallegos, F. (2009). Information Technology Control and Audit. Third ed.: Auerbach Publications.

Sgallari, L. (2009). Reducing Infrastructure Cost Through Virtualization. *The Architecture Journal,* 20, 33-43.

Stratus Technologies. (2009). *Server Virtualization and Cloud Computing: Four Hidden Impacts on Uptime and Availability.* Stratus Technologies Bermuda Ltd. Available: http://www.status.com [Accessed 8 August 2010].

Strom, D. (2008). Virtual Servers Update: VMware vs. Microsoft vs. Xen. *What to Expect With Virtualization.* Jupitermedia Corp.

Sun Microsystems Inc. (2009). *Take your business to a higher level.* Sun Microsystems Inc.,. Available: https: //slx.sun.com/ [Accessed 17 July 2009].

VMware Inc. (2006). *Virtualization Overview.* California: VMware Inc. Available: http://www.nitro.ca/ [Accessed 3 July 2009].