Suggestion of Security Audit Framework for Virtual Desktop Infrastructure

A Case Study of Citrix XenDesktop

Jun Pan, Sergey Butakov, Ron Ruhl and Shaun Aghili
Department of Information Systems Security and Assurance
Concordia University College of Alberta, Edmonton, Canada
jpan@student.concordia.ab.ca, { sergey.butakov, ron.ruhl, shaun.aghili }@concordia.ab.ca

***Abstract*—Traditional desktop infrastructures evolve to incorporate new paradigms such as Virtual Desktop Infrastructure (VDI) since it improves agility, security and productivity for business. VDI also creates additional security challenges and risks including data leakage, lack of visibility, and single point of failure and shielding critical desktops. Knowing this and having a well-developed security governance strategy in place is critical for success. This paper uses *COBIT 5 for Assurance* and *COBIT 5 for Risk* as guidance to develop a security audit framework illustrated by an audit program in Citrix XenDesktop VDI environment. The proposed audit framework can assist organizations to mitigate the risk and optimize the performance of VDI deployment.**

Keywords—VDI Security; VDI Audit; COBIT5; Virtual Desktop Infrastructure; Desktop virtualization

I. Introduction

Virtualization technology has been revolutionizing IT in many ways. The success of server virtualization in many organizations has moved their attention to the desktop. The desktop environment is going through a transformation from an environment primarily relied on a personal computer running desktop applications to an environment where users are expected to access the corporate resources (data, applications) from anywhere and anytime with any devices (desktop, laptop, tablets, and cell phones) [1]. VDI incorporates needs of both IT and end users, and it enables mobile work styles by delivering windows desktops as mobile services.

VDI is a virtualization technology that enables desktops to be accessed, supported and managed from central servers hosted in a datacenter through a remote device [2]. Users connect to the virtual desktop over LAN, WAN or Internet. VDI has attracted a lot of interest from companies of all sizes because of its obvious business such as operational improvement, cost saving, compliance requirement and increased security [3]. More organizations are considering the operational and security reasons for moving to VDI since hardware acquisition cost is reduced by extending the useful lifecycle of desktop and laptop hardware instead of replacing obsolete physical computers [4]. Some companies deploy a centralized VDI environment that can be accessed by relatively low-cost terminals, and Bring Your Own Devices (BYOD) becomes possible with implementation of VDI [4]. One of the obvious areas of growth is to use tablets like iPad to access virtual desktops hosted in a datacenter to carry various tasks. Additional cost benefits can be achieved by reducing recurrent desktop management tasks; for instance, centralized patch management and the deployment can be rolled out in a short time. VDI can lower the cost of compliance and increase security for desktops [3]. It provides major shift from the distributed desktop environment to the centralized environment to standardize the enterprise's compliance policy through centralized configuration and control in the datacenter.

The common VDI implementation includes core components as Figure 1 illustrates, and specific Citrix architecture is included in the bracket [4].

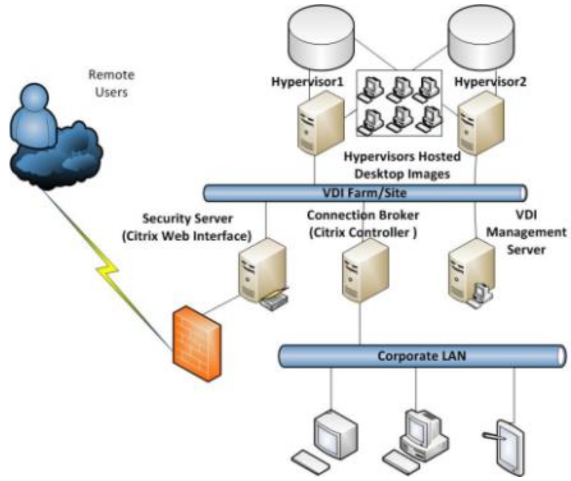
Remote Users
Hypervisor1
Hypervisor2
Hypervisors Hosted Desktop Images
VDI Farm/Site
Security Server (Citrix Web Interface)
Connection Broker (Citrix Controller)
VDI Management Server
Corporate LAN

Figure 1 Core components of an average VDI implementation

The first components all VDI users encounter are **clients,** and this could be Remote Desktop Protocol (RDP) client or a proprietary client such as Citrix Receiver or VMware View Client. Proprietary clients can provide user High Definition Experience (HDX) including video, audio and 3D graphics.

Security Server/Gateway handles the encrypted traffic from VDI clients via SSL/TLS on the Internet. In addition, the security server/gateway also denies and accepts client requests based on user identity and passes them to VDI site. In Citrix architecture, this component is called “Web Interface” in XenDesktop 5.X and “StoreFront” in 7.X.

Connection Broker authenticates users, manages the assembly of user’s virtual desktop environments, takes all the incoming requests and directs the request to the appropriate virtual desktops. Broker communicates with security server to obtain the required policies and manages the “shelf life” of each desktop [4]. Additionally broker determines whether users receive a desktop from a shared pool of virtual machines or a dedicated virtual desktop. Citrix Desktop Delivery Controller (DDC) and VMware Horizon View Connection Server are some examples of connection brokers.

Hypervisor and **storage** are inevitable component in this infrastructure. VDI architecture uses the hypervisor to host multiple desktop virtual machines as well as a large-scale storage to store desktop image files. VMware VSphere®, Citrix XenServer®, and Microsoft Hyper-V® are the most popular choices for hypervisors.

Virtual Desktop is the last component of the environment. Virtual machine contains the user’s configuration and data [2].

Gartner estimates that approximately 15 percent of current worldwide traditional professional desktop PCs will migrate to VDI by 2014, and the worldwide Virtual Desktop Market will surpass $65 Billion in 2013 [5]. Although there are many advantages, VDI is not risk-free or completely secure. Enterprises have to accept additional risks and security concerns when enjoying VDI benefits. The security challenges brought to organizations by this technology includes data leakage, IT governance complexity, single point of failure and shielding critical desktops [3]. VDI solutions are offered by various software vendors, including Citrix, VMware and Microsoft. According to the IDC research, Citrix’s VDI solution-Citrix XenDesktop is positioned in the 2011/2012 IDC MarketScape Leaders Category for Client Virtualization, and VMware Horizon suite (formally called VMware Viewer) ranks the second position in the leader’s category [6]. Although Citrix is the largest player in the VDI market, no in-depth security guidance for its VDI solutions is available either from the vendor or other parties; therefore Citrix XenDesktop has been chosen as a case study for this research.

The objectives of this research are to assess risks related with VDI implementation and to develop an audit framework for VDI in the Citrix XenDesktop environment based on *COBIT 5 for Assurance* and *COBIT 5 for Risk*. The research starts with the introduction of VDI and is followed by review of related research works in Section II. Section III attempts to analyze major VDI security risks with mitigation suggestions by adopting risk scenarios categories from *COBIT 5 for Risk*, and those risk areas should be given special attention when developing security audit instances. The audit methodologies based on *COBIT 5 for Assurance* is analyzed in section IV. Section V and VI present a template of refined audit scope with selected instances and assessment criteria illustrated by COBIT 5 enablers for Citrix XenDesktop as a case study. At the same time, a virtual lab as described in section VII has been used to verify some of the controls described in the assurance steps. Section VIII concludes the paper with the summary of the work has been done.

II. Related Work

The review of relevant literature has been organized into following four subsections in order to understand VDI security audit.

A. *Knowledge of VDI Security*

Special security concerns for VDI environments include types of virtual desktop groups, linked clone and firewall arrangements.

There are two major types of VDI desktops that can be deployed- persistent desktops and ephemeral desktops [4]. A persistent desktop is similar to a traditional desktop; a user’s change can be retained once logged off. Ephemeral desktops, also called hosted shared desktop group, which are provisioned each time when user logs in, provide a lock-down of standard applications to all users since the desktop will be reset once the user is logged off [7]. It is crucial for the audit professional to understand the difference between the desktops types when developing a VDI audit plan.

“Linked clone” is another important knowledge which does not exist in either a virtualized server or a traditional desktop environment. One of the advantages of “Linked clone” is that the disk usage of a linked clone virtual machine is far less than a full clone of the new virtual machine [2]. Another advantage of “Linked clone” technology is that patch management and configuration change are accelerated. “Linked clone” also creates new security implications for VDI. ISACA concluded this as one of the risks areas introduced by adopting VDI [3].

In order to secure VDI environment, firewall access control has been suggested between the VDI environment and the production assets [4]. The control has been further illustrated by implementing multiple firewalls to protect VDI environments [2]. The detailed three levels (External FW, Broker and Production) firewall solutions were illustrated in Figure 2. In this manner, organizations’ networks have been segregated into three zones, and it would be quite easy to create VDI implementation of different classification levels. (Figure 10.7 [2])

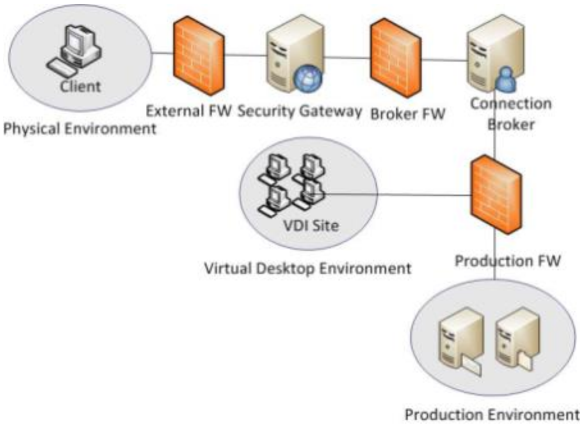

Figure 2 VDI implementation with multiple firewalls

B. *IT Security Audit for Virtual Environments*

The papers directly related to VDI audit are very scarce since VDI is an emerging technology. Security risks in virtual IT systems have been classified into three types: Architectural vulnerability, Software vulnerability and Configuration risks [8]. The category of the risk areas can be referenced for classification of VDI risks in this paper. The authors also present the significant audit points which can serve as guidelines, benchmarks and best practices for virtual IT system. Some of those audit points are also relevant in VDI environment.

C. *Security Audit Framework*

The third part of the review was the existing security audit framework since a framework is very crucial to develop and manage any audit programs. These frameworks are a "blueprint" for building an information security program to mitigate risk and reduce vulnerabilities, and they enable a quick start, not from a scratch, but with a framework and resources that have been tested and are used by peers.

The first framework reviewed is NIST 800-53, which outlines controls needed to be compliant with the Federal Information Security Management Act of 2002, developed by the National Institute of Standards and Technology (NIST). NIST 800-53 is a comprehensive collection of recommended security controls, but it applies to Federal government agencies only.

Alternatively, there is guidance for information security management systems auditing ISO 27000 series developed by the International Standards Organization (ISO). ISO 27000 provides a broad information security framework that can be applied most of organizations and can be considered as the information security equivalent of ISO 9000 quality standards for manufacturing [9]. Although ISO 27000 is best used where a company needs to promote information security capabilities through the ISO 27000 certification, it’s not granular enough to be used to develop a technology based security audit program like VDI audit.

The third framework, Control Objectives of Information and related Technology (COBIT), is a framework and set of control objectives developed by the Information Systems Audit and Control Association (ISACA). This framework started out primarily focused on reducing technical risks in organizations, and has evolved recently into COBIT 5 which includes alignment of IT with business-strategic goals. COBIT provides a checklist and process approach to IT governance with a list of control objectives that must be accomplished according to goals defined. COBIT 5 has been taken consideration as guidance for security audit framework for this research.

D. *Relevant Security Audit Programs*

Among SANS audit programs, Security Audit of Citrix NFUSE Server is a typical technical audit of the IT infrastructure system could be used as a reference [10]. Citrix NFUSE Server allows users to access their applications through the web, and this is Citrix’s virtualization solution in an early stage. The audit programs starts with risk analysis and a developed audit checklist in section 2. The audit checklist comes up with reference, risk areas, compliance with illustrated test method, evidence and findings, which are quite practical. Another template with test objectives, stimulus response, actual outcome and assessment, was presented in the third section. The approach conducted is quite comprehensive, but it lacks the support of a well-accepted security audit framework as methodology. Therefore, the developed audit program is subjective in nature. Furthermore, the program is purely process-based with technology audit items. The audit item has been illustrated in too much detail with graphical steps, which are beyond auditor’s capacity.

ISACA has released a number of audit/assurance (AA) programs served as a tool for the completion of a specific assurance process. Among those AA programs, VMware Server Virtualization AA Program published in 2011 is one of the most relevant researches that can be used as the reference for developing VDI Audit program [11].

The template of program steps used by VMware Virtualization Server is not much different with other ISACA’s COBIT assurance framework programs. However, the scope of the audit is focused on the governance, configuration and management of the relevant VMware virtualized servers in the enterprise, with emphasis on control issues specific to virtualized environments. VDI is similar to server virtualization because numerous VMs are being hosted on clusters of hypervisors [4]. Therefore, those security assurance areas are also very beneficial for the development of VDI audit. For instance, the control item “4.3.1 VM Maintenance” can be used as a reference guide when developing audit considerations for Virtual desktop in this research. There are also significant differences between desktop and server virtualization from the assurance perspectives. In addition, ISACA’s audit program is based on COBIT 4.1 release.

In [2] and [4], the authors recommend some security controls for VDI, but no structured security risk analysis and security assurance guidance are provided. The inherent risks and risk mitigation guidance was discussed in [8], but this paper does not cover desktop virtualization environment. This research attempts to focus on the desktop virtualization with risk analysis and proposes a structured audit framework based on the latest version of COBIT framework - COBIT 5. Citrix XenDesktop is used as a case study. The proposed audit framework is helpful for the development of security audits for any VDI solutions.

III. VDI Security Risks Analysis

A risk-driven approach is used to develop the security audit program in this research. As indicated by literature review from a risk analysis perspective, server virtualization has attracted more attention than desktop virtualization. However, there are several key differences between server and desktop virtualization as summarized in Table 1.

Table 1 Key difference between server and desktop virtualization

Category	*Server Virtualization*	*Desktop Virtualization*	*Related risk category and scenarios*
Master Image	VMs are independent, and no master image was used.	Most VMs are cloned from master image.	Infrastructure Risk -Master Image
Thin Provision	VMs do not use thin provision.	VMs use thin provision	

Category	*Server Virtualization*	*Desktop Virtualization*	*Related risk category and scenarios*
VM Quantity	< 10 VMs per physical server	30-80 VMs per physical server	Infrastructure Risk -Lack of Visibility
Power of VM	VMs remain powered on all the time since the infrastructure and applications hosts	VMs can be powered on or off when not in use	
Monitoring	Focused on Server resources (CPU, RAM, disk usage,etc.)	Focused on user demands.	

In the following section of paper, *COBIT 5 for Risk* is used as guidance for risk analysis. It contains a comprehensive set of risk categories with risk scenarios to help the organization to identify risks [12]. An IT risk scenario is a description of an IT related event that can lead to an uncertain impact on the achievement of the enterprise's objectives. The impact can be positive or negative, and this research is mainly focused on negative scenarios.

The genetic 20 risk categories listed in the Table II applies to all organizations. A bottom-up approach is used to derive the most relevant risk categories with risk scenarios for VDI security audit.

Step 1, all risk scenarios suggested by *COBIT 5 for Risks* have been reviewed, and the most relevant scenarios for VDI in each category were selected for further analysis. Those categories, such as category 13 "Geopolitical" and category 19 "Acts of nature", are not VDI related and have been excluded, since they will not affect the result of the audit.

Step 2, the relevant risk categories have been assigned value with the risk type associated by a professional-Citrix Certified Administrator (CCA) based on the suggestion from [12]. 'P' indicates a primary (higher degree) fit and 'S' represents a secondary (lower degree) fit. Blank cells indicate that the risk category is not relevant for the risk scenario at hand.

Step 3, the risk categories with a high degree fit into at least two risk types (highlighted in Table 2 with grey color) and have been selected for further risk analysis and development of risk mitigation suggestion.

TABLE 2 VDI RISK SCENARIOS MATRIX

COBIT 5 Risk Category Reference	**Risk Scenario Category**	**Risk Type**			**Example Scenario/ Explanation**
		IT Benefit/Value Enablement	***IT Program and Project Delivery***	**IT Operations and Service Delivery**	
01	**Portfolio establishment and maintenance**	P	S	S	•This category is quite relevant in VDI project initiation stage but it is less relevant for VDI security audit.
02	**Program/projects life cycle management**	S	P	S	•There is a VDI project budget overrun.
03	**IT investment decision making**	P		S	•The wrong decision of Anti-Virus Software may infect the VDI performance.
04	**IT expertise and skills**	S	S	P	•There is a lack of VDI training for IT Administrator due to new technology.
05	**Staff operations (human error and malicious intent)**	S	S	P	•User has been assigned to wrong desktop group thus user get the access to unauthorized virtual desktop.
06	**Data breach: damage, leakage and access**	P	S	P	•Sensitive information is accidentally disclosed due to user access virtual desktop via unsecured network.
07	**Architecture**	P	P	P	•There is a potential **single point of failure** due to architecture design of VDI. •VDI in remote office is highly depends on network availability.
08	**Infrastructure**	S	P	P	•**Lack of visibility** due to fast proliferation of virtual desktops. •Takes longer time to identify compromised virtual machine due to **lack of visibility**.
		P	S	P	•**Master image** is corrupted or compromised. This has caused all Virtual desktops fail to start.
09	**Software**	P	S	P	•**Misconfiguration of desktop and user items** cause the loss of data or improper access of virtual desktop.
10	**Business ownership of IT**	S	P	S	•Business does not assume accountability about VDI function requirement.
11	**Supplier selection**		S	P	•Support and services delivered by vendors are inadequate and not in line with the SLA, for instance, the stability of the WAN has affected the connectivity of VDI to remote office.
12	**Regulatory compliance**	P	S	S	•VDI helps to follow the regulatory compliance.
13	Geopolitical				•Not related with VDI.
14	**Infrastructure theft or destruction**	S	S	P	•There is accidental destruction of individual devices. (Data does not remain in device in VDI.)
15	**Malware**	S		P	• There is an intrusion of malware on virtual desktop computer. (Malware will disappear once the non-persistent desktop reboots.)
16	**Logical attacks**	S		P	•There is a virus attack.
17	**Industrial action**	S	S	P	• Key staff is not available through industrial action (e.g., transportation strike).
18	**Environmental**	S	S	P	•VDI datacenter environment has met the regulation requirement.
19	Acts of nature				•Not related with VDI.
20	**Innovation**	P	S	S	•New technology trends for VDI are not identified.

A. Data breach(Category 06 [12])

VDI uses centralized data storage, which significantly strengthens information security, but potential data breach risks are ubiquitous due to following reasons:

*a) Access data from anywhere:*With the mobility initiatives, a substantial percentage of users are likely to require access to their desktops from a remote location, and often over an insecure public network.

*b) Endpoint proliferation:*With the rise of BYOD, a variety of end point devices are expected to connect to the network including those are no longer owned or controlled by the organization. Although VDI can eliminate local retention of sensitive data, compromised client devices still pose a threat to data.

c) Malicious web content: Using Internet from a virtual desktop is not different from surfing the web from a physical desktop; therefore user error and careless browsing can cause the same types of damage as on a conventional desktop.

Mitigation: Organization should promote a security-awareness culture to all employees and develop an effective "Data leakage prevention policy" and "BYOD usage policy or Mobile Device Management (MDM) policy". Furthermore, organizations should implement the VPN solution to encrypt traffic between VDI clients and hosts and using two-factor authentication to protect user identity during VDI login. In addition to all these controls, the login-banner should be in place on all virtual desktops prior to access and warn users about that the system is being monitored to detect inappropriate use and other illegal activity. Although this does not improve security, such information is required by law in some countries when monitoring or auditing is taking place [2].

B. Architecture Risks(Category 07 [12])

Single Point of Failure: With the VDI deployment, organizations have put all their eggs into one basket by implementing centralized VMs in a data center instead of having physical desktop machines residing in every cubical. All user computing relies on VDI since a user does not have the apps and data installed in the endpoint devices.

Mitigation: Organization should develop a proper backup plan for when VDI is down. The response plan should also include a response to the interruption of network since a substantial amount of users need to access VM images concurrently. This will be even vital for branch office users and remote users since they need to have the connectivity to VDI site for operation [4]. In addition, some high availability and disaster recovery options should be considered during the designing, for example, installing the broker software in a physical cluster solution other than virtual machines; site resiliency mechanisms such as site failover [3]. Auditor should check the DRP specific to VDI and evaluate the test result.

C. Infrastructure Risks (Category 08 [12])

VDI also creates some specific risks area that are only specific to VDI solutions:

1) Lack of Visibility

Two factors have caused the lack of visibility compared to other systems. The first is that VDI environments are multi-vendors in nature. For example, the VDI solution is supplied by one vendor (Citrix), the hypervisor by another (VMware) and the SAN storage by another (EMC). There is a server virtualization management tool for the hypervisor (such as XenCenter for Xen Server), an administrator console for connection broker and a network monitoring tool for network. The problem of "Lack of Visibility" is sophisticated because the different admin tools have different capabilities and interfaces. The hypervisor's monitoring tool is used to manage VMs but not users. In order to handle the response from user, the helpdesk has to log in to a broker management interface to determine which user has been assigned, then go to the hypervisor monitor to check the performance of VM again. The issue is mainly because the integration among the diverse tools [13]. Another factor is due to fast desktop provisions, which may cause the organization to lose the visibility of every VM need to be protected for [3]. All this has created a challenge in monitoring due to the lack of visibility.

Mitigation: Organizations should implement a monitoring solution, which covers all aspects of an IT environment, and enable integrating all real-time data within a single tool or console. The proactive monitoring solution can decrease the time required to determine the root cause of an issue [14].

2) Master Image

Master image is similar like the term "Linked clone" talked about in section II, and it is a technology being widely used in many VDI solutions. Master image enables VDI desktops be deployed from a "parent" VM through thin provision. Pooled and dedicated desktop store all changes in a differential disk that is layered on top of the thin provisioned image, but pooled and dedicated desktop groups operate differently after the initial creation. When the desktop reboots, the differential disk of the pooled desktop is deleted, and the user starts with a brand new virtual desktop; but the differential disk of the dedicated desktop is maintained, and all user changes persist [7].

When the master image is updated, the pooled desktop utilizes the latest snapshot during the next reboot, and this makes the configuration change and a patch update can be implemented more easily than ever. However, the dedicated desktop continues to use the original, non-updated image. The desktop management tools should be used in order to make the dedicated desktop synchronize with master image.

Mitigation: New configuration changes and patch management can be easily accomplished through updating master image, but this also creates a significant new threat. The impact will affect all VMs have inherited from parent VM if the master image is corrupted or compromised. Organizations should implement a master image management policy to effectively protect the master image. For instance, the policy should limit the administrators who have the right to update master image; master image backup and master image update have followed the organization's change control policy. Auditor should pay special attention for the difference of patch management through master images update and should review at least one of the change controls for the master image update [15].

D. Software Risks (Category 09 [12])

Software configuration errors will be inevitable in such a fast deployed environment like VDI and include the misconfiguration of desktop and user items.

1) Misconfiguration of desktop items

a) Cut and paste: transfer of user data between the User Device clipboard and the virtual desktop clipboard.

b) Client drive mapping: access to mapped client drives from the virtual desktop.

c) USB devices access: access to attached USB devices from the virtual desktop [16].

Mitigation: The cut and paste, client drive mapping and USB device access functions can be separately enabled/disabled by an administrator either globally (for all desktop users), for groups of desktop users, or for individual desktop users by implementing through desktop policy [16]. In addition, organizations will often require configuring both Active Directory policies and VDI broker policies to create a completely tailored environment. In order to avoid confusion, it is recommended that Active Directory policies only be configured where there is no corresponding policy in the broker level (Citrix XenDesktop Policy) can be used [14].

2) Misconfiguration of User Items

a) User Profile: User profile indicates where users saves their personal data. Roaming profile should be used for non-persistent desktops.

b) User Privilege: users should be granted access to the authorized desktop group only [17].

Mitigation: Organizations should ensure that no data is left in the VM when user logs off from non-persistent desktop pool. For instance, the user data should be saved in a mapped network drive with access right control. User's profile plays a critical role in determining the success of user's experience; thus the user profile solution chosen must align with the personalization characteristics of the user group [16]. Auditor should audit the access control list for various desktop groups and assure the access should be revoked when a user's job function has been changed.

IV. Audit Methodologies

Based on the study of security audit frameworks in section II and following ISACA's approach, *COBIT 5 for Assurance* has been used as the audit methodology for this research. *COBIT 5 for Assurance* builds on the COBIT 5 framework, and it provides guidance on planning, scoping, executing and following up a subject mattered audit topic using a road map based on well-accepted assurance approaches [18].

COBIT 5 for Assurance provides a high level and generic guidance on how to provide assurance over enablers. The seven categories of enablers support the provisioning of assurance over enterprise IT including VDI.

- **Principles, Policies and Frameworks**- VDI-related principles, policies and compliance approach have been identified. For instance, master image management policy.
- **Processes**-The assurance-specific processes that are related with VDI, including sub-process under 5 categories: Evaluate, Direct and Monitor (EVM); Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); Monitor, Evaluate and Access (EVA).
- **Organizational Structures**-The organizational structures that can enable assurance provisioning for VDI. For instance, VDI council is an informal organization group, but it is very effective to deal with VDI affairs. Since the council has included representatives from different IT function groups, they have a regular meeting to follow `up VDI specific issues [19].
- **Culture, Ethics and Behavior**-Guidance on how culture, ethics and behavior can enable assurance provisioning in the enterprise. For example, the culture of IT security importance can reduce the risk of VDI deployment.
- **Information**-Information items can enable assurance provisioning, for instance, the security and architecture design of VDI.
- **Services, Infrastructure and Applications**- A list of selected services relevant for the provisioning of assurance in VDI, for example, Data linkage prevention service or Security token for two factor authentications.
- **People, Skills and Competencies-** Skills and competencies specific to VDI, for example, Citrix authorized administrator training and Citrix Certified Administration (CCA) certification.

This paper uses COBIT 5 for Assurance as a roadmap to obtain assurance objectives over enablers in three phases as shown in Figure 3 (Figure 32 [18]).

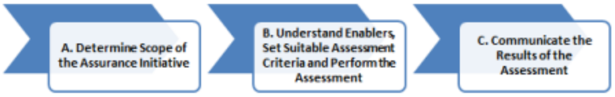
A. Determine Scope of the Assurance Initiative
B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment
C. Communicate the Results of the Assessment

Figure 3 COBIT5-based Assurance Engagement Approach

Phase A and B will be illustrated in section V and VI respectively. In phase C, the assurance professionals who are using this template to conduct the audit will document the gap and communicate with management about the findings. Phase C will not be illustrated in this paper since it is specific to an organization.

This research develops a template of a detailed assurance initiative program based on *COBIT 5 for Assurance* using Citrix XenDesktop as an example. The assurance work program structures an assurance engagement in three major phases, as depicted in Figure 3. The proposed assurance engagement approach refers explicitly to all COBIT 5 enabler categories. There is potential for a lot of duplications when developing the audit/assurance program with all enablers in the scope. In reality, the assurance professional should tailor the audit program to avoid duplication of work. For instance, in this research, the security audit for hypervisors (Virtualization platform) is not included because such program is available from ISACA [11].

V. VDI Audit Program Phase A

The Citrix based example outlined in this paper provides a partially elaborated audit program for the VDI deployment in an enterprise.

The objectives of the audit:

- Access if the deployment of VDI is in line with good practices.
- Evaluate if the deployment of VDI reaches the intended business objectives.
- Effectively manage VDI related risks.

Phase A identifies all COBIT 5 enablers with processes which are related with Citrix XenDesktop. This phase helps to reduce the scope and related assurance engagement efforts by selecting detailed structure enablers or some enabler instances. For most of the enablers, there are several instances in scope. However, only one or a few key instance of each enabler is fully elaborated in this paper due to time and resource constraints.

The scope of the assurance engagement is expressed in function of the seven COBIT 5 enablers, as per the detail in Table 3. In the Guidance column, the shaded text is specific to the example and provides practical guidance, e.g., examples of the processes to include in scope, and setting assessment criteria for the different enablers. Two additional columns are included, in which the assurance professional can identify and cross-reference issues and record comments. The chosen format follows ISACA's recommendations for audit and assurance programs based on COBIT 5 [18].

TABLE 3 CITRIX XENDESKTOP VDI AUDIT PROGRAM PHASE A

Citrix XenDesktop VDI Audit Program Phase A- Define Scope of the Assurance Initiative					
Ref	Assurance Step	Guidance		Issue Cross-Reference or comment	
A	Determine the enablers in scope				
A1	Define the **principles, policies and framwork** in scope.	Following could be considerred in review: • Employee BYOD agreement • VPN Usage Policy • Data Leakage Prevention Policy • Master image management policy • Change Management Policy			
A2	Define which **processes** are in scope of the review	The resulting list contains key processes to be considered during this assurance engagement.			
		Key Process	•APO12 Manage Risk •BAI04 Manage Availability and Capacity •BAI06 Manage Change •BAI10 Manage Configuration •DSS01 Manage Operations •DSS05 Manage Security Service •All MEA process		
A3	Define which **organisational structures** will be in scope.	The following organizational structures and functions are considered to be in scope of this assurance engagement			
		Key Organizational Structures	• IT Security Team • IT Infrastructure Team • VDI Council		
A4	Define the **culture, ethics and behaviour** aspects in scope.	The following enterprise wide behaviors are in scope: • Security awareness exists. • Organizational culture emphasizes security importance. • Management recognizes the need for a secure VDI infrastructure and commits sufficient resources to it.			
A5	Define the **information** items in scope.	Key Information Items	• IT information: -Security design of the VDI application -Architecture design of the VDI infrastructure		
A6	Define the **services, infrastructure and applications** in scope.	• Services in scope: Security monitoring services - Data leakage prevention services • Infrastructure in scope: -Storage systems -Security Infrastructure -Security tokens			
A7	Define the **people, skills and competencies** in scope.	The following skill sets are included in scope: • Security skills • Architectural skills • Risk management skills • Helpdesk Skills			

VI. VDI AUDIT PROGRAM PHASE B

In phase B, the enablers selected in phase A will be further elaborated with assurance steps, guidance and suitable assessment criteria to perform the assessment.

Citrix XenDesktop Security Audit is a technology-based audit program; therefore the focus of the audit is how to use the second enabler- Processes to protect data security. The goal of data security is characterized as the preservation of Integrity, Availability and Confidentiality of the asset [15]. In order to protect the asset, a virtual desktop layer model has been used from the architecture design of the VDI as illustrated in Figure 5 to construct audit instances for process enablers [14].

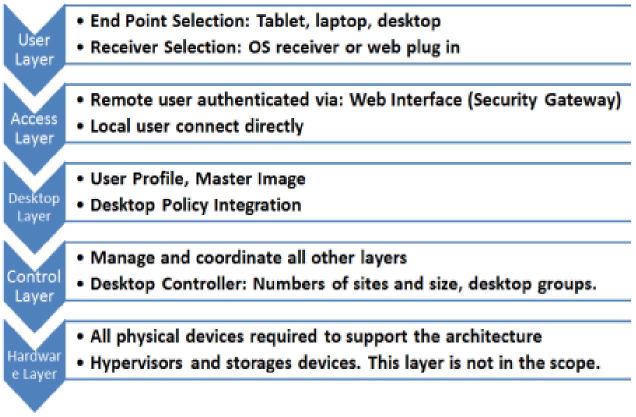
User Layer
• End Point Selection: Tablet, laptop, desktop
• Receiver Selection: OS receiver or web plug in
Access Layer
• Remote user authenticated via: Web Interface (Security Gateway)
• Local user connect directly
Desktop Layer
• User Profile, Master Image
• Desktop Policy Integration
Control Layer
• Manage and coordinate all other layers
• Desktop Controller: Numbers of sites and size, desktop groups.
Hardware Layer
• All physical devices required to support the architecture
• Hypervisors and storages devices. This layer is not in the scope.

Figure 4 Five-layer architecture designs

TABLE 4 CITRIX XENDESKTOP VDI AUDIT PROGRAM PHASE B

Citrix XenDesktop VDI Audit Program Phase B- Understand the Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref	Assurance Step and Guidance		Issue Cross-Reference or comment	
B1	**Obtain understanding of the principles, policies and frameworks in scope and access**.			
Principles, policies and frameworks: Master Image Management (MIM) Policy				
B1.1	Understand good practice and agree on the relevant criteria			
	Good Practice/Criteria	**Assessment Step**		
	• **Comprehensivenness:** The MIM is comprehensive in scope. It covers master image configure, install, clone, in production, change, rollback and retirement.	• Verify with policy or Standard Operation Procedure that the policy is comprehensive in its coverage.		
	• **Currency:** The policy is up to date. This requires at least a yearly validation that the policy is still up to date.	• Verify that the policy is up to date and has a version number. This requires at least a check of when the last update of the policy occurred.		
	•**Availability:** The policy is available to all stakeholders. It is easy to	• Verify that the policy is available to all IT members. • Verify that the policy is easy to		

Citrix XenDesktop VDI Audit Program Phase B- Understand the Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref	Assurance Step and Guidance		Issue Cross-Reference or comment	
	navigate and has a logical and hierarchical structure.	navigate and has a logical and hierarchical structure.		
Repeat steps B1.1 for all remaining in scope A1.				
B2	**Obtain understanding of the processes in scope and set suitable assessment criteria. Assess the processes. For each process in scope (as determined in step A2), additional information is collected and assessment criteria are defined.**			
BAI10 Manage Configuration				
	Reference Process Practice	**Assessment Step**		
B2.1a	**User:** • End Point Device should have Citrix receiver installed to improve performance.	•Select a few samples of users. •Observe the availability of Citrix Receiver in OS.		
B2.1b	**Access:** • Citrix Web Interface has properly configured to grant user access with different End point devices.	• Login assigned Citrix Desktop group with test user to verify the configuration. • Verify the desktop access via different endpoints, including laptop, tablet and mobile device.		
B2.1c	**Desktop:** • Client Cliboard, Client drive maping and USB device redirection should be disabled unless there is a business justification.	•Review Central Configuration Database if available. •Log in to DDC, open desktop policy. •Select "Prohibit" in "Client clipboard redirection", "Client drive redirection" and "Client removable drives". •Verify the setting with sample user.		
B2.1d	•Login banner has been enabled prior logging to Virtual machine	• Access Xendesktop website • Observe the login banner (Some company may choose to implement banner upon login to desktop)		
B2.1f	•Virtual Desktop Access is only available to a user authorised to have access.	• Select a sample of users. • Determine the correct desktop group has been assigned within the user's job function.		
B2.1g	**Control:** •Master image has been setup for pooled desktop group VM update.	•Open Citrix Studio from DDC •Verify the master image being selected in "Machine category".		
BAI06 Manage Change				
	Reference Process Practice	**Assessment Step**		
B2.2	**Desktop:** Master image changes are subject to appropriate review and authorization prior to production.	1. Obtain a copy the documented policy and promoting master image into production. 2. Select a representative sample of master image to production. 3. Determine that policies and procedures have been followed.		
DSS05 Manage Security Service				
	Reference Process Practice	**Assessment Step**		
B2.3a	**User:** •End point computers should have standard ani-virus defense.	•Select samples of users to verify that industry-standard antivirus software is installed.		
B2.3b	**Desktop:** • All virtual desktops have been protected by Antivirus. •Patches update has done throught master image	•Login to virtual desktop to verify Antivirus is installed and the patch is up-to-date. •Review the last patch update log via master image.		
B2.3c	**Access:** •Two factor authentications has been setup for remote access of desktop.	•Verify setting in Citrix Web Interface. •Select samples of users to verify the function of two-factor authentication.		
B2.3d	**Control:** •All data traversing the Internet between the Web Interface (Secure Gateway) and the Endpoint is encrypted using the Secture Sockets Layer (SSL) [17]	•Access the Citrix web gateway via public Internet. •Verify the proper SSL certificate is installed in browser.		
B2.3e	•Communication between user devices and desktops is secured through Citrix Secure ICA which is configured by default to 128-bit encryption.	• Verify "Enable Secure ICA" has been selected in Basic settings of Delivery groups • For details, see http://support.citrix.com/proddocs/topic/xendesktop-7/cds-secure-ica-rho.html#cds-secure-ica-rho		
B2.3g	**Hardware:** •Multiple firewalls should be used to protect VDI farm/site.	• Determine that Virtual desktops are in a less trusted security zone segregated with firewall from production environment.		
BAI04 Manage Availability and Capacity				
	Reference Process Practice	**Assessment Step**		
B2.4a	**User :** •Ensure user experience is optimized for performance.	•Interview for user satisfaction, for instance, the average time for user to log in desktop and the availability of desktops.		
B2.4b	**Desktop:** •Ensure Virtual desktop is available in each desktop groups.	•Obtain the user quantity of different desktop groups from BU. •Login to Citrix Studio to verify the available		
B2.4c	**Access:** •Consider to install the second Web interface (Storefront) Server to provide redundancy and load balance.	• Verify the Solution is being implemented in the organizations. The solution can be build two web interface servers, or Citrix's NetScaler application, or even using windows Network Load Balancing (NLB).		
B2.4d	**Control:** •DCP plan should included specific section for VDI.	•Obtain the latest version of DRP to verify that recovery plan for VDI is included.		
B2.4e	•Appropriate backup plan schedules have been established for VDI.	•Interview with the backup team and verify that VDI has been included in organization's backup plan. •Verify master image is being included in the backup plan.		
B2.4f	•Ensure desktop and application access if Delivery Controllers fail.	• For details, see http://support.citrix.com/proddocs/topic/xendesktop-7/cds-plan-high-avail-vda-rho.html		
B2.4g	**Hardware:** •Create multiple VDI sites or bulid a cluster solution for the DDC to prevent single point of failure.	•Verify the high availability solution is being used in the organization.		
B2.4h	•Enable NIC teaming in windows 2012 server to improve Network performance for VDI [20].	•Verify the setting in windows 2012 server. •The setting can be enabled in hypervisor if the server is a virtual server.		
MEA03 Monitor, Evaluate and Assess Performance and Conformance				
	Reference Process Practice	**Assessment Step**		
B2.5	•An industry-standard monitoring software should be used to monitor the VM performance. IT should look at peak usage times and determine the supply and demand.	• Verify the monitoring solution is being used. • Verify real-time dashboards and regular management report is available. • Select samples of daily, weekly and monthly log		
B3	**Obtain understanding of the organizational structures in scope. Assess the organizational structure**			
Organizational structure: VDI Council (or similar function)				
B3.1	Understand good practice and agree on the relevant criteria			
	Good Practice	**Assessment Step**		

Citrix XenDesktop VDI Audit Program Phase B- Understand the Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref	Assurance Step and Guidance		Issue Cross-Reference or comment	
	•VDI Council has includes all functins of IT department. •Regular meetings take place and meeting reports/minutes are available and meaningful.	•Access organization's IT structure and council list. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and meaningful.		
	•IT key executives are the head of the VDI Council	•Access organization's IT structure and council list		
	Escalation procedures: • Escalation procedures are defined and applied	•Verify the existence and application of escalation procedures.		
Repeat steps B3.1 for all remaining in scope A3.				
B4	**Obtain understanding of the culture, ethics and behavior in scope. Assess culture, ethics and behavior.**			
Culture, ethics and behavior: Organizational culture emphasizes security importance.				
B4.1	Understand good practice and agree on the relevant criteria.			
	Good Practice /Criteria	**Assessment Step**		
	•**Awarenness:** IT Security awareness training (include VDI) has been included to new emplyee orientation training.	•Obtain training program. •Determine that the content of the program has addressed security policy including VDI. •Inspect attendance logs.		
	•**Incentives and rewards:** Management has a policy of rewarding employees who obtain specific certification in the area of IT Security.	•Verify that management has a policy of recognizing and rewarding employees who obtain specific certification in the area of IT governance and security.		
Repeat steps B4.1 for all remaining in scope A4.				
B5	**Obtain understanding of the information items in scope. Assess information items.**			
Information item: Architecture design of the VDI infrastructure				
B5.1	Understand good practice and agree on the relevant criteria			
	Good Practice	**Assessment Step**		
	•**Accuracy** The Architecture information is accurate (cofirm through audit).	•Verify that architecture information is accurate based on confirmed actual data.		
	•**Completeness** The latest VDI diagrams should include sites, DDC, hypervisors, storage.	•Obtain the latest architectural diagrams of the VDI environment.		
	•**Currency:** The documentation should be updated when there is a change.	•Verify the document is updated and has a version number.		
Repeat steps B5.1 for all remaining in scope A5.				
B6	**Obtain understanding of the services, infrastructure and applications in scope and access.**			
Services, infrastructure and applications: Data leakage Prevention (DLP) Service				
B6.1	Understand good practice and agree on the relevant criteria			
	Good Practice	**Assessment Setup**		
	•**Service definition:** The DLP serives is clearly defined and the service is available in all virtual desktops.	•Access the DLP solution being used •Verify DLP service is available in all desktops		
	•**Use:** The scope of the service is clearly defined, for instance when it needs to be used and by whom.	•Verify that the use of the service is clear, i.e., users are aware of that there is such a service in place. •Verify that the actual use is in line with requirements.		
Repeat steps B6.1 for all remaining in scope A6.				

Citrix XenDesktop VDI Audit Program Phase B- Understand the Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref	Assurance Step and Guidance		Issue Cross-Reference or comment	
B7	**Obtain understanding of the people, skills and competencies in scope. Assess people, skills and competencies.**			
People, skills and competencies: Helpdesk Skills				
B7.1	Understand good practice and agree on the relevant criteria			
	Good Practice	**Assessment Step**		
	•Helpdesk has received sufficent training to handle VDI related support requests.	•Obtain a sample of VDI-related help desk requests to indicate whether the request was resolved within the service level agreement(SLA)		
	•Citrix Director has been rolled out for troubleshooting problem.	•Verify the access of the Director console with one of the helpdesk staff •The Director Console can be open via URL: https://<yourservername>Director		
Repeat steps B7.1 for all remaining in scope A7.				

VII. EXPERIMENT

In order to verify the process practice developed in process enabler, a virtual lab environment has been setup with two Citrix sites (5.6 and 7) by using VMware workstation depicted in Figure 5.

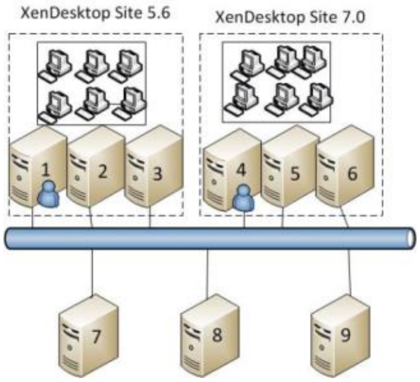

Figure 5 Virtual Lab Components

A. *Virtual Lab Setup and components*

Table 5 Virtual Server Assignment

No.	Server OS	Function of the server	Site Information
1	Windows Server 2008 R2 SP1	Citrix XenDesktop Web Interface	Citrix 5.6
2	Windows Server 2008 R2 SP1	DDC, Studio, Director, SQL Database	Citrix 5.6
3	VMware vSphere 5.1	Hypervisor platform	Citrix 5.6
4	Windows Server 2008 R2 SP1	Citrix XenDesktop Store Front	Citrix 7.0
5	Windows Server 2012 R1	DDC, Studio, Director, SQL Database	Citrix 7.0
6	VMware vSphere 5.1	Hypervisor platform	Citrix 7.0
7	Windows Server 2008 R2 SP1	DC, DNS, and DHCP of Active Directory Domain	Both Sites
8	Windows Server 2008 R2 SP1	VMware Vcenter Hypervisor Management Server	Both Sites
9	Windows 7 Professonal SP1	VDI management Station	Both Sites

B. Audit Findings and Recommendation

An audit has been conducted in order to evaluate the effectiveness of the audit program developed to mitigate the major risks areas identified in section II. Table 6 summarizes the findings and recommendations.

TABLE 6 AUDIT FINDINGS AND RECOMMENDATION

Risk areas with Audit Reference	Audit Findings	Suggestion/Recommendation
Data Breach		
Data Breach B1.1 B2.1c B2.1d B2.3a-B2.3g B6.1	• SSL has been used to encrypt traffic. • AVG Antivirus solution has been installed in virtual desktop, but the update of Antivirus has created unexpected network traffic and disk usage. • Two factor authentications are not being used to protect the user identity. •No data leakage prevention solution is being implemented.	• Installation of a VDI-aware antivirus solution is suggested to avoid the downtime caused by AV storm [21]. •Using two factor authentications is strongly recommended to protect user identity when users access desktop from remote location via unsecured network. •Data leakage prevention service should be in place in virtual desktop.
Architecture Risk		
Single point of failure B2.4c-B2.4g	•Two VDI sites have been implemented to mitigate the risk of single point of failure. •User has to choose the VDI sites manually since two sites are built by two different version of the release.	•Organizations should evaluate the resources and implement either site failover or broker high availability solutions to tackle single point of failure.
Infrastructure Risk		
Lack of visibility B2.5	•The Virtual Lab environment is created by using two vendors' solutions (Citrix and VMware). Therefore, it does create some challenge for visibility capability. Some management tasks need to be done via VMware's tools. •Citrix Director console of v7 has some improvement for the management of VM. Helpdesk can directly find out user's session and launch remote control. The administrator does not require to login to hypervisor's management's console to initialize remote assistance.	•Organizations should evaluate the design of the VDI solution in early stage and try to avoid selecting multiple vendors' solution. For instance, choose the VDI broker and hypervisor solutions from one vendor. • An industry-standard monitoring software solution is highly recommended for better tackling visibility problems in VDI. Organizations may consider using cross-platform virtualization management tools like VMware vCenter Operations Management Suite or Microsoft System Center Operations Manager 2012 [14].
Master image B2.2	•Master image has been used for provision of pooled desktop. •Master image roll out and change are in control. •Master image roll back test is successfully conducted.	•Organizations should pay special attention to the protection of access to the hypervisor's management console since master image update is conducted via this tool. •Segregation of duties: ensure that administrative access for management of servers is separated from administrative access for management of virtual desktop environment.
Software Risk		
Misconfiguration of Desktop items B2.1c	•Security desktop policy is being applied to some desktops. •Security desktop policy (Disable clipboard, USB access) has not been added to the baseline desktop policy.	•VDI Administrator should clarify the default security policy configuration for VDI desktop provisioned. •A baseline desktop security policy should be created and ensure all desktop groups have implemented the policy.

VIII. CONCLUSION

With the state of the desktop shifting from existing on traditional models to VDI, organizations need to have a well-developed AA program in place in order to succeed. Based on the detailed analysis four out of twenty risk areas listed in COBIT 5 were found to be of high relevance to VDI audit and assurance programs: Data leakage, Architecture, Infrastructure and software risks. Using the risks areas and COBIT 5 for Assurance, the paper presented a structured AA program for Citrix XenDesktop environment. The scope of this research covered desktop infrastructure only. Therefore, organizations still have to look into the other areas including the security of hypervisors, storages, and application security in order to address the comprehensive risk areas brought by VDI development.

The future research should follow the trend of VDI deployment. Desktop personalization and support for user customizations with reduced storage of non-persistent desktop are part of the natural evolution [22]. Following this direction, the assurance focus will aim to secure personalized virtual desktop environment without compromising data security.

IX. BIBLIOGRAPHY

[1] L. G. Harbaugh, "Review: Citrix XenDesktop 7 Simplifies VDI," 10 Oct. 2013. [Online]. Available: http://www.edtechmagazine.com/higher/article/2013/10/review-citrix-xendesktop-7-simplifies-vdi. [Accessed 25 Nov. 2013].

[2] E. L. Haletky, "Chapter 10. Virtual Desktop Security," in *VMware vSphere™ and Virtual Infrastructure Security: Securing the Virtual Environment*, Prentice Hall, 2009, pp. 315-342.

[3] N. Zacharopoulos, N. Karatzas and P. Leon, "Virtualized Desktop Infrastructure (VDI)," 2012. [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/VDI_WP.pdf.

[4] D. Shackleford, "Chapter 11: Additional Security Considerations for Virtual Infrastructure," in *Virtualization Security: Protecting Virtualized Environments*, Sybex, 2012.

[5] C. STAMFORD, "Press Release," March 2009. [Online]. Available: http://www.gartner.com/newsroom/id/920814.

[6] I. F. Brett Waldman, "IDC MarketScape: Worldwide Client Virtualization 2012 Vendor Analysis," 2012. [Online]. Available: http://www.citrix.com/content/dam/citrix/en_us/documents/oth/idc-marketScape-2012.pdf.

[7] "Citrix XenDesktop 5 Reference Architecture," [Online]. Available: http://support.citrix.com/servlet/KbServlet/download/30706-102-697507/XD%20-%20Modular%20Reference%20Architecture.pdf.

[8] A. Chaudhuri, S. (. v. Solms and D. Chaudhuri, "Auditing Security Risks in Virtual IT Systems," *ISACA Journal,* vol. 1, 2011.

[9] J. Granneman, "IT security frameworks and standards: Choosing the right one," [Online]. Available: http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one. [Accessed 29 Nov. 2013].

[10] D. J. O'Neill, "Security Audit of Citrix NFUSE WWW Server Published Application Infrastructure," [Online]. Available: http://it-

audit.sans.org/community/papers/security-audit-citrix-nfuse-www-server-published-application-infrastructure_159. [Accessed 25 10 2013].

[11] J. Kalwerisky, "VMware Server Virtualization Audit/Assurance Program," 2011. [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/VMware-Server-Virtualization-Audit-Assurance-Program.aspx.

[12] S. A. Babb, E. Anton, J.-L. Bleicher, S. Reznik, G. Rouissi and A. Tuteja, COBIT 5 for Risk, ISACA, 2013.

[13] I. eG Innovations, "Optimizing the Deployment & Management of Virtual Desktop Infrastructures with the eG VDI Monitor," [Online]. Available: http://www.eginnovations.com/whitepaper/eG_VDI.pdf. [Accessed 29 Nov. 2013].

[14] D. Feller, R. Meesters, R. LaMarca, A. Baker, M. Brooks, E. Duncan, T. Berger and A. Arshed, "Citrix Virtual Desktop Handbook 5.X," 03 Sep. 2013. [Online]. Available: http://support.citrix.com/article/CTX136546. [Accessed 18 Nov. 2013].

[15] R. Janssen, "VDI and security," *Network Security,* pp. 8-11, 03 2010.

[16] G. A. Silvestri, Citrix XenDesktop 5.6 Cookbook, Packt Publishing, 2013.

[17] C. Criteria, "Common Criteria Security Target for Citrix XenDesktop 5.6 Platinum edition," 7 Nov. 2012. [Online]. Available: http://www.commoncriteriaportal.org/files/epfiles/ST271%20v1-1%20for%20Citrix%20XenDesktop%205.6.pdf. [Accessed 25 Nov. 2013].

[18] A. Noble, P. G. Andrews, J. M. Fodor, R. D. Johnson and W. Khalid, COBIT 5 for Assurance, ISACA, 2013.

[19] J. D. Gardner and D. Nordhues, "Client Virtualization best practices," [Online]. Available: http://h20621.www2.hp.com/video-gallery/us/en/bb819a9bc4c2c9f77f6bbeb57fb087f363ee2eda/r/video. [Accessed 10 Nov. 2013].

[20] B. Posey, "Implementing NIC teaming to keep VDI in balance," [Online]. Available: http://searchvirtualdesktop.techtarget.com/tip/Implementing-NIC-teaming-to-keep-VDI-in-balance. [Accessed 19 Nov. 2013].

[21] T. d. Benedictis, C. Hsieh and J. Birnbaum, "Antivirus Best Practices for VMware® Horizon View™ 5.x," [Online]. Available: https://www.vmware.com/files/pdf/VMware-View-AntiVirusPractices-TN-EN.pdf. [Accessed 29 Nov. 2013].

[22] S. Wexler, "Citrix Revolutionizes The Virtual Desktop," 25 Aug. 2011. [Online]. Available: http://www.networkcomputing.com/virtualization/citrix-revolutionizes-the-virtual-deskto/231600134. [Accessed 29 Nov. 2013].