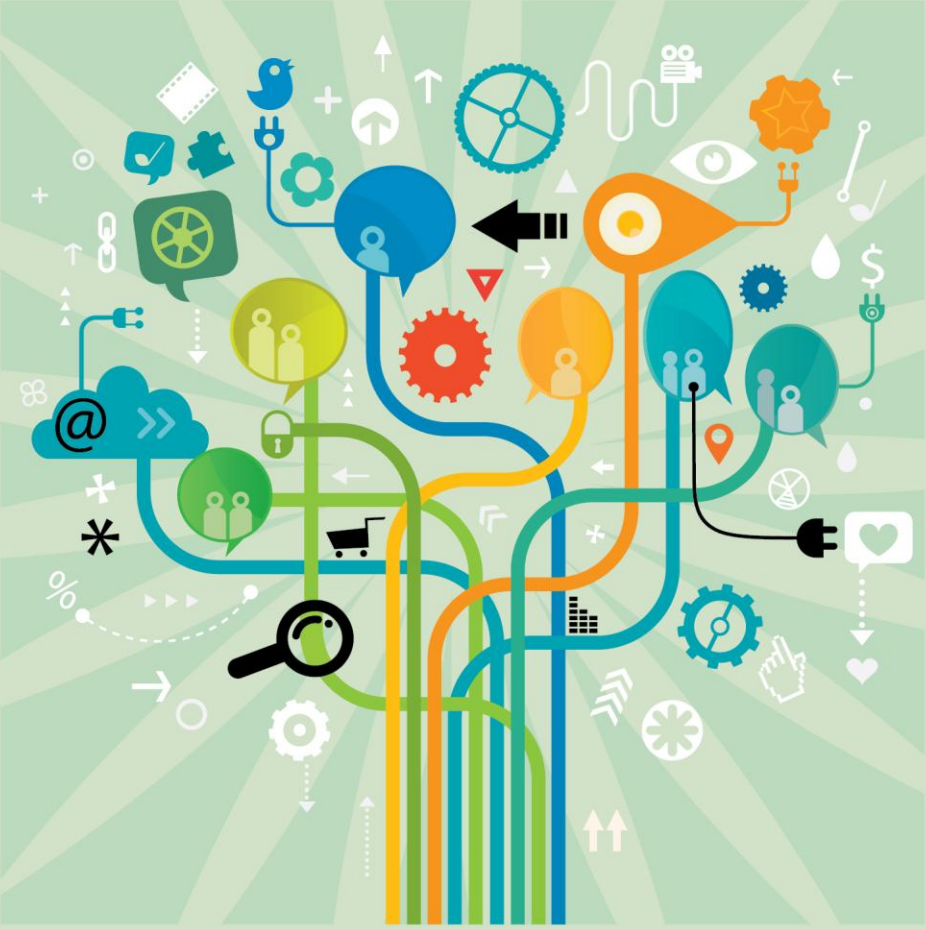
cloud security alliance



Best Practices for Mitigating Risks in Virtualized Environments

April 2015

Acknowledgements

Co-Chairs
Kapil Raina, Zscaler
Kelvin Ng, Nanyang Polytechnic

Contributors
Abhik Chaudhuri, Tata Consultancy Services
Heberto Ferrer, HyTrust
Hemma Prafullchandra, HyTrust
J.D. Sherry, Cavirin
Kelvin Ng, Nanyang Polytechnic
Xiaoyu, Ge, Huawei
Yao Sing, Tao, Infocomm Development Authority of Singapore
Yiak Por, Heng, Nanyang Polytechnic

CSA Global Staff
Frank Guanco, Research Analyst
Victor Chin, Research Analyst

This paper is based on TR 30 : 2012, "Technical Reference for virtualisation security for servers", developed by the Information Technology Standards Committee under the purview of the Singapore Standards Council which is appointed by SPRING Singapore, the national standards body in Singapore. Information on the Singapore Standardisation Programme can be found at:
http://www.spring.gov.sg/Building-Trust/Std/Pages/standards-council-standards-development-organisations.aspx

The virtualization working group is sponsored by

TREND MICRO™
Securing Your Journey to the Cloud

Table of Contents

Scope

This white paper provides guidance on the identification and management of security risks specific to compute virtualization technologies that run on server hardware—as opposed to, for example, desktop, network, or storage virtualization. The audience includes enterprise information systems and security personnel and cloud service providers, although the primary focus is on the former.

1. Introduction

Virtualization has made a dramatic impact in a very short time on IT and networking and has already delivered huge cost savings and return on investment to enterprise data centers and cloud service providers. Typically, the drivers for machine virtualization, including multi-tenancy, are better server utilization, data center consolidation, and relative ease and speed of provisioning. Cloud service providers can achieve higher density, which translates into better margins. Enterprises can use virtualization to shrink capital expenditures on server hardware as well as to increase operational efficiency.

Some think that virtualized environments are more secure than traditional ones for the following reasons:

- Isolation between virtual machines (VMs) provided by the hypervisor
- No known successful attacks on hypervisors[1] save for theoretical ones, which require access to the hypervisor source code and ability to implement it
- Ability to deliver core infrastructure and security technologies as virtual appliances such as network switches and firewalls
- Ability to quarantine and recover quickly from incidents

Others think that the new virtualized environment requires the same type of security as traditional physical environments. As a result, it is not uncommon to see legacy security solutions, processes, and strategies applied to the virtual environment. The bottom line, though, is that the new environment is more complex and requires a new approach to security.

As enterprises embark on their virtualization journeys, it is critical to review existing processes and develop strategies to address security risks across physical and virtual environments in order to ensure compliance and security visibility in the data center.

In the 2013 edition of the *Cloud Computing Top Threats* report by CSA[2], experts identified the following nine critical threats to cloud security (ranked in order of severity):

1. Data breaches
2. Data loss
3. Account or service traffic hijacking
4. Insecure interfaces and APIs
5. Denial of services
6. Malicious insiders
7. Abuse of cloud services
8. Insufficient due diligence
9. Shared technology vulnerabilities

[1] http://www.jwgoerlich.us/blogengine/post/2014/01/03/Attacking-hypervisors-without-exploits.aspx
[2] https://cloudsecurityalliance.org/research/top-threats/

Given the number of notable breaches reported in 2014, virtualization security should be given due consideration in the planning, creation, and management of enterprise and provider environments. This white paper proposes a security framework to help secure your virtual environment and to prevent any threats, including the aforementioned, from exploiting vulnerabilities. This paper primarily considers virtualization security from the hypervisor perspective and briefly mentions related security concerns where appropriate.

2. Securing Virtualization Platforms and Establishing Governance

When an organization embarks on a server virtualization initiative, it must ensure that its information security governance framework also applies to its virtualized IT systems and services. All information security management activities must drive business value.

Security risks and concerns around virtual IT systems can be broadly classified into three types:

1. **Architectural:** The layer of abstraction between physical hardware and virtualized systems running IT services is a potential target for attack. A VM or group of VMs connected to the same network can be the target of attacks from other VMs on the network.
2. **Hypervisor software:** The most important software in a virtual IT system is the hypervisor. Any security vulnerability in the hypervisor and associated infrastructure and management software / tools puts VMs at risk.
3. **Configuration**: Given the ease of cloning and copying images in a virtual environment, a new infrastructure can be deployed very easily. This introduces configuration drift. As a result, controlling and accounting for rapidly deployed environments becomes a critical task.

Enterprises opting for virtualization must identify and assess these security risks and concerns and establish appropriate controls to address them before implementation. ISO/IEC 27001:2013 and ISO/IEC 27005:2011 provide more details on a process that can be used or adapted by enterprises of various sizes and complexities. Some of the key elements to be considered when performing a virtualization risk assessment can be found in Appendix I of this paper.

Delivering enterprise stakeholder value through virtualization initiatives requires good governance and management of information and technology assets. Organizations that choose to virtualize should opt for a comprehensive framework, like COBIT 5, that enables them to meet their technology goals and deliver value. An organization should establish policies and procedures that include an audit program geared to virtual IT systems. Roles and responsibilities of system administrators and users should be clearly defined and documented. An organization should govern a virtualization initiative by evaluating, directing, and monitoring every step in the process. In this context, IT managers must ensure that virtualization policies and procedures are followed by their teams holistically across the enterprise.

During the initiation phase, an organization should identify virtualization needs, providing an overall vision for how virtualization solutions will support its mission; creating a high-level strategy for implementing virtualization solutions; developing virtualization policy and identifying platforms and applications that can be virtualized; and specifying business and functional requirements.

During the planning and design phase, an organization should provide necessary guidance for specifying and evaluating the technical characteristics of the virtualization solution and related components, including authentication methods and cryptographic mechanisms to protect communications. Major considerations include selection of virtualization software, storage system, network topology, bandwidth availability, and business continuity. **The design should also take into account the appropriate logical segregation of instances that contain sensitive data**. Separate authentication should be established for application / server, guest operating system, hypervisor, and host operating system to provide different layers of security and protection. An organization should also define and document processes for handling incidents that involve virtualization solutions.

During implementation, an organization should ensure that sound security practices are established through extensive assessment of the vulnerability of the virtualization components. The underlying virtualization platform should be hardened using vendor-provided guidelines and/or third-party tools. In a virtualized environment, robust key management is essential to access control and proof of ownership for both data and keys. Role-based access policies should be enforced to enable segregation of duties, thereby facilitating proof of governance. Proper data governance measures are required to identify, track, and control where data instances containing sensitive assets reside at any given time. Proper VM encryption is required to significantly reduce the risk associated with user access to physical servers and storage containing sensitive data.

During the disposition phase, tasks should be clearly defined as regards sanitizing media before disposition. The VM retirement process must meet legal and regulatory requirements in order to prevent data leakage and breaches, including shredding or revocation of keys associated with encrypted VMs.

Periodic internal and external audits of the virtualized environment will help identify and mitigate weakness and vulnerabilities and also make it possible to meet legal and regulatory requirements.

3. Virtualization Risks and Controls

This section details the various virtualization risks and recommended security controls for securing a virtualization environment. Key virtualization vendors and other stakeholders assisted in the identification of these security risks and countermeasures.

While virtualization provides numerous benefits through the use of VMs, moving to a virtualized environment does not exempt IT systems from the security risks applicable to such setup in a physical environment. Furthermore, the use of VMs may introduce new and unique security risks or lead to more significant impacts for particular known risks. Consequently, as part of assessing the risks of virtualization, the following should be considered:

Risk 1 – VM Sprawl
Uncontrolled proliferation of VMs can lead to an unmanageable condition of unpatched and unaccounted-for machines.

Risk 2 – Sensitive Data Within a VM
Data confidentiality within VMs can be easily compromised, because data can be easily transported and tampered with.

Risk 3 – Security of Offline and Dormant VMs
Dormant and offline VMs can eventually deviate so far from a current security baseline that simply powering them on introduces massive security vulnerabilities.

Risk 4 – Security of Pre-Configured (Golden Image) VM / Active VMs
VMs exist as files on a virtualization platform, which can lead to unauthorized access, resulting in machine configuration changes or viral payload injection into the platform's virtual disks.

Risk 5 – Lack of Visibility Into and Control Over Virtual Networks
Software-defined virtual networks can cause network security breaches, because traffic over virtual networks may not be visible to security protection devices on the physical network.

Risk 6 – Resource Exhaustion
Uncontrolled physical resource consumption by virtual processes can lead to reduced availability.

A risk factor unique to virtual environments is the hypervisor. Hypervisor is the software and/or firmware responsible for hosting and managing VMs. It provides a single point of access into the virtual environment and is also potentially a single point of failure. A misconfigured hypervisor can result in a single point of compromise of the security of all its hosted components. It does not matter how individual VMs are hardened—a compromised hypervisor can override those controls and provide a convenient single point of unauthorized access to all the VMs. The following security risks related to the use of hypervisor should be considered by those planning to use or currently using virtual technologies:

Risk 7 – Hypervisor Security
Hypervisor security is the process of ensuring that the hypervisor, the software that enables virtualization, is secure throughout its life cycle, including development, implementation, provisioning, and management.

Risk 8 – Unauthorized Access to Hypervisor

Administrative access controls to the hypervisor may not be adequate to protect against potential hacker attacks.

Compared to traditional IT environments, virtualization of IT systems inevitably leads to changes in operational procedures. As a result, some common defense-in-depth practices used in securing physical servers may be affected or ignored, while newly introduced features or functions may expose the environment to additional risks. The following security risks related to changes in operation procedures should be considered:

Risk 9 – Account or Service Hijacking Through the Self-Service Portal

Portal vulnerabilities can lead to privilege escalation attacks.

Risk 10 – Workloads of Different Trust Levels Located on the Same Server

Ensure that there is sufficient security segregation of workloads on a physical host.

Some enterprise infocom personnel may elect to apply virtualization technologies through outsourcing services from cloud service providers. In such cases, it may be necessary to consider additional risk factors, including the following.

Risk 11 – Risk Due to Cloud Service Provider APIs

A hybrid (private / public) cloud virtualization implementation can pose security risks due to account / authentication federation.

Refer to Appendix 1 for an example of risk assessment and treatment of virtualized server assets. Threats to assets and services, their impact on associated processes and ultimately the organization, and the vulnerabilities that can be exploited should be evaluated, in order to compute the level of each risk. For any risk level above the acceptance criteria, responses should be developed to continually monitor and mitigate the risk.

3.1 Risk #1 – VM Sprawl

3.1.1 Risk Table

Risk Name	VM Sprawl
Risk Description	VM sprawl describes the uncontrolled proliferation of VMs. Because VM instances can be easily created and existing instances can be easily cloned and copied to physical servers, the number of dormant VM disk files is likely to increase. In addition, the unique ability to move VMs from one physical server to another creates audit and security monitoring complexity and loss of potential control. As a result, a number of VMs may be unmanaged, unpatched, and unsecured.
Relevant Security Aspect	Risk to confidentiality, integrity, and availability
Relevant Governance Risk Area	Architectural and configuration risk
Vulnerabilities	Proper policy and control processes to manage VM lifecycle do not exist. Placement / zoning policies or enforcement of where a dormant VM can instantiate or reside do not exist. A discovery tool for identification of unauthorized VMs does not exist.
Affected Assets	VM
CCM v3.0.1	CCC-05

3.1.2 Potential security impact

In a traditional IT environment, physical servers must be procured. This requirement enforces effective controls, because change requests must be created and approved before hardware and software can be acquired and connected to the data center.

In the case of virtualization, however, VMs can be allocated quickly, self-provisioned, or moved between physical servers, avoiding the conventional change management process. Without an effective control process in place, VMs and other virtual systems with unknown configurations can quickly proliferate, consuming resources, degrading overall system performance, and increasing liability and risk of exposure. Because these machines may not be readily detectable or visible, they may not be effectively monitored or tracked for the application of security patches or effectively investigated should a security incident occur.

3.1.3 Security Controls for Mitigating Risks

To mitigate risk, consider implementing the following security controls:

- Put effective policies, guidelines, and processes in place to govern and control VM lifecycle management, including self-service and automated scripts / DevOps tools.
- Put effective policies, guidelines, and processes in place to govern and control VM lifecycle management, including self-service and automated scripts / DevOps tools.
- Control the creation, storage, and use of VM images with a formal change management process and tools. Approve additions only when necessary.
- Keep a small number of known-good—and timely patched—images of a guest operating system separately and use them for fast recovery and restoration of systems to the desired baseline.
- Discover virtual systems, including dormant ones and the applications running on them, regularly. Discovering, classifying, and implementing appropriate security controls for each VM and its associated network connections is critical. This process includes quarantine or rollback capability in case of a compromise.
- Use virtualization products with management solutions to examine, patch, and apply security configuration changes to VMs.

3.2 Risk #2 – Sensitive Data Within a VM

3.2.1 Risk Table

Risk Name	**Sensitive Data Within a VM**
Risk Description	VMs containing sensitive data, such as passwords, personal data, bash profiles, bash history files, encryption keys, and license keys, also capture the corresponding data in their images and snapshots. This data is much easier to move as individual files than it is to move the hard disk of a physical server. Snapshots pose even greater risks, because they also contain the contents of memory at the time the snapshot was taken. In addition, if VMs are migrated, data remnants may be exposed in their previous locations.
Relevant Security Aspect	Risk to confidentiality and integrity
Relevant Governance Risk Area	Configuration risk

Vulnerabilities	• VM images and snapshots are not treated the same way as the sensitive data they contain. They are not protected from unauthorized access, modification, duplication, and replacement
	• Policies and procedures to restrict storage of VM images and snapshots do not exist, including:
	  ○ Formal change management processes that govern image creation, security, distribution, storage, use, retirement, and destruction
	  ○ Monitoring and control of stored images and snapshots, including activities logging

Affected Assets	VM and Storage
CCM v3.0.1	IVS-02

3.2.2 Potential security impact

Although VM images and snapshots provide a way to deploy or restore virtual systems quickly and efficiently across multiple physical servers, this capability means that copies of images and snapshots can be removed from a data center easily via USB or the console of a hypervisor installed elsewhere. This removal includes current memory contents, which are not intended to be stored on the storage devices themselves.

In a virtualized environment, therefore, it is no longer possible to ensure that sensitive data such as system password files is safe from unauthorized personnel. This sensitive information and the VM containing it can be moved easily, making it possible to compromise a VM and reintroduce it into the system later.

Without proper controls, security loopholes may exist through the inadvertent capture, storage, and deployment of sensitive information, including rogue virtual instances of critical services. Potential hackers or disgruntled staff can gain access and insert malicious code into VM images and snapshots, which may then be rapidly deployed throughout the environment, resulting in its compromise.

3.2.3 Security Controls for Mitigating Risks

To mitigate risk, consider implementing the following security controls:

- Encrypt data stored on virtual and cloud servers to make it unreadable. Seek a solution that incorporates simple, policy-based key management of data stored in physical, virtual, and cloud servers. Release encryption / decryption keys only to validated and authorized physical or virtual servers. Provide options to manage the keys on premises and/or in the cloud as a service. Leverage a policy-based key management system to determine where and when encrypted data can be accessed. In addition, apply identity and integrity checks when VMs request access to secure storage volumes. We recommend that both boot and data volumes be encrypted.
- Develop policies to restrict storage of VM images and snapshots. If it is necessary to store images and snapshots, proper authorization, such as secondary level of approval, should be obtained and corresponding monitoring and control processes established. To reduce risk, carefully consider where to store these duplicate images or snapshots. For review or audit purposes, mitigation should include logging of activities, as well as establishing a formal image change management process that includes creation, distribution, storage, use, retirement, and destruction.
- Put policies in place to ensure that backup and failover systems, including temporary upgrade / patch instances, are cleaned when deleting and wiping (zero-filling) the VM images. Special care should be taken when using SSD drives to avoid “residual data.”
- Consider using cryptographic checksum protection to detect unauthorized changes to VM images and snapshots.
- Identify critical data files within the VM that may need a higher degree of monitoring as well as log management.

3.3 Risk #3 – Security of Offline and Dormant VMs

3.3.1 Risk Table

Risk Name	**Security of Offline and Dormant VMs**
Risk Description	Enterprises leverage the dynamic nature of VMs by provisioning and decommissioning them as needed for uncontrolled environments, scheduled maintenance, and disaster recovery and to support workers who need computational resources on demand. The state of a VM can range from active (running), to dormant (suspended), to offline (shut down). Dormant and offline VMs can eventually deviate so far from a current security baseline that simply powering them on introduces massive security vulnerabilities. In short, if a VM is not online during deployment or security software updates, it will be unprotected and instantly vulnerable when it comes online. Users running tainted images are exposed to the risk of data theft and corruption.
Relevant Security Aspect	Risk to availability, confidentiality, and integrity
Relevant Governance Risk Area	Architectural and configuration risk
Vulnerabilities	Security patches on the offline or dormant VM are out of date. Guidelines on the activation of offline or dormant VMs do not exist.
Affected Assets	VM
CCM v3.0.1	IVS-02

3.3.2 Potential Security Impact

Dormant or offline VMs can easily be overlooked and left out of the execution of important security procedures. For example, it is likely that a dormant VM will not be updated with the latest security patches. As a result, when the VM is run again, it may be exposed to the latest vulnerabilities. Similarly, dormant VMs may also lack up-to-date access control policy or be excluded from essential security monitoring functions, which may cause security loopholes in the virtualized environment.

Critical infrastructure, management, and security services are increasingly packaged and delivered as virtual appliances. These appliances require proper classification and treatment to prevent rogue instances of non-compliant policies and configurations. In addition, if these appliances are not limited to specific clusters of physical hosts or storage, exposure to risk may increase.

3.3.3 Security Controls for Mitigating Risks

To mitigate risk, consider implementing the following security controls:

- Control the backup, archiving, distribution, and restart of VMs with effective policies, guidelines, and processes such as suitably tagging the VM based on sensitivity / risk level.
- Use virtualization products with management solutions that examine, patch, and apply security configuration changes. While evaluating these products, consider the coverage provided across hypervisors and if there are exceptions in fine print.
- Create a controlled environment to apply security patches and control policies to an offline or dormant VM.
- Avoid problems—systems accidentally or intentionally powered off / deleted or rogue instances—with appropriate architecture and design as well as regular monitoring of virtual appliances that provide critical infrastructure, management, and security services.

3.4 Risk #4 – Security of Pre-Configured (Golden Image) VM / Active VMs

3.4.1 Risk Table

Risk Name	**Security of Pre-Configured / Active VMs**
Risk Description	VMs exist as files on a virtualization platform. Unauthorized access can lead to VM hardware configuration changes or viral payload injection into the virtual disks of an affected VM. In addition, pre-configured VMs may also be subjected to unauthorized changes to hardware or the network or even to viral payload injection. These pre-configured VMs, sometimes known as golden image or VM templates, significantly impact the virtualized environment as new clones are created.
Relevant Security Aspect	Risk to confidentiality, integrity, and availability
Relevant Governance Risk Area	Architectural, software, and configuration risk
Vulnerabilities	Deploying these “compromised” VMs may lead to loss of integrity of the virtualization platform. Unauthorized changes to hardware, network, and storage may impact the availability of a VM. A viral payload injection may impact the entire virtualized environment.
Affected Assets	VM
CCM v3.0.1	IVS-02, IVS-07

3.4.2 Potential Security Impact

Virtual machines exist as files on a virtualization platform. As such, they can be easily transported via physical means or through a network. Unauthorized access through malicious interception can compromise these VM images. Often, golden VM images are made, making it easy to deploy cloned copies and to compromise the integrity of the virtualized environment.

3.4.3 Security Control to Mitigate Risks

To mitigate risk, consider implementing the following security controls:

- Ensure proper hardening and protection of VM instances through VM guest hardening.
- Augment VM operating systems with built-in security measures, leveraging third-party security technology, such as discovery and monitoring tools, to provide layered security controls.
- Consider implementing an integrity checksum mechanism for all VM images.
- Encrypt VM images to prevent unauthorized modification. (Be aware that there may be performance concerns depending on underlying physical server capabilities.)
- Implement strict controls and processes around access, creation, and deployment of VM images/instances.

3.5 Risk #5 – Lack of Visibility Into and Controls Over Virtual Networks

3.5.1 Risk Table

Risk Name	**Lack of Visibility into and Controls Over Virtual Networks**
Risk Description	Lack of visibility into and control over internal software-based virtual networks created for VM-to-VM communications hinders existing security policy enforcement in most organizations. Traffic over virtual networks may not be visible to security protection devices, such as network-based intrusion detection and prevention systems, on the physical network.
Relevant Security Aspect	Risk to confidentiality, integrity, and availability
Relevant Governance Risk Area	Architectural and configuration risk
Vulnerabilities	Virtual networks cannot be monitored in the traditional sense. Inter- VM-to-VM network traffic does not originate from the host and therefore cannot be monitored with conventional network tools. The hypervisor may not be able to intercept and monitor all inter-VM communications. Consistent security policy enforcement cannot be applied on physical and virtual networks. Comprehensive monitoring across physical and virtual networks cannot be implemented. Physical and virtual network configuration may not be managed by the same team
Affected Assets	VM and network
CCM v3.0.1	IVS-06

3.5.2 Potential Security Impact

Traditional IT infrastructure network traffic is monitored and secured as data flows across actual routers, switches, and firewalls. On a virtual network, this can become unmanageable unless the traffic is explicitly redirected to physical or virtual appliances for monitoring. Virtual network configuration can be modified with relative ease; this capability may cause conflicts with actual physical network security policies.

3.5.3 Mitigating Security Controls

To mitigate risk, consider implementing the following security controls:

- Monitor virtual networks and data traffic similarly to physical networks. Organization must carefully determine the tool to use for this task and should configure it with network port mirroring to preferably give a unified view of traffic across physical as well as virtual networks.
- Consider a hypervisor that can monitor each guest operating system—introspection—as it is running if separate tools are not installed to monitor communications between VMs. that are done via memory within the same host instead of through physical network switches
- Implement security technologies that span physical and virtual environments with a consistent policy management and enforcement framework.
- Create consistent security policy and configuration across the physical/virtual network.
- Use VM-specific security mechanisms embedded in hypervisor APIs to provide granular monitoring of traffic crossing VM control and data planes. Leverage tools that implement emerging technologies such as SDN/OpenFlow. These mechanisms will be opaque to traditional network security controls.

3.6 Risk #6 – Resource Exhaustion

3.6.1 Risk Table

Risk Name	**Resource Exhaustion**
Risk Description	In a virtualized environment, software that uses particular physical server resources intensively may exhaust those resources and hence affect VM availability. This condition occurs because the shared environment in a physical server magnifies the severity of resource contention, especially when multiple VMs are running the same resource-intensive software at the same time—as in anti-virus scanning.
Relevant Security Aspect	Risk to availability
Relevant Governance Risk Area	Architectural and hypervisor software risk
Vulnerabilities	Servers can be burdened by concurrent execution of resource-intensive software such as anti-virus software on multiple VMs. Simultaneous automated operating system patches on a group of VMs can create an enormous excess strain on a common storage resource.
Affected Assets	VM
CCM v3.0.1	IVS-05, IVS-04

3.6.2 Potential Security Impact

Resource-intensive software tends to exhaust resources in a physical server when it is implemented in multiple VMs. For example, anti-virus and other security software interrupt every call to disk or memory in order to monitor and prevent security incidents such as hacking or viruses. When anti-virus software runs simultaneously in different VMs on the same physical server, it can potentially consume the host resource pool. Automated operating system patches on a large group of VMs can have the same effect.

3.6.3 Mitigating Security Controls

To mitigate risk, consider implementing the following security controls:

- As per classification of virtual machines based on sensitivity/risk level, put in place suitable resource allocation and/or reservation policies.
- Use resource-intensive software—including anti-virus and other security software—that is virtualization-aware (e.g., anti-virus software that is designed to scan outside individual VMs).
- Implement mechanisms to minimize resource contention. These mechanisms include staggering the scanning of VMs on the same physical server, using agentless deployment of anti-virus software, implementing distributed storage resources, and implementing a workload affinity policy.
- Define and implement a standard operating procedure that detects VMs that are throttled due to resource exhaustion—similar to Denial of service—and puts a remedy in place instantly.

3.7 Risk #7 – Hypervisor Security

3.7.1 Risk Table

Risk Name	**Hypervisor Security**
Risk Description	The hypervisor (or VM monitor) is an additional layer of software between VMs and the underlying hardware platform with or without a host OS. Thus, it is also a surface by which hackers can potentially gain unauthorized access to the VMs—guest OSs—hosted on it.
Relevant Security Aspect	Risk to confidentiality, integrity, and availability
Relevant Governance Risk Area	Architectural and hypervisor software risk
Vulnerabilities	• Hypervisor configuration may not be hardened to reduce areas of vulnerability, such as unused services. • Vendor-recommended best practices have not been adopted. • Unused physical hardware devices are connected, and clipboard / file-sharing services are not disabled. • Vendor security bulletins / alerts are not implemented promptly. • Hypervisor self-integrity checks (or the equivalent) are not conducted upon boot-up. • Ongoing monitoring, including analysis of hypervisor logs, does not occur. • The attack surface is further increased through uncontrolled use of hypervisor management APIs by IT / DevOps tools and scripts and other infrastructure technologies.
Affected Assets	Hypervisor
CCM v3.0.1	IVS-11

3.7.2 Potential Security Impact

A hypervisor can control all aspects of VM operation, so it is a natural target of malicious attacks. Securing a hypervisor is vital, yet more complex than it seems. In an attack known as “hyper-jacking,” malware that has penetrated one VM may attack the hypervisor. When a guest VM attempts this attack, it is often called a “guest VM escape,” because the guest VM breaks out of its isolated environment and attacks the host hypervisor. Once compromised, the hypervisor can be used as an attack platform to compromise guest VMs hosted by it or other hypervisors with which it may be able to interact.

All hypervisors in common use include a very rich set of remote management APIs, increasing their attack surfaces. Calling tools / scripts / applications may not adequately implement identity and access control, especially if a hypervisor uses locally managed service accounts.

3.7.3 Security Controls for Mitigating Risks

To mitigate risk, consider implementing the following security controls:

- Choose a hypervisor with a smaller footprint—Type 1 rather than Type 2—for a reduced attack surface and list of vulnerabilities. (Refer to Appendix II for details.)
- Harden the hypervisor's configuration to reduce areas of vulnerability (e.g., disabling memory sharing between VMs running within the same hypervisor hosts).
- Put vendor-provided best practices in place where applicable.
- Disconnect unused physical hardware devices and disable clipboard or file-sharing services.
- Conduct self-integrity checks upon boot-up to confirm whether or not the hypervisor has been compromised. Use a hypervisor integrity monitoring technology, for example, Intel Trusted Platform Module/Trusted Execution Technology.
- Monitor for signs of compromise by analyzing hypervisor logs on an ongoing basis.
- Subscribe to your hypervisor vendor's security bulletins / alerts and implement security updates promptly.
- Make sure that an effective hypervisor patch management practice is in place.
- Implement and maintain effective identity and access control across all tools / scripts / applications calling hypervisor management APIs. (See Section 3.8 for additional guidance.)

3.8 Risk #8 – Unauthorized Access to Hypervisor

3.8.1 Risk Table

Risk Name	**Unauthorized Access to Hypervisor**
Risk Description	Administrative access controls to the hypervisor may not be adequate for protection against potential hacker attacks. At the same time, hypervisor management software, which is typically used to control and manage one or more hypervisors, is an even more prominent and attractive target for attack. As a result, the hypervisor and associated management software are both subject to risk.
Relevant Security Aspect	Risk to confidentiality, integrity, and availability
Relevant Governance Risk Area	Architectural, hypervisor software, and configuration risk
Vulnerabilities	• Access to the virtualization layer is not restricted as with any sensitive OS (i.e., using console access restricted by firewalls). • The hypervisor may not support role-based access control of administrative responsibilities. • Additional third-party tools designed to provide tight administrative control are not deployed. • Separate authentication is not used to restrict access. • Hypervisor management APIs / CLIs are not adequately protected. • A separate “management LAN” is not deployed to manage access to hypervisors. • Remote management of hypervisors is not disabled. • Administrative interfaces are accidentally exposed through network configuration errors and lack of change management procedures.
Affected Assets	Hypervisor (and its management tool / APIs)
CCM v3.0.1	IVS-11, IAM-04, IAM-13

3.8.2 Potential Security Impact

The hypervisor itself creates a new attack surface that does not exist in traditional IT environments and that is vulnerable to direct attacks. With hypervisor software that uses only locally managed passwords, access control may be too weak to support specific security policies, especially when considering that most hypervisors can be managed remotely. Furthermore, the usual default configuration for a hypervisor is often not the secure one available.

Hypervisors can be managed in different ways, and some hypervisors allow management via multiple methods. In a typical data center, management software is usually not used to manage a group of hypervisors. If management software is not equipped with effective access control, hackers may be able to leverage it to gain unauthorized access to a large number of hosts, eliminating the need to attack individual hypervisors one by one.

3.8.3 Security Controls for Mitigating Risks

To mitigate risk, consider implementing the following security controls:

- Deploy virtualization platforms that support role-based access control of administrative responsibilities. Or consider third-party tools to provide tight administrative control more uniformly across the environment and to reduce the audit burden. For environments with shared responsibilities, consider the two-person rule to provide additional oversight. For example, an authorized contractor can create a network switch only after an authorized network engineer reviews and approves the request.
- Restrict access to the virtualization layer, including hypervisor management software and APIs / CLIs—as with any sensitive operating system—through firewalls that restrict console access.
- Once role-based access control is implemented, evaluate implemented access control policies in order to ensure that they are functionally correct.
- Limit the number of user accounts—including privilege accounts—requiring direct access to the hypervisor host to a bare minimum. Integrate user accounts with robust credential management and authentication systems to enforce security policies (i.e., password policies and use of 2-factor authentication).
- Use multifactor and/or split control authentication, such as Microsoft Active Directory or 2-factor authentication, to restrict access. Refer to ISO/IEC 27002:2013 9.1.1 and 11.1.2 for guidance.
- Implement proper change management on any infrastructure component—configuration, for example—that might accidentally allow unauthorized access to the hypervisor.
- Secure each locally and remotely accessible hypervisor management interface. Disable remote management of hypervisors. If you cannot avoid this, consider providing access over a secure network connection and using 2-factor authentication. In addition, implement management session policies. For example, close idle / inactive connections to prevent abuse of management / client.
- Deploy a separate “management LAN” to manage access to hypervisors.

3.9 Risk #9 – Account or Service Hijacking Through the Self-Service Portal

3.9.1 Risk Table

Risk Name	**Account or Service Hijacking Through the Self-Service Portal**
Risk Description	Access to the self-service portal increases exposure to risks such as account or service hijacking through more administrative privileges than are typically granted to end users.
Relevant Security Aspect	Risk to confidentiality, integrity, and availability confined to the designated virtual environment
Relevant Governance Risk Area	Architectural and hypervisor software risk
Vulnerabilities	• Strong authentication control is lacking. • Policy governing the creation and use of self-service portals does not exist. • Policy-based self-service portal management is not used. • Unauthorized activity is not proactively monitored. • Account management (e.g., password reset sent in clear text) is “relaxed.”
Affected Assets	Applications, VMs, and virtualization platform
CCM v3.0.1	IAM-02, IAM-04, IAM-09, IAM-10, IAM-11, IAM-12

3.9.2 Potential Security Impact

A self-service portal is typically used to delegate specific parts of virtual infrastructure provisioning and management to assigned self-service administrators. Liberal use of self-service portals in cloud computing services will increase susceptibility to security risks, including account or service hijacking.

3.9.3 Security Controls for Mitigating Risks

To mitigate risk, consider implementing the following security controls:

- Use administrative controls selectively, based on users' roles and needs.
- Apply strong authentication techniques where possible, preferably securing both the client and server side of cloud computing against potential attacks. Use a multifactor and/or split control authentication to restrict access. For example, use Microsoft Active Directory or 2-factor authentication. (Refer to ISO/IEC 27002:2013 9.1.1 and 11.1.2 for guidance.)
- Employ proactive monitoring to detect unauthorized activities.
- Evaluate a cloud service provider's security policies and service level agreements.
- Consider policy-based management of self-service portals.
- Review and update policies and guidelines to include creation and use of self-service portals.
- Enforce secure management of accounts, identities, and credentials.
- Conduct regular penetration testing of the self-service portal to uncover vulnerabilities.

3.10 Risk #10 – Workload of Different Trust Levels Located on the Same Server

3.10.1 Risk Table

Risk Name	**Workload of Different Trust Levels Located on the Same Server**
Risk Description	VMs with mission-critical workloads reside on the same host as less-critical VMs, resulting in a virtual environment of mixed trust levels. In a multi-tenant environment, regulatory concerns may warrant segregation with physical or logical mechanisms.
Relevant Security Aspect	Risk to confidentiality, integrity, and availability
Relevant Governance Risk Area	Architectural and configuration risk
Vulnerabilities	• VMs of different trust-levels are hosted on or migrated to the same physical server (host). • Physical or logical software-defined networks for VMs of different trust levels are not segregated. • Physical and virtual firewalls are not deployed to isolate groups of VMs from other hosted groups, for example, production from development systems or development from other cloud-resident systems. • Virtual desktop workloads are not isolated from rest of the physical data center. • Administrative separation of duties may not be implemented, allowing unauthorized changes or accidental misconfiguration that violates the logical zoning.
Affected Assets	VMs on the same physical server
CCM v3.0.1	IVS-09, IVS-08

3.10.2 Potential Security Impact

Enterprises can attempt to segregate VMs of different trust levels on separate host machines. However, that effort may not be effective unless there is effective implementation of systems and data categorization, as well as implementation of adequate network, security, and management controls. VMs of lower trust levels will typically have weaker security controls than VMs of higher trust levels. Those VMs can therefore be easier to compromise, potentially providing a stepping stone to higher-risk, more sensitive VMs on the same host. It is important to have consistency in the levels of protection for VMs of different trust levels across physical and virtual environments. In short, hosting VMs of different trust levels on the same host tends to reduce overall security for all components to that of the least-protected component.

3.10.3 Security Controls to Mitigate Risks

To mitigate risk, consider implementing the following security controls:

- Implement policies and processes to categorize systems and data according to different security classifications.
- Assign users of workloads of different trust levels to different VLAN networks and, if possible, to physically or logically separated servers where different security policies may be applied. That is, virtual desktop workloads should be isolated from the rest of physical data center.
- Run workloads of different trust levels on different physical and/or logical networks. Consider the feasibility of segregating VMs by creating security zones based on type of use (e.g., desktop vs. server), production stage (e.g., development, production, and testing), and sensitivity of data on separate physical clusters of hardware components such as server, storage and network.
- Use firewalls, whether physical or virtual, to isolate groups of VMs from other hosted groups. For example, separate production systems from development systems or development systems from other cloud-resident systems
- Carefully design and implement access from each trust level to physical and virtual management and security systems.

3.11 Risk #11 – Risk Due to Cloud Service Provider API

3.11.1 Risk Table

Risk Name	**Risk due to Cloud Service Provider API**
Risk Description	Enterprises may embark on a hybrid cloud services approach. This integration of private and public cloud infrastructure services poses a challenge, because enterprise identification, authentication, policy management, and governance framework(s) may not naturally extend into the public cloud.
Relevant Security Aspect	Risk to confidentiality, integrity, and availability
Relevant Governance Risk Area	Architectural and configuration risk
Vulnerabilities	• The cloud service provider's API set is not secured. • Data transmitted or stored in the cloud is not protected by encryption. • Strong authentication / access control is not implemented for external systems. • Identity and credential federation, such as Active Directory services or another LDAPv3 directory, is not used. Traffic is not transmitted via a private / out-of-band encrypted channel that is separate from normal internal traffic. • Security, compliance, and governance controls and monitoring are not consistently enabled.
Affected Assets	Security of the hybrid environment
CCM v3.0.1	IAM-12

3.11.2 Potential Security Impact

Cloud service providers expose a set of software interfaces or APIs that an enterprise can use to manage and interact with cloud services. Such interfaces must be designed to protect against accidental and malicious attempts to circumvent enterprise policies.

3.11.3 Security Controls for Mitigating Risks

To mitigate risk, consider implementing the following security controls:

- Implement strong authentication and granular access control with encrypted transmission.
- Use two different authentication zones—one for internal organizational systems and another for external systems.
- Transmit Active Directory traffic via a private / out-of-band encrypted channel that is separate from normal Internet traffic if it is used across the Internet.
- Explore using identity federation, which may involve the use of:
  - Formal Internet standards, such as the OASIS Security Assertion Mark-up Language specification
  - Open source technologies and/or other openly published specifications, such as Information Cards, OpenID, the Higgins trust framework, or the Novell Bandit project
- Apply enterprise security, compliance, and governance policies to assets managed in hybrid clouds and implement comprehensive monitoring and reporting.

4. Conclusion

The massive sharing of infrastructure resources—including compute, network, storage, management, and security, in a multi-tenanted environment enabled by virtualization technologies, especially with users who span different organizations and security needs—creates a "shared virtual computing environment" where users / organizations are no longer clearly separated by physical server racks and networks. Inside a cloud, it is difficult to identify where data is stored and how it is segregated. This lack of visibility and the ability to control, audit, and verify poses a number of security and compliance concerns for IT personnel, end-users, and regulators.

While the cloud community is still grappling with these emerging risks, virtualization technologies are continuing to be rapidly innovated. An example is the emergence of Linux Containers and Dockers, software-defined networking that enables even more fine-grained controls. In addition, new uses of current virtualization technologies continue to be discovered. To manage such a dynamic risk environment, organizations should put effective governance and risk management processes and controls in place to continually monitor and proactively mitigate the evolving risks.

Appendix I – Risk Assessment Matrix

Evaluation of Risk

Vulnerability	Likelihood (See Table 1)	Impact Due to Confidentiality Compromise (See Table 2)	Impact Due to Integrity Compromise (See Table 2)	Impact Due to Availability Compromise (See Table 2)	Evaluate Risk Level (See Table 3)	Risk Treatment Control to be implemented	Evaluate Residual Risk Level (See Table 3)
Type of Risk: 1 – VM Sprawl							
Asset exposed to risk: VM							
Lack of effective control process to manage VM lifecycle	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Lack of placement / zoning policies or enforcement of where a dormant VM can instantiate or reside	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Lack of discovery tool to identify unauthorized VMs	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 2 – Sensitive Data in VM							
Asset exposed to risk: VM and Storage							
VM images and snapshots are not treated in the same way as the sensitive data.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Policies and processes are not in place to control storage of VM images and snapshots.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 3 – Security of offline / dormant and pre-configured VMs							
Asset exposed to risk: VM							
Security patches on the offline/dormant VM are out of date.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Guidelines on the activation of offline/dormant VMs are not in place.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 4 – Security of Pre-Configured (Golden Image) VM / Active (Running) VMs							
Asset exposed to risk: VM							
Deployment of compromised VMs may lead to loss of integrity of the virtualization platform.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
VM with unauthorized changes to hardware, network, and storage may cause disruption in VM availability.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			

Vulnerability	Likelihood (See Table 1)	Impact Due to Confidentiality Compromise (See Table 2)	Impact Due to Integrity Compromise (See Table 2)	Impact Due to Availability Compromise (See Table 2)	Evaluate Risk Level (See Table 3)	Risk Treatment Control to be implemented	Evaluate Residual Risk Level (See Table 3)
VMs with viral payload injection may impact the entire virtualized environment.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 5 – Lack of Visibility and Controls on Virtual Networks							
Asset exposed to risk: VM and network							
Virtual networks cannot be monitored using traditional tools.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Hypervisor may not be able to intercept and monitor inter-VM communication.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Consistent security policy enforcement cannot be applied on physical and virtual networks.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Comprehensive monitoring across physical and virtual network cannot be implemented	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Physical and virtual network configuration may not be managed by the same team.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 6 – Resource Exhaustion							
Asset exposed to risk: VM							
Servers are burdened by concurrent execution of resource-intensive software.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Simultaneous OS automated patching on a group of VMs causes enormous access strain on a common storage resource.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 7 – Hypervisor Security							
Asset exposed to risk: Hypervisor							
Configuration of hypervisor may not be hardened to reduce areas of vulnerabilities.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Vendor- recommended best practices are not adopted.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Unused physical hardware devices are connected. Clipboard / file-sharing services are not disabled.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			

Vulnerability	Likelihood (See Table 1)	Impact Due to Confidentiality Compromise (See Table 2)	Impact Due to Integrity Compromise (See Table 2)	Impact Due to Availability Compromise (See Table 2)	Evaluate Risk Level (See Table 3)	Risk Treatment Control to be implemented	Evaluate Residual Risk Level (See Table 3)
Vendor security bulletins /alerts are not subscribed to. Security updates are not implemented promptly	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Self-integrity checks or equivalence are not conducted upon boot-up to confirm whether or not hypervisor has been compromised.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Ongoing monitoring including analysis of hypervisor logs does not occur.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Attack surface is further increased through uncontrolled use of hypervisor management APIs by IT/DevOps tools and scripts and other infrastructure technologies.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 8 — Unauthorized Access to hypervisor							
Asset exposed to risk: Hypervisor (and mgmt. tool)							
Access to virtualization layer is not restricted as with any sensitive OS (i.e., restricting console access via firewalls).	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Hypervisor may not support role-based access control of administrative responsibilities.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Additional third-party tools that provide tight administrative control are not deployed.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
A separate authentication is not used to restrict access.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Hypervisor management APIs/CLIs are not adequately protected	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Separate “management LAN” authentication is not used to restrict access.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Remote hypervisor management is not disabled.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			

Vulnerability	Likelihood (See Table 1)	Impact Due to Confidentiality Compromise (See Table 2)	Impact Due to Integrity Compromise (See Table 2)	Impact Due to Availability Compromise (See Table 2)	Evaluate Risk Level (See Table 3)	Risk Treatment Control to be implemented	Evaluate Residual Risk Level (See Table 3)
Administrative interfaces are accidentally exposed through network configuration errors and lack of change of management procedures	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 9 — Account or Service Hijacking through Self- Service Portal							
Asset exposed to risk: Privileged access to applications, VM, and Virtualization Platform							
Strong authentication control is lacking.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Policy governing creation and use of self-service portals is lacking.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Policy-based management of self-service portal is not used.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Proactive monitoring of unauthorized activity does not occur.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Account management is “relaxed” (e.g., password reset sent in clear text)	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Type of Risk: 10 — Workload of Different Trust Levels Located on the Same Server (Commingling of Data)							
Asset exposed to risk: VMs in the same physical server							
VMs of different trust levels are hosted on or migrated to the same physical server.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Physical or logical software defined-networks for VMs of different trust levels are not separated.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Physical and virtual firewalls are not deployed to isolate groups of VMs from other hosted groups, such as production from development systems or development rom other cloud-resident systems.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Virtual desktop workloads are not isolated from the rest of the physical data center.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Administrative separation of duties may not be implemented, allowing unauthorized changes or accidental misconfiguration that violates logical zoning.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			

Vulnerability	Likelihood (See Table 1)	Impact Due to Confidentiality Compromise (See Table 2)	Impact Due to Integrity Compromise (See Table 2)	Impact Due to Availability Compromise (See Table 2)	Evaluate Risk Level (See Table 3)	Risk Treatment Control to be implemented	Evaluate Residual Risk Level (See Table 3)
Type of Risk: 11 – Risk Due to CSP API)							
Asset exposed to risk: Security of the hybrid environment							
Cloud service provider API set is not secured.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Data transmission is not protected by encryption.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Strong authentication/ access control is not implemented for external systems.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Active Directory traffic is not transmitted via a private/out-of- band encrypted channel (separated from normal internal traffic)	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Identity federation is not used.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			
Security, compliance, and governance controls and monitoring are not consistently enabled.	Low Medium High	Low Medium High	Low Medium High	Low Medium High			

Table 1 – Likelihood Rating for Related Vulnerability

Likelihood Rating	Evaluation Criteria
High	Relevant security control(s) is not in place.
Medium	Relevant security control(s) is in place but not consistent or effective.
Low	Relevant security control(s) is in place and effective.

Table 2 – Impact Rating for Related CIA Compromise

Impact Rating	Evaluation Criteria
High	There is significant business impact to the enterprise.
Medium	There is tangible or intangible loss to the enterprise.
Low	There is insignificant business loss due to minor inconvenience / inefficiency in business operations.

Table 3 – Risk Matrix showing the Defined Risk levels

	Impact		
Likelihood	Low	Medium	High
Low	1 (Insignificant)	2 (Minor)	3 (Medium)
Medium	2 (Minor)	3 (Medium)	4 (High)
High	3 (Medium)	4 (High)	5 (Very High)

Appendix II – Types of Virtualization

Virtualization has developed rapidly. In general, virtualization can refer to a wide variety of technologies, which can be grouped into the following categories:

1. Full virtualization
2. Para-virtualization
3. Operating system virtualization
4. Desktop virtualization
5. Storage virtualization
6. Network virtualization

Full Virtualization

In general, there are two types of virtualization hypervisors. Type 1—bare metal—hypervisors execute VMs directly over computer hardware, with no need for an underlying operating system. Type 2—hosted—hypervisors must be hosted on top of an operating system. Type 2 hypervisors must be started like a regular software application before any VMs can be controlled.

Para-Virtualization

In this implementation, the underlying operating system kernel presents a set of software interfaces to VMs in order to access underlying hardware. In theory, hardware access speeds are increased for these VMs, as compared to Type 2 hypervisors. In practice, the operating systems of these VMs must be para-virtualized-aware for the speed impact to be realized.

Operating System Virtualization

The latest virtualization technology involves the development of Linux Containers and Dockers. These containers support software applications that can execute with virtual resources and do not require the creation of a VM. In other words, a hypervisor in the traditional sense of the word does not exist. Management of virtual resources is implemented by virtualizing the operating system. Docker technology is currently used by companies such as Google, Amazon, and Microsoft. Docker isolation appears to be an issue at this writing[3]. Hence, adoption of Docker technology from a security perspective must be carefully considered.

Desktop Virtualization

Here, the PC desktop environment is rendered remotely to a special-access client using low bandwidth. Desktop virtualization is much like a remote desktop session, except that these machines are virtual and centrally managed.

[3] https://blog.xenproject.org/2014/06/23/the-docker-exploit-and-the-security-of-containers/

Storage Virtualization

This technology uses a logical raw disk made from physical disk storage and distributed to server hardware using a network connection. This is a popular technique for sharing and managing disk storage from a centralized appliance on a server farm.

Network Virtualization

Traditional network infrastructures supporting enterprise virtualization environments require careful planning and implementation, especially when any of the VMs interface with the Internet. With ease of VM creation, a traditional approach to data separation using VLANs may not be feasible, as in the case of the 4000 VLAN limit of an enterprise. A new approach, network virtualization, is being developed to overcome this constraint. Entire network infrastructures, consisting of routers and switches are virtualized to support VM agility and flexibility. This approach may pose a security problem, because monitoring tools have yet to evolve with the pace of change.