Description of document:	Three (3) reports on the 2015 electronic computer system outage at the Merit Systems Protection Board (MSPB), 2015-2016
Appeal date:	09-March-2016
Released date:	21-November-2016
Posted date:	28-November-2016
Source of document:	FOIA Request Merit Systems Protection Board 1615 M Street, NW Washington, DC 20419 FOIA Web Portal

U.S. MERIT SYSTEMS PROTECTION BOARD

Office of the Chairman
1615 M Street, NW
Washington, DC 20419-0002

Phone: (202) 653-7101; Fax: (202) 653-7208; E-Mail: chairman@mspb.gov

Chairman

NOV 21 2016

Tracking No. FOIA-OCB-2016-000098

This letter responds to your appeal of the MSPB Clerk's Office's February 25, 2016 disposition of your Freedom of Information Act (FOIA) request. I previously notified you that the MSPB would require multiple extensions in considering your appeal; I appreciate your patience as we reviewed the records you requested. For the reasons discussed below, I am granting your appeal in part and denying it in part.

On February 17, 2016, you requested "a copy of the report concerning the July 2015 electronic computer system outage at MSPB." Three such reports exist. On February 25, 2016, the Clerk's Office denied your request on the basis that the reports were protected by the deliberative process privilege, FOIA Exemption 5. 5 U.S.C. § 552(b)(5). You appealed this determination on March 9, 2016.

I find that the Clerk's Office correctly determined that the reports are protected by Exemption 5 because they render conclusions and make recommendations that the Board may use in determining how to respond to the computer system outage. The reports therefore are part of the deliberative process and are privileged. However, portions of the reports address purely factual issues or make observations and these portions are reasonably segregable from the recommendations. I am therefore providing these sections of the reports. In addition, I am releasing certain recommendations made in the reports which the agency has decided to implement or not implement.

Portions of the reports also are redacted pursuant to FOIA Exemption 6, which protects information in personnel and similar files the disclosure of which could constitute a "clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). With respect to the reports, this information consists of names, positions, and contact information for agency employees or employees of the companies contracted to produce the reports.

Finally, certain sensitive technological information is redacted pursuant to FOIA Exemption 7(E), which protects certain law enforcement information. 5 U.S.C. § 552(b)(7)(E).

This is the Board's final decision in your appeal. Pursuant to 5 U.S.C. § 552(a)(4)(B), you have the right to seek judicial review of this decision in an appropriate United States District Court.[1]

Sincerely,

Susan Tsui Grundmann

Attachments:

Kelyn Professional Services report (partially redacted)
VMware Professional Services report (partially redacted)
Cask LLC report (partially redacted)

[1] The 2007 FOIA amendments created the Office of Government Information Services (OGIS) to offer mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your right to pursue litigation. Nor does using OGIS services or contacting OGIS toll or extend the statute of limitations or any other deadline. If you are requesting access to your own records, which is most often, but not always, considered a Privacy Act, or first-party request, you should know that Privacy Act matters fall outside the scope of OGIS's mission. You may contact OGIS in any of the following ways:

Mail: Office of Government Information Services (OGIS), National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740-6001
E-mail: ogis@nara.gov; Telephone: 202-741-5770; Fax: 202-741-5769; Toll-free: 1-877-684-6448

Assessment and Recommendations

Prepared for:

Merit Systems Protection Board

Prepared by
Kelyn Professional Services
May 17, 2016

Version History

Version Number	Revision Date	Contributor's Name	Revision Description
1.0	8/3/2015	(b) (6)	First Draft
1.1	8/12/2015	(b) (6)	Minor revision

Prepared by Kelyn Professional Services

Table of Contents

Introduction

In June 2015, MSPB experienced a catastrophic failure of its VMWare virtual environment. Most of the virtual servers were successfully rebuilt, but one particularly critical virtual server had not had a successful backup, and critical data was lost in this failure. MSPB has requested Kelyn technologies to perform an assessment, assist with configuration and troubleshooting, and recommend changes and improvements to the CommVault environment that will reduce the likelihood of future data loss.

This document records some of the key configuration changes made during the on-site visit. It is also a current state analysis of MSPB's CommVault backup environment, and makes recommendations in accordance with CommVault best practices that will make the backups more robust and increase the likelihood of being able to restore data going forward. This analysis was researched at the MSPB offices Washington DC.

While on site, the Kelyn engineer also assisted the customer in attempting to locate and retrieve lost data that had had expired from backups, but had potentially not been overwritten on tape. Unfortunately, the specific data in question was not in the backup sets that were on tape.

Recommendations and Improvements

Summary of Configuration Changes

While the Kelyn engineer was on-site, certain key configurations were changed. Among them are the following:

Automatic discovery of VMs. The default subclient was configured to automatically discover VMs as they are created and back them up. This will require continual monitoring and removal of VMs where backup is not required.

Modified the schedule for Oracle backups. There was a conflict in the schedule for Oracle backups that was causing a backup job to fail, which in turn was causing data to be retained too long on tapes, so that there were no longer tapes available, and aux copy jobs were not able to run.

According to CommVault best practices, storage policies should be kept to a minimum number, which is determined by retention requirements and location of the libraries. At the start of the engagement, there were seven storage policies. We were able to remove three storage policies that were obsolete, and establish a plan for consolidating the remaining policies into a single policy.

Recommendations for Architectural Improvements

Define requirements for frequency of backups and retention. A business impact analysis (BIA) that includes definition of Recovery Point Objective (RPO) and Recovery Time Objectives (RTO) should be performed to assess the relative importance of data and determine schedule and retention requirements based on RPO and RTO.

Definitions:
RPO - the maximum targeted period in which data might be lost from an IT service due to an incident

RTO - the targeted duration of time within which a business process must be restored after a disruption of service

Based on the RPO and RTO that is established by management retention policy and schedule may need to be adjusted

> Retention policy: While the Kelyn engineer was on site, management instructed the backup administrator to change the primary and secondary copies from 4 days 2 cycles to a 14 day and 1 cycle retention. A monthly full backup is retained on tape for 6 months. The primary retention is a much shorter than what is typically seen in backup environments, and restores from more than 14 days may require tapes to be retrieved from offsite. Kelyn recommends that the backup environment be designed so that it most cases short of a disaster, recoveries can be performed from the primary (onsite) copy.
>
> Based on the RPO established by management, the backup schedule could be adjusted from one backup per day for all data, to schedules where backups can be performed multiple times per day for critical servers.
>
> In order to enable quick recovery of data, it is advisable that retention on local disk be adequate in duration that nearly all restore operations can be performed from local disk. Offsite backups should generally be considered an option of last resort in case of a major disaster. Additional data retention will require significant increases in the amount of disk space needed in the disk library unless deduplication is implemented.

Use disks at an offsite data center or a cloud provider for secondary copy instead of using tapes. Tape management and handling is a very time consuming task for backup administrators and adds additional risks to the backup process than can be avoided by performing data replication electronically to an offsite center or a cloud provider. Tapes are notoriously unreliable and fail at a much higher rate than disks. This, coupled with the handling of tapes, moving them in and out of the tape library, moving them to the offsite location, exposes the data to significant risks including loss of data, interception of data, and human error.

Implement CommVault deduplication: Deduplication will drastically decrease the amount of time that it takes to perform backups, reduce the amount of data transferred over and allow storage of multiple backups of a single host while using a significantly reduced of disk space over non-deduplicated backups. It is a foundation technology that serves as the base for other recommendations: Increase retention on local media agent, and transfer offsite backups to offsite disks or a cloud provider.

The primary backup copy is being written to the same Nutanix hardware as the primary storage for the virtual servers. There is redundancy and replication built into the storage, but in general, separate hardware for the CommVault backup libraries is recommended. This architecture should be reviewed to determine if this single point of failure is putting data at risk.

CommCell Environment Evaluation

Product Release Level

CommCell Service Level: Simpana® V10R2SP11
CommServe: (b) (7)(E) [redacted]
CommCell: (b) (7)(E) [redacted]
Observations:
All CommVault components are up-to-date, or at the latest release supported for the operating system.
Remediation:

- **None**

Product Updates

Installed Updates: Service Pack 11
Additional Updates: none
Needed Updates: none
Observations:

- **Up to date**

Remediation:

- **None**

Disaster Recovery Backup Configuration

The Disaster Recovery backup is the crucial element of restoring the CommVault backup environment in case of a failure of CommVault. It backs up the CommVault SQL database that resides on the Commserve server.

Observations:

- **DR backups are written on the commserve server,** (b) (7)(E)**. Configured to retain the last seven backups**
- **Two additional copies are written to tape using the CommServeDR storage policy**
- **DR backup copies on tape have an infinite retention**

Remediation:

- **DR backups have a short useful life, making the infinite retention unnecessary. The tape copy retention can be reduced and free up most of the tapes that contain DR backups**
- **Confirm that the most recent DR backup tapes are being removed from the tape library and taken offsite weekly.**

Index Cache

Observations:

- Each media agent has an index cache that is located at the following locations:
  (b) (7)(E) (b) (7)(E)
  (b) (7)(E) (b) (7)(E)

Remediation:

- None

Storage Policy

Observations:

- According to best practices, storage policies should be kept to the minimum number to meet retention requirements. At the beginning of the engagement, there were seven storage policies, we were able to remove three, and advised the backup administrator to consolidate the four remaining storage policy into a single storage policy.

Remediation:

- Reduce storage policies to the minimum to meet retention requirements. Since all backups require the same number of days of retention, all of the hosts that are backing up should be configured to use the same storage policy. Two of the storage policies, one for full backups, and one for incrementals were recently created using new disk, while two of the storage policies are using the older disk. All subclients should be changed so that they are associated (both full and incremental backups) with one of the new storage policies. The storage policy can then be renamed to accurately describe its purpose.

Virtual Sever Backup

Observations:

- **Subclients are set up to contain servers according to their business function.**
- **Automatic discovery of new virtual servers was enabled during the course of this assessment.**

Remediation:

- Continue to monitor automatic discovery of VMs

CommVault Customer Support Hotline

For a list of all Global Technical Support Hotline numbers please click on the following link:

CommVault Support	Telephone Support – phone 1-877-780-3077 In order to open a case with support, you will need to provide your commcell ID: (b) (7)(E)

CommVault Web Support

Access the Maintenance Advantage Customer Support Portal at the following link:

Maintenance Advantage	http://ma.commvault.com
Documentation	http://documentation.commvault.com

Please be aware that critical calls cannot be opened on the Web and will need to be called in to the Support Hotline. To increase the severity of an incident contact the Customer Support Hotline.

VMware IMPLEMENTATION METHODOLOGY

VMware Desktop Virtualization Health Check Services

Health Check Report

for

MSPB

Prepared by

(b) (6)

VMware Professional Services

(b) (6)

Version History

Date	Ver.	Author	Description	Reviewers
9/1/2015	.1	(b) (6)	Draft	
9/3/2015	.5	(b) (6)	Add Content	
9/4/2015	1.0	(b) (6)	Organize Findings	
9/6/2015	1.5	(b) (6)	Added Recommendations	
9/8/2015	2.0	(b) (6)	Organized Recommendations	
9/9/2015	2.5	(b) (6)	Checked Formatting sent to (b) (6) for review	(b) (6)

VMware, Inc
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

1. Executive Summary

MSPB engaged VMware Professional Services to conduct a health check of their VMware View™ environment. This engagement included a health check of MSPB's current VMware vSphere® configuration, operations, and usage. If there are issues with the underlying vSphere implementation, the impact on the View environment could be severe.

2. Health Check Background

2.1 Scope

This document applies to the vSphere and Horizon View environments in the Washington DC office. All of the server systems are hosted in house and managed by internal personnel. This engagement is limited to the documentation and data gathered within the VMware Health Analyzer and the logs collected from each VMware component. The vSphere environment exists on Nutanix Hardware.

Infrastructure and VDI – Nutanix 3450

ComVault environment – Nutanix 6250

2.2 Health Check Participants

The following personnel were active participants during the course of the health check.

- (b) (6) - VMware
- (b) (6) – VMware
- (b) (6)
- (b) (6)
- (b) (6)
- (b) (6)

2.3 Summary of Activities

The following activities were conducted during the course of this project.

- Assessed and summarized the MSPB VMware vSphere environment health and architecture, focusing on technical and organizational aspects.
- Interviewed participants to determine priority issues and concerns.
- Collected View component information.
- Inventoried all hosted virtual desktops.
- Inventoried all linked clone pools, individually assigned virtual machines, and corresponding user entitlements.
- Researched MSPB's issues and concerns with View performance.
- Conducted basic knowledge transfer on following topics:
    - View operations best practices
    - Pool management best practices
    - View storage best practices

- Hosted desktop image build process
- PCOIP sizing considerations
- PCOIP protocol tuning

2.4 Next Steps

Review this report and consider the recommended action items. Consider follow-up consulting engagement and/or health check. If required, the VMware Professional Services Organization or one of the VMware partner organizations can help MSPB implement the recommended actions.

3. Findings and Recommendations

The assessment results are presented in a prioritized format. Table 1 summarizes the priority categories of the assessment.

Table 1. Priority Categories

Priority	Definition
P1	Items that require immediate attention and the corresponding actions to address each item.
P2	Items of potential concern. The items are either non-critical, or require further investigation.
P3	Deviation from best practices, but addressing these might not be an immediate priority.

3.1 Summary of vSphere Findings

The following table contains a summary of the results of the vSphere Health Check that was performed during this project.

3.1.1 Compute

Item	Comments
Observation 1	Remote syslog logging is configured but not enabled for 10 host(s).
Priority	P1
Recommendation	Use persistent and remote syslog logging to improve manageability.
Justification	Remote logging both persistently on each host and to a central host (syslog server) can greatly improve administration and management. By making files available when needed and gathering files on a central server, you can easily monitor all hosts and perform event correlation, aggregate analysis, and make root cause analysis easier for troubleshooting. Also, gathering the log files on a remote system allows you to retain more historical information for postmortem analysis of compromised systems. To collect syslog information, all the systems must have synchronized time and the correct firewall ports open between hosts so that events can be correlated. Also, log messages are not encrypted when sent to the remote host, so the network for the service console should be isolated from other networks. With vSphere 6.0, the vSphere Syslog Collector (Windows) or the VMware Syslog Service (Appliance) are installed by default and thus can be used to provide this function once configured. **References:** *Configure Syslog on ESXi Hosts* section of the *vSphere Installation and Setup* Guide http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-installation-setup-guide.pdf *ESXi tab in the VMware Security Hardening Guides* *http://www.vmware.com/security/hardening-guides.html*

Item	Comments
Observation 2	ESXi shell has been enabled or configured to start automatically on 7 host(s). SSH access has been enabled or configured to start automatically on 10 host(s).

Priority	P1
Recommendation	Configure VMware vSphere ESXi Shell and SSH access per manageability requirements.
Justification	The vSphere ESXi Shell and ESXi host SSH access can provide essential host access that can be used when standard remote management or CLI tools do not function. Access to the vSphere ESXi Shell and SSH is primarily intended for use in break-fix scenarios and can be enabled from either the graphical user interface, or from the Direct Console User Interface (DCUI). When enabled, a warning is shown on the host, so that you are aware when vSphere ESXi Shell or SSH access to a host has been enabled. For security reasons, VMware recommends disabling these options until required by an administrator to decrease the attack surface of the ESXi host. **References:** *Using ESXi Shell in ESXi 5.x* and 6.0 (2004746) http://kb.vmware.com/kb/2004746 *ESXi tab in the VMware Security Hardening Guides* *http://www.vmware.com/security/hardening-guides.html*

Item	**Comments**
Observation 3	2 cluster(s) have host HBA(s) configured inconsistently across ESX hosts. 1 cluster(s) have host NIC(s) configured inconsistently across ESX hosts.
Priority	P1
Recommendation	Place host devices in a consistent order and location.
Justification	Putting host devices in a consistent bus or slot for a particular type (vendor/model) facilitates automated installation and configuration, and makes administration and troubleshooting easier. Place storage adapters and network adapters on separate buses to reduce bus contention and improve performance. This does not apply for converged network adapters (CNA) with network and storage traffic. **References:** vSphere Installation and Setup Guide: http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-installation-setup-guide.pdf

Item	**Comments**
Observation 4	2 cluster(s) have host advanced parameter settings configured

	inconsistently across ESX hosts.
Priority	P2
Recommendation	Avoid unnecessary changes to advanced parameter settings.
Justification	Advanced parameters can cause unexpected behavior on ESXi hosts, if not configured correctly. It is best to avoid using them unless absolutely necessary. If they are used, it is best to perform a check to determine whether advanced parameters are consistently configured across ESXi hosts in a cluster. **References:** *Configuring Advanced options for ESXi (1038578)* http://kb.vmware.com/kb/1038578 *vSphere Availability* guide http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-availability-guide.pdf

3.1.1 Datacenter

Item	Comments
Observation 1	Strict Admission Control for 2 VMware HA enabled cluster(s) is not enabled.
Priority	P1
Recommendation	Size with HA host failure considerations.
Justification	VMware vCenter Server uses admission control to verify that sufficient resources are available in a cluster to provide failover protection and to protect virtual machine resource reservations. There are three different admission control policies: • The number of host failures that the cluster tolerates policy - In this case, HA calculates the slot size for the cluster. The slot size is generally based on the worst case CPU and memory reservation of any given virtual machine in the cluster but it can be configured differently as specified in the cluster configuration. This calculation can result in a conservative admission control policy, but is fully automated and allows virtual machines to be restarted in the event of a host failure. • The percentage of reserved cluster resources reserved policy - In this case, HA does not use the slot size calculation and uses a percentage of CPU and Memory resources for recovery from host failure. If the percentage reserved is low, virtual machines might not being protected due to insufficient resources. • Use Failover hosts - In this case, a host(s) are reserved as

	failover hosts. Sufficient capacity must be available on these stand-by hosts to ensure that recovery is possible in the event that a failure occurs. Selecting the number-of-host failures for HA admission control policy is recommended unless there are virtual machines with large reservations that result in a very conservative HA admission control policy. VMware recommends that all hosts in a cluster have similar CPU and memory configurations to have a balanced cluster and optimal HA resource calculations. **References:** VMware HA Admission Control section in *vSphere Availability* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-availability-guide.pdf

Item	**Comments**
Observation 2	2 cluster(s) contain VM(s) and/or template(s) with mixed hardware versions.
Priority	P2
Recommendation	Maintain compatible virtual hardware versions for virtual machines.
Justification	Although not a recommended practice, clusters can have compatible but different versions of ESXi. This is known as Mixed Mode. Although this configuration allows you to create virtual machines with different virtual hardware, it also has these disadvantages: • New hardware virtual machines cannot be powered-on on older version hosts. • vSphere vMotion migrations are not possible between new and older hosts if the hardware level of the VM is not supported. • Limitations on deployment and creation of virtual machines per host. **References:** Virtual Machine Compatibility section of the *vSphere Virtual Machine Administration* Guide http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-virtual-machine-admin-guide.pdf

Item	**Comments**
Observation 3	10 virtual object(s) do not appear to follow a standard naming convention.

Priority	P2
Recommendation	Use a consistent naming convention for all virtual data center objects.
Justification	Using defined, documented, and consistent naming conventions provides order to the VMware virtual infrastructure and helps administrators readily and correctly identify its objects such as virtual machines, datacenters, clusters, resource pools, ESX hosts, vCenter folders, virtual switch port groups/dvport groups, uplink groups, datastores, templates, snapshots, and vApps. Define and use a consistent naming convention for datastores used in the VMware virtual infrastructure. Some attributes to incorporate in the naming convention are: • Type of storage (FC, NFS, and iSCSI) • Array vendor or type • Location • Business unit or function • Performance characteristics (RAID level) • Availability characteristics (replicated and non-replicated) • Hostname tag for local datastores Naming standards also help to streamline the troubleshooting and support process.

Item	**Comments**
Observation 4	5 user session(s) have been idle for at least 1 hour.
Priority	P2
Recommendation	Disconnect vSphere Clients from the vCenter Server when they are no longer needed.
Justification	vCenter Server must keep all client sessions current with inventory changes. When this process is used for connected but unused sessions attached to the vCenter Server, the vCenter Server system’s CPU usage and user interface speed can be affected. To improve the performance of vCenter Server, disconnect vSphere Client sessions from the vCenter Server when they are no longer needed. This issue is true only for the vSphere Client. This behavior does not occur with the VMware vSphere Web Client. **References:** *Performance Best Practices for VMware vSphere 6.0* http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

3.1.2 Network

Item	Comments
Observation 1	3 cluster(s) have inconsistently configured standard switches across ESX hosts. 1 cluster(s) have inconsistently configured distributed switches across ESX hosts.
Priority	P1
Recommendation	Configure networking consistently across all hosts in a cluster.
Justification	Minimize differences in the network configuration across all hosts in a cluster. Consistent networking configuration across all hosts in a cluster eases administration and troubleshooting. Also, because services such as vMotion require port groups to be consistently named, it is important to have a consistent configuration so that DRS and vSphere vMotion capabilities are not disrupted. A consistent naming convention for virtual switches, port groups, and uplink groups should also be used in the environment to prevent confusion when configuring virtual machines. VMware vSphere Distributed Switch™ can be used here to reduce administration time and promote consistency across the virtual data center. This is because changes to the distributed virtual port group are consistently and automatically applied to all hosts that are connected to the distributed switch. **References:** *vSphere Networking Guide* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-networking-guide.pdf* *Security Hardening Guide* (vNetwork tab) http://www.vmware.com/security/hardening-guides.html

Item	Comments
Observation 2	1 host(s) has VMKernel port groups with no NIC redundancy.
Priority	P1
Recommendation	Verify that there is redundancy in networking paths and components to avoid single points of failure.
Justification	To avoid service disruption, make sure that the networking configuration is fault resilient to accommodate networking path and component failures. For example, provide at least two paths to each network. To do this configure all port groups and distributed virtual port

	groups with at least two uplink paths using different vmnics. NIC teaming can be used with at least two active NICs, to provide redundancy along with an increase in the available bandwidth for the network. Standby NICs can also be used, but are often seen as wasted resources, because they do not pass traffic unless a failure occurs. Set failover policy with the appropriate active and standby NICs for failover. Connect each physical adapter to different physical switches for an additional level of redundancy. In addition, upstream physical network components should also have the necessary redundancy to accommodate physical component failures. **References:** *vSphere Networking Guide* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-networking-guide.pdf

Item	**Comments**
Observation 3	2 cluster(s) have portgroups configured inconsistently (either name or active NIC total speeds) across ESX hosts. 1 cluster(s) have distributed portgroups configured inconsistently (either name or active NIC total speeds) across ESX hosts.
Priority	P1
Recommendation	Minimize differences in the number of active NICs across hosts within a cluster.
Justification	Variance in the number of active NICs across hosts within a cluster can lead to inconsistent network performance when virtual machines are migrated to other hosts within a cluster. Hosts that have fewer NIC ports than others might experience network bottlenecks, but this might not be obvious if you assume that all hosts have the same number of active NIC ports available.

Item	**Comments**
Observation 4	18 standard portgroup(s) have NICs with mixed speed settings.
Priority	P1
Recommendation	Avoid mixing NICs with different speeds and duplex settings on the same uplink for a port group/dvport group.
Justification	Having a port group/dvportgroup mapped to multiple vmnics at different speeds is not recommended because, depending on the traffic load balancing algorithm, the network speed of the traffic can be arbitrarily and randomly determined and the result can be undesirable.

	For example, suppose there are several virtual machines all connected to a single vSwitch with two outbound adapters, one at 100-Mbps and one at 1-Gbps. Some virtual machines would have better performance than others depending on how their traffic is routed. A best practice is to verify that the speed is predictable and deliberately chosen.

Item	Comments
Observation 5	Network I/O Control is not enabled for 1 distributed virtual switch(es) that use 10 Gbps uplinks.
Priority	P1
Recommendation	Use Network I/O Control (NetIOC) to prioritize traffic.
Justification	All network traffic can benefit from NetIOC traffic prioritization during contention scenarios. 10-Gb Ethernet particularly can benefit from it as it provides high bandwidth for ESXi systems. If this bandwidth is not managed properly, an individual host can quickly saturate upstream network systems. VMware recommends enabling NetIOC to prioritize the correct network traffic across your data center. **References:** *Performance Evaluation of Network I/O Control in vSphere 6.0* *https://www.vmware.com/resources/techresources/10454*

Item	Comments
Observation 6	1 host(s) has VMKernel port groups with no NIC redundancy.
Priority	P1
Recommendation	Set up network redundancy for VMKernel network ports.
Justification	VMKernel network ports are the basis for many of the tasks that are performed on an ESXi host. Redundancy should be configured for each of the vmkernel ports, including: • Management Networks • iSCSI/NFS Storage networks • vMotion Networks • Fault Tolerance Logging Networks • Virtual SAN Networks Redundancy can most easily be accomplished by having multiple vmnics attached to the vSwitch. **References:** *vSphere Networking Guide*

	http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-networking-guide.pdf

Item	Comments
Observation 7	4 DV Port Groups for Distributed Virtual Switches do not use Load-Based Teaming.
Priority	P1
Recommendation	Use Load-Based Teaming to balance virtual machine network traffic across multiple uplinks.
Justification	If link aggregation is not employed, Load-Based Teaming is the best option for spreading virtual machine traffic across multiple links. No additional physical network configuration is required when compared to the default, "Route based on originating virtual port ID." **References:** *Performance Evaluation of Network I/O Control in VMware vSphere 6* *https://www.vmware.com/resources/techresources/10454*

Item	Comments
Observation 8	10 host(s) have standard port groups which use a network that is not dedicated to a single type of traffic.
Priority	P1
Recommendation	Configure networks so that there is separation of traffic (physical or logical using VLANs).
Justification	Separate the following traffic where appropriate: • Management • IP storage • vMotion • Fault Tolerance Logging • Virtual machine • Virtual SAN • Provisioning • vSphere Replication Traffic separation improves performance, prevents bottlenecks, and increases security. Use physical separation or logical separation using VLANs as appropriate. Configure the physical switch ports as trunk ports for VLANs. **References:**

	Performance Best Practices for VMware vSphere 6.0 http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

Item	Comments
Observation 9	Outgoing traffic shaping is not enabled on 1 distributed virtual switches. Incoming traffic shaping is not enabled on 1 distributed virtual switches.
Priority	P1
Recommendation	Use DV Port Groups to apply policies to traffic flow types and to provide Rx bandwidth controls through the use of Traffic Shaping.
Justification	Configure each of the traffic flow types with a dedicated DV Port Group. For example, you might want to enable Traffic Shaping for the egress traffic on the DV Port Group used for vSphere vMotion. This can help in situations where multiple vMotion operation initiated on different vSphere hosts converge to the same destination vSphere server. **References:** *Performance Evaluation of Network I/O Control in VMware vSphere 6* *https://www.vmware.com/resources/techresources/10454*

Item	Comments
Observation 10	9 ESX host(s) have one or more port groups with physical NICs that share the same PCI bus.
Priority	P2
Recommendation	Distribute vmnics for a port group across different PCI buses for greater redundancy.
Justification	Distributing vmnics for a port group across different PCI buses provides protection from failures related to a particular PCI bus. Team vmnics from different PCI buses to improve fault resiliency from component failures.

Item	Comments
Observation 11	1 host(s) have physical NICs with misconfigured link speeds.
Priority	P3
Recommendation	Configure NICs, physical switch speed, and duplex settings consistently. Set to autonegotiation for 1-Gb NICs.
Justification	Incorrect network speed and duplex settings can impact performance. The network adapter (vmnic) and physical switch settings must be checked and set correctly. If your physical switch is configured for a specific speed and duplex setting, you must force the network driver to

	use the same speed and duplex setting. For Gigabit links, network settings should be set to auto-negotiate and not forced. You can set network adapter speed and duplex settings from the vSphere Client, but a reboot is required for changes to take effect. **References:** Solutions for Poor Network Performance section of *vSphere Monitoring and Performance vSphere 6.0* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-monitoring-performance-guide.pdf

3.1.3 Security

Item	Comments
Observation 1	3 default users/group(s) are being used for vCenter user roles/permissions.
Priority	P1
Recommendation	Use vCenter Server roles, groups, and permissions to provide appropriate access and authorization to the virtual infrastructure. Avoid using Windows built-in groups such as the Administrators group.
Justification	By default, the administrator access is defined as a part of the Platform Services Controller installation. The configured user or group who has full administrative control of vCenter Server (and the virtual infrastructure). This can allow other system administrators who are not virtual infrastructure administrators access the infrastructure, if a dedicated group or user is not created. **References:** vSphere Users and Permissions section of the *vSphere Security Guide for vSphere 6.0* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf

Item	Comments
Observation 2	Tech Support Mode (TSM) timeout is not enabled for 10 host(s).
Priority	P1
Recommendation	Enable the ESXi Shell timeout feature and configure it per customer security requirements.
Justification	In ESXi, the ESXi Shell timeout feature automatically logs out unused ESXi Shell sessions to prevent unauthorized access.

	Set a timeout that does not disrupt the standard VMware administrator workflow. Setting appropriate timeout also avoids indefinite idle connection and unwanted privileged host access. **References:** ESXi tab in the *VMware Security Hardening Guides* http://www.vmware.com/security/hardening-guides.html

Item	Comments
Observation 3	Default firewall settings have been modified from default for 10 ESX host(s).
Priority	P1
Recommendation	Configure firewall rules and ports according to best practices.
Justification	The default firewall rules are configured to provide adequate security while allowing communication with the appropriate VMware virtual infrastructure components. Unless required to enable communication for VMware virtual infrastructure services, avoid changing firewall rules because this can introduce additional security issues. VMware recommends that you leave the default security firewall settings in place. These settings block all incoming and outgoing traffic that is not associated with enabled service. If you enable a service and open ports for it, document the changes, including the purpose for opening each port. Consistently make the changes on all the appropriate ESXi hosts and avoid changing the default ports unless necessary. **References:** VM and ESXi tabs in the *VMware Security Hardening Guides.* *http://www.vmware.com/security/hardening-guides.html* *TCP and UDP Ports required to access vCenter Server, ESX hosts, and other network components (1012382)* http://kb.vmware.com/kb/1012382 TCP and UDP Ports section in the *vSphere Security Guide* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf

Item	Comments
Observation 4	(b) (7)(E) [redacted].
Priority	P2
Recommendation	(b) (7)(E) [redacted]

Justification	(b) (7)(E) [redacted].
	(b) (7)(E) [redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	(b) (7)(E) [redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	References:

	VM Tab of the *VMware Security Hardening Guides* http://www.vmware.com/security/hardening-guides.html

Item	Comments
Observation 5	10 host(s) have one or more port groups that allow forged transmits. 10 host(s) have one or more port groups that allow MAC address changes.
Priority	P2
Recommendation	Change port group security default settings for Forged Transmits, Promiscuous Mode, and MAC Address Changes to Reject unless required.
Justification	VMware recommends that port group security default settings for Forged Transmits, Promiscuous Mode, and MAC Address Changes be set to Reject for improved security. When the MAC address changes option is set to Reject, ESXi does not honor requests to change the effective MAC address to a different address than the initial MAC address. This setting protects the host against MAC impersonation. To protect against MAC impersonation, you can set the **Forged transmits** option to **Reject**. If you do, the host compares the source MAC address being transmitted by the guest operating system with the effective MAC address for its virtual machine adapter to see if they match. When the addresses do not match, the ESXi host drops the packet. Promiscuous mode eliminates any reception filtering that the virtual machine adapter performs so that the guest operating system receives all traffic observed on the wire. By default, the virtual machine adapter cannot operate in promiscuous mode. **References:** Securing ESXi Configurations section in the *vSphere Security Guide for vSphere 6.0* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf *vNetwork Tab of the VMware Security Hardening Guides* *http://www.vmware.com/security/hardening-guides.html*

Item	Comments
Observation 6	277 VM(s) have not configured RemoteDisplay.maxConnections value.
Priority	P2
Recommendation	Limit sharing console connections if there are security concerns.

Justification	By default, more than one user at a time can connect to remote console sessions. When multiple sessions are activated, each terminal window gets a notification about the new session. If an administrator in the virtual machine logs in using a VMware remote console during their session, a non-administrator in the virtual machine might connect to the console and observe the administrator's actions. Also, this can result in an administrator losing console access to a virtual machine. For example, if a jump box is being used for an open console session, and the administrator loses connection to that box, then the console session remains open. Allowing two console sessions permits debugging by way of a shared session. For highest security, only one remote console session at a time should be allowed. **References:** *VM Tab of the VMware Security Hardening Guides* *http://www.vmware.com/security/hardening-guides.html*

Item	Comments
Observation 7	9 host(s) have host bus adapters without bidirectional CHAP authentication setup.
Priority	P2
Recommendation	Enable bidirectional CHAP authentication for iSCSI traffic so that CHAP authentication secrets are unique.
Justification	vSphere allows for the use of bidirectional authentication of both the iSCSI target and host. By not authenticating both iSCSI target and host, there is a potential for a man-in-the-middle attack where an attacker can impersonate either side of the connection to steal data. Bidirectional authentication can mitigate this risk. If the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploitation. VMware recommends that the mutual authentication secret for each host be different. Set the secret different for each client authenticating to the server so that if a single host is compromised, an attacker cannot create another arbitrary host and authenticate to the storage device. With a single shared secret, compromise of one host can allow an attacker to authenticate to the storage device. **References:** ESXi tab of the *VMware vSphere Security Hardening Guides* http://www.vmware.com/security/hardening-guides.html

3.1.4 Storage

Item	Comments
Observation 1	10 host(s) have standard port groups that use a network that is not dedicated to a single type of storage(NFS or iSCSI) traffic.

Priority	P1
Recommendation	Configure NFS and iSCSI storage traffic for performance and security.
Justification	Storage traffic is potentially the most important of all for Virtual Machine performance. When configuring the network for storage traffic it should be: • low latency and have adequate bandwidth • Use dedicated pNICs • Use a dedicated IP storage network • Use isolated networks that are placed on different subnets **References:** *vSphere Storage Guide for vSphere 6.0* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-storage-guide.pdf*

Item	**Comments**
Observation 2	18 datastore(s) do(es) not have Storage I/O Control enabled.
Priority	P2
Recommendation	Use Storage I/O Control (SIOC) to prioritize high importance virtual machine traffic.
Justification	SIOC engages only if the storage system hosting a virtual machine becomes congested, as measured by increased latency. If congestion occurs, SIOC enforces disk I/O fairness among virtual machines, even across different hosts, respecting disk shares per virtual machine. Without SIOC, disk shares enforce fairness only among virtual machines on the same host. SIOC does not function correctly unless all datastores that share the same spindles on the array have the same congestion threshold. **References:** Storage I/O Resource Allocation section in *Performance Best Practices for VMware vSphere* 6.0 http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

Item	**Comments**
Observation 3	2 datastore(s) have both VMs and Templates.
Priority	P2
Recommendation	Allocate space on shared datastores for templates and media/ISOs separately from datastores for virtual machines.

Justification	To improve performance, separate virtual machine files from other files such as templates and ISO files that have higher I/O characteristics. As best practice, dedicate separate shared datastores/LUNs for virtual machine templates and to separate ISO/FLP files from the virtual machines. As of vSphere 6.0, VMware recommends using the Content Library for Media and template storage. Media files can be placed either locally on each host or in a shared datastore. To avoid storing unnecessary copies, place media files on shared storage.

3.1.5 Virtual Machines

Item	Comments
Observation 1	11 VM(s) do not meet some of the VMotion requirements (either floppy/cd-rom found, VM in internal network, network or datastore not visible to all ESX in cluster). VMotion traffic for 10 host(s) is on less than 1 GB network.
Priority	P1
Recommendation	Verify that virtual machines meet the requirements for vSphere vMotion.
Justification	To facilitate vSphere vMotion operations of virtual machines between hosts the following requirements must be met: • The source and destination hosts must use shared storage and the disks of all virtual machines must be available on both source and target hosts, or storage will be migrated. This comes with a cost in performance, resource utilization (storage and network) while migration occurs. • The port group names must be the same on the source and destination hosts or the networking will also need to be migrated. This could impact connectivity if incorrect network is chosen. • vSphere vMotion requires a 1-Gbps network interface. However, using a 10-Gbps network interface or multiple 1-Gbps network interfaces will result in significant improvements in vSphere vMotion performance. • CPU compatibility - source and destination hosts must have compatible CPUs [relaxed for Enhanced vMotion Compatibility(EVC)]. • No devices are attached that prevent vSphere vMotion (CDROM, floppy, serial/parallel devices) are attached. Prior to bringing an ESXi host into production, testing vMotion is recommended..

	References: VMware vMotion Best Practices in the VMware vMotion section of *Performance Best Practices guide for VMware vSphere 6.0* http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf *vSphere Networking Guide for vSphere 6.0* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-networking-guide.pdf*

Item	**Comments**
Observation 2	15 VM(s) have snapshot(s).
Priority	P1
Recommendation	Limit use of snapshots, and when using snapshots limit them to short-term use.
Justification	Snapshots allow point-in-time state captures, which allow virtual machines to have their states reverted to a snapshot for testing and recovery. However, multiple snapshots result in more disk usage. Although SCSI contention was significantly improved in VMFS5, VMware recommends limiting use of snapshots, and when used, limiting them to short-term use.

Item	**Comments**
Observation 3	1 VM(s) do not have VMware Tools installed. 9 VM(s) have VMware Tools installed that are not up to date. 1 VM(s) do not have VMware Tools running.
Priority	P1
Recommendation	Verify that VMware Tools is installed, running, and up to date for running virtual machines.
Justification	Install VMware Tools (including open-vm-tools where applicable) in all guests that have supported VMware Tools available. **Note :** *open-vm-tools* is the open source implementation of VMware Tools and consists of a suite of virtualization utilities that improves the functionality, administration, and management of virtual machines within a VMware environment. The primary purpose for open-vm-tools is to enable operating system vendors and/or communities and virtual appliance vendors to bundle VMware Tools into their product releases. For compatibility and optimal performance, upgrade VMware Tools for older virtual machines to the latest versions supported by their ESXi hosts. For security purposes, disable the tools `autoinstall` option by setting

	the parameter `isolation.tools.autoInstall.disable` to True.

Item	**Comments**
Observation 4	11 VM(s) has(ve) unnecessary virtual device(s) that is/are either connected or start connected.
Priority	P2
Recommendation	Allocate only as much virtual hardware as required for each virtual machine. Disable any unused or unnecessary or unauthorized virtual hardware devices.
Justification	Provisioning a virtual machine with more resources than it requires can reduce the performance of that virtual machine and virtual machines that share the same host. For example, configuring more vCPUs than required for an application that is single threaded can reduce overall performance. Also, configuring more memory than required can impact the other virtual machines on the same host. In addition to disabling unnecessary virtual devices within the virtual machine, verify that no device is connected to a virtual machine if it is not needed there. For example, serial and parallel ports are rarely used for virtual machines in a data center environment, and CD/DVD drives are usually connected only temporarily during software installation. Disabling any unused or unnecessary virtual hardware devices improves performance (because it can reduce device polling), improves security, and reduces the probability of these devices preventing vSphere vMotion from succeeding. Disabling or disconnecting unauthorized devices enhances the security levels of the virtual machines and their hosts. Virtual machine performance can also be improved by configuring the virtual machines to use ISO images instead of physical drives. Physical drives can be avoided entirely by disabling optical drives in the virtual machines when the devices are not needed. **References:** Best Practices for Virtual Machine and Host Security sections of the *vSphere Security Guide for vSphere 6.0* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf*

Item	**Comments**
Observation 5	61 VMs are not using latest virtual hardware profile.
Priority	P2
Recommendation	Use the latest virtual hardware version to take advantage of additional capabilities.

Justification	ESXi 6.0 introduces virtual hardware version 11. By creating virtual machines using this hardware version, or upgrading existing virtual machines to this version, additional capabilities become available. This hardware version is not compatible with versions of ESXi prior to 6.0. If a cluster of ESXi hosts contains some hosts running pre-6.0 versions of ESXi, the virtual machines running on virtual hardware version 10 are constrained to run only on the ESXi 6.0 hosts. This could limit vSphere vMotion choices for vSphere DRS or DPM. **References:** *vSphere Virtual Machine Administration* Guide for vSphere 6.0 http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-virtual-machine-admin-guide.pdf

Item	**Comments**
Observation 6	2 VM(s) are not using VMXNET3 even though their configuration and guest OS support it.
Priority	P2
Recommendation	Use the latest version of VMXNET that is supported by the guest operating system.
Justification	For best performance, use the VMXNET3 paravirtualized network adapter for operating systems where it is supported. This requires that the virtual machine use at least virtual hardware version 7 and that VMware Tools be installed in the guest operating system. If VMXNET3 is not supported by the guest OS, use Enhanced VMXNET (VMXNET2). If Enhanced VMXNET is not supported in the guest operating system, then use the flexible device type, which automatically converts each AMD PCnet32 device (vlance) network device to a VMXNET device when VMware Tools is installed. Refer to information in the Knowledge Base article and product documentation for supported guest operating systems for the particular adapter. **References:** *Choosing a network adapter for your virtual machine* (1001805) http://kb.vmware.com/kb/1001805 Guest Operating System Networking Considerations section in *Performance Best Practices for VMware vSphere 6.0* http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

Item	**Comments**

Observation 7	10 VM(s) have an installed OS that differs from the configured type.
Priority	P3
Recommendation	Select the correct guest operating system type in the virtual machine configuration to match the guest operating system.
Justification	Selecting the guest operating system type determines the following: • Optimal monitor mode to use • Default optimal devices for the guest OS (such as SCSI controller and network adapter) • The optimal default resource configuration for CPU/RAM • Appropriate VMware Tools to be installed in the guest OS Verify that the guest OS type matches the operating system installed in the virtual machine to maintain the performance and manageability of the virtual machine. You can change the guest OS type only when the virtual machine is powered off.

Item	**Comments**
Observation 8	
Priority	P3
Recommendation	Use reservations and limits selectively on virtual machines.
Justification	Setting reservations and limits on virtual machines increases the management overhead of the VMware virtual infrastructure, so selectively set these only on virtual machines that need it. For reservations do not set them too high because doing so can limit the number of virtual machines that you can power on in a resource pool, cluster, or host. Setting reservations can also affect the slot size calculation for HA clusters, which can affect the admission control policy of an HA cluster (for admission control policy of number of host failures). For limits, do not set them too low because doing so can affect the amount of CPU or memory resources available to the virtual machines, which can affect the overall performance. **References:** General Resource Management section in *Performance Best Practices for VMware vSphere 6.0* http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

3.2 Findings and Recommendations for View

The following table contains summary of the results of the View Health Check that was performed during this project. Details of these items are in the following sections of this document.

Table 2: Summary of View Health Check Findings and Recommendations

Priority	Component	Recommended Action Item
P1	Desktop Operating System	Verify that all guest OS installations were performed using a clean install.
P1	Desktop Operating System	Verify that the guest operating system was created using the VMware optimization guides. Determine which optimizations were applied and verify.
P1	Infrastructure	Verify that the Horizon View environment is configured to collect event information in a Horizon View events database.
P1	View Administrator	Verify that no Horizon View services or servers are down or have been down.
P1	View Connection Server	Verify that the Horizon View connection servers are configured with a system disk of at least 70 GB.
P1	vSphere Storage	Verify that the network is configured for jumbo frames on NFS/iSCSI connections.
P1	vSphere Storage	Verify that virtual desktops are distributed evenly across datastores.
P2	ESX/ESXi hosts	Verify that there are no unusually high disk I/O latencies or IOPS (CMDS/s, GAVG).
P3	vCenter	Verify that vCenter servers supporting the Horizon View environment are dedicated only to supporting Horizon View. Use separate vCenter servers for supporting the virtualized server environment.

3.3 Priority 1 Recommendations

Item	Comments
Observation 1	Master image has optimization potential
Priority	P1
Infrastructure Qualities	Configuration.
Recommendation	Verify that all guest OS installations were performed using a clean install.
Justification	While it is common for enterprises to take an existing physical desktop

	image and convert it to be virtualized, this generally results in slower performance to both the desktop and the virtual infrastructure. Creating a clean virtual machine and installing from scratch, with the proper optimizations in place and only the required applications, provides a much better performing virtual machine and subsequently better performing host and environment. **References** Windows XP Deployment Guide http://www.vmware.com/files/pdf/XP_guide_vdi.pdf VMware View Optimization Guide for Windows 7 http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf

Item	Comments
Observation 2	Master image has optimization potential
Priority	P1
Infrastructure Qualities	Performance, configuration.
Recommendation	Verify that the guest operating system was created using the VMware optimization guides. Determine which optimizations were applied and verify.
Justification	This is critical for a smooth-running desktop operating system. Customizations improve performance considerably. **References** *VMware View Optimization Guide for Windows 7* http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf *VMware OS Optimization Tool* http://labs.vmware.com/flings/vmware-os-optimization-tool

Item	Comments
Observation 3	No event database has been running in Horizon View environment to collect View events. This observation was collected when the event database was offline. The Database periodically goes on and offline. Recommend detaching and reattaching using FQDN of database server.
Priority	P1
Infrastructure Qualities	Availability, manageability, configuration.
Recommendation	Verify that the Horizon View environment is configured to collect event information in a Horizon View events database.

Justification	This allows for segregated management of the server and isolation of components supporting Horizon View. **References** *VMware Horizon with View Installation (6.x)* https://pubs.vmware.com/horizon-view-60/topic/com.vmware.ICbase/PDF/horizon-view-60-installation.pdf *VMware Horizon View Installation (5.x)* http://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-installation.pdf

Item	**Comments**
Observation 4	4 View service(s) or server(s) is/are down.
Priority	P1
Infrastructure Qualities	Availability, configuration.
Recommendation	Verify that no Horizon View services or servers are down or have been down. Two connection servers are offline (intentional) and the events database connection periodically shows as an error.
Justification	These events can indicate problems in the environment.

Item	**Comments**
Observation 5	2 Connection server(s) are configured with system disk size less than the recommended size.
Priority	P1
Infrastructure Qualities	Availability, manageability, configuration.
Recommendation	Verify that the Horizon View connection servers are configured with a system disk of at least 70 GB.
Justification	The system disk should be 70GB or greater if you are configuring Horizon View. **References** *VMware Horizon with View Architecture Planning (6.x)* https://pubs.vmware.com/horizon-view-60/topic/com.vmware.ICbase/PDF/horizon-view-60-architecture-planning.pdf *VMware Horizon View Architecture Planning (5.x)* http://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-architecture-planning.pdf

Item	Comments
Observation 6	10 NFS/ISCSI connections have been found to have management ports not configured for jumbo frames.
Priority	P1
Infrastructure Qualities	Performance, scalability, configuration.
Recommendation	Verify that the network is configured for jumbo frames on NFS/iSCSI connections.
Justification	Use of jumbo frames enhances storage performance. **References** *Performance Best Practices for VMware vSphere (5.5)* http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf *Performance Best Practices for VMware vSphere (5.1)* http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf *Performance Best Practices for VMware vSphere (5.0)* http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf

Item	Comments
Observation 7	Desktops on 2 datastore(s) are not distributed evenly.
Priority	P1
Infrastructure Qualities	Manageability, performance, scalability, configuration.
Recommendation	Verify that virtual desktops are distributed evenly across datastores.
Justification	This reduces storage contention and balances I/O loads. This helps to avoid SCSI reservation locking, for example. An even distribution of desktops spreads the I/O load so you do not have a single datastore handling most of the total I/O or causing unnecessary storage I/O contention. This goes together with the practice of rebalancing. In some situations, there may be different datastores for those very different desktop pool workloads, but even then you should balance the desktop distribution.

3.4 Priority 2 Recommendations

Item	Comments
Observation 1	Monitor VM statistics to ensure appropriate sizing.

Priority	P2
Infrastructure Qualities	Performance.
Recommendation	Verify that there are no unusually high disk I/O latencies or IOPS (CMDS/s, GAVG).
Justification	Many Horizon View implementations are impacted by poor storage design or performance. These issues can be identified on ESX hosts running virtual desktop workloads using ESXTOP. **References** Interpreting esxtop 4.1 Statistics http://communities.vmware.com/docs/DOC-11812

3.5 Priority 3 Recommendations

Item	**Comments**
Observation 1	1 vCenter(s) is/are not exclusively used for Horizon View environment.
Priority	P3
Infrastructure Qualities	Manageability, performance, scalability, configuration.
Recommendation	Verify that vCenter servers supporting the Horizon View environment are dedicated only to supporting Horizon View. Use separate vCenter servers for supporting the virtualized server environment. This is a small environment. It is best practice to have two vCenter servers, one managing the server systems and another managing only the desktop systems.
Justification	This allows for segregated management and provides room for growth as desktop deployments increase in the future. **References** *VMware Horizon with View Installation (6.x)* https://pubs.vmware.com/horizon-view-60/topic/com.vmware.ICbase/PDF/horizon-view-60-installation.pdf *VMware Horizon View Installation (5.x)* http://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-installation.pdf

5. VMware View Environment

The MSPB VMware View infrastructure must support up to 300 virtual desktops. There are currently 225 users configured.

This section provides the inventory of VMware View infrastructure collected during this engagement. It is important for MSPB to consider the recommendations given earlier in this document. The recommendations will assist MSPB in optimizing the existing implementation and enable the environment to scale with an acceptable and stable level of performance.

5.1 VMware View Inventory

5.1.1 View Connection Servers

5.1.1.1. Platform Specifications

- System: VMware Virtual Machine
- CPU: 4 vCPU
- RAM: 10 GB
- Disk: 140,0,120 GB

5.1.1.2. View Connection Server Virtual Machines

(b) (7)(E) [redacted]

- Role: (b) (7)(E) [redacted]
- NICs: 1 vNIC
- VMware Tools: guestToolsCurrent
- Virtual Devices: CD/DVD ,1 Floppy
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

(b) (7)(E) [redacted]

- Role: (b) (7)(E) [redacted]
- NICs: 1 vNIC
- VMware Tools: guestToolsCurrent
- Virtual Devices: CD/DVD ,1 Floppy
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

(b) (7)(E) [redacted]

- Role: (b) (7)(E) [redacted]
- NICs: 1 vNIC
- VMware Tools: guestToolsCurrent
- Virtual Devices: CD/DVD ,1 Floppy
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

(b) (7)(E)

- Role: (b) (7)(E)
- NICs: 1 vNIC
- VMware Tools: guestToolsCurrent
- Virtual Devices: CD/DVD ,1 Floppy
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

(b) (7)(E)

- Role: (b) (7)(E)
- NICs: 1 vNIC
- VMware Tools:
- Virtual Devices: N/A
- Version: - 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

(b) (7)(E)

- Role: (b) (7)(E)
- NICs: 1 vNIC
- VMware Tools:
- Virtual Devices: N/A
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

5.1.2 Hosted View Desktop Environment

vCenter Server Clusters

- (b) (7)(E) [redacted]
    - ESX Versions: VMware ESXi - 5.5.0
- (b) (7)(E) [redacted]
    - ESX Versions: VMware ESXi - 5.5.0
- (b) (7) (E) [redacted]
    - ESX Versions: VMware ESXi – 5.5.0

5.1.3 View Desktop Pools

The configuration of these desktop pools is detailed in the following sections.

TEST

Type	Automated Desktop Pool
Desktop persistence	Floating
Desktop source	vCenter (linked clone)
Display state	Enabled
Number of desktop sources	6
vCenter Server	(b) (7)(E)
Tags	
When virtual machine is not in use	alwaysOn
Automatic logoff after disconnect	After
Allow user resets	No
Allow multisessions per user	No
Default display protocol	PC-over-IP
Allow user protocol override	Yes
Adobe Flash quality	noControl
Adobe Flash throttling	Disabled
Advanced Parameters	PCoIP # of monitors: 4 PCoIP Resolution: 1920x1200

MSPB

Type	Automated Desktop Pool
Desktop persistence	Floating
Desktop source	vCenter (linked clone)
Display state	Enabled

Number of desktop sources	200
vCenter Server	(b) (7)(E)
Tags	
When virtual machine is not in use	alwaysOn
Automatic logoff after disconnect	After
Allow user resets	No
Allow multisessions per user	No
Default display protocol	PC-over-IP
Allow user protocol override	Yes
Adobe Flash quality	noControl
Adobe Flash throttling	Disabled
Advanced Parameters	PCoIP # of monitors: 4 PCoIP Resolution: 2560x1600

5.1.4 Virtual Desktop Master Images

A virtual machine master is a copy, or *golden image*, of a virtual machine that can be used to create and provision new virtual machines. Typically, a master image includes an installed guest operating system and a set of applications.

It is a best practice to deploy a desktop pool manually or automated from a standardized desktop source, or template. Provisioning virtual machines in a desktop pool configures all virtual machines with the same settings, loaded operating system, applications and patches.

In addition, consider multiple desktop templates based on pool, department, or function. This is so that specific optimizations can be made to particular department virtual desktops without adversely affecting another desktop pool, while maintaining an efficient virtual desktop environment.

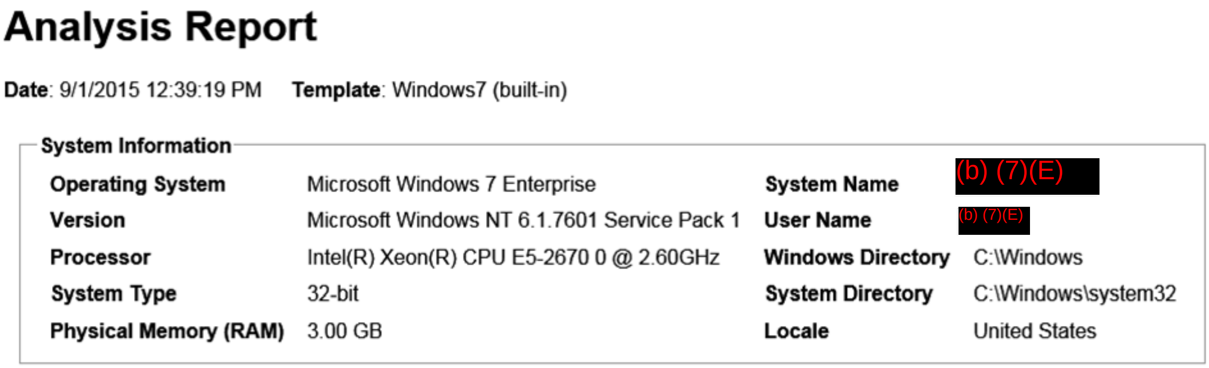
Conforming to these best practices reduces the complexities of troubleshooting, desktop pool deployments, recomposing, or recovering processes.

5.1.4.1. Desktop Master Build Process

The current desktop build process adheres to VMware best practices. MSPB uses the VMware Optimization Tool to maximize the performance on the linked clone desktops. It is recommended to continue to use the Optimization Tool and create additional master images dedicated to different use cases with isolated applications specific to users needs.

5.1.4.2. Master Desktop Virtual Machine Specifications

The following is a detailed report for the master image. All of the items identified with a yellow box are available optimizations that MSPB may benefit from configuring on the master image.



Analysis Report

Date: 9/1/2015 12:39:19 PM **Template**: Windows7 (built-in)

System Information

Operating System	Microsoft Windows 7 Enterprise	**System Name**	(b) (7)(E)
Version	Microsoft Windows NT 6.1.7601 Service Pack 1	**User Name**	(b) (7)(E)
Processor	Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz	**Windows Directory**	C:\Windows
System Type	32-bit	**System Directory**	C:\Windows\system32
Physical Memory (RAM)	3.00 GB	**Locale**	United States

Details:

	Steps	Description	Expected Result	Actual Result
Apply HKCU Settings to Registry				
	Load HKCU for editing	Open HKey Users (Default User Profile) for Editing		
	Action Center Icon - Disable	The Action Center Icon notifies the user of the firewall, anti virus, security related things, etc. that may be configured differently than expected. Disabling this service can be useful to avoid end user confusion.	1	
	Default power setting	Set Start button > Power to log off as the default.	1	
	Default Screen Saver	Set the default screen saver to "Blank" - any graphics screensaver will put extra load on the virtual infrastructure.	%windir%\system32\scrnsave.scr	
	Lower Terminal Server Client send interval	Lower Terminal Server Client send interval	1	
	Reduce Menu Show Delay	Delay Show the Reduce Menu	120	

	Steps	Description	Expected Result	Actual Result
	RSS Feeds - Disable	Perform this task to disable RSS feed capability and potentially improve performance and reduce requirements for disk space growth related to this service.	0	
	Screen Save Secure	Secures the VM in case a user walks away	1	🟨
	Screen Saver Timeout	Timeout set to 10 mins	600	🟨
	Set Default Wallpaper	Set wallpaper to a "non existing" file to disable the end users ability to set a wallpaper.		
	Temporary Internet Files to Non Persistent	Purge cache for IE on every close of IE. Non persistence	0	
	Visual Effects	Set Windows Visual Effects to Optimized for best performance.	3	🟨
	Unload HKCU for editing	Very Important Step! Need to close the ntuser.dat file to save changes.		
Apply HKLM Settings				
	Application Event Log Max Size	Set max size on Event Log to 1 MB	1048576	1048576
	Application Event Log Retention	Set no retention	0	0
	Background Layout Service - Disable	Disable Background Layout Service	0	0

	Steps	Description	Expected Result	Actual Result
	CIFS Change Notifications - Disable	Disable CIFS Change Notifications	1	1
	Crash Control - Automatically Reboot - Enable	Enable Automatically Reboot for the Crash Control	1	1
	Crash Control - Sending alert - Disable	Disable sending alert for the Crash Control	0	0
	Crash Control - Writing event to the system log - Disable	Disable writing event to the system log for the Crash Control	0	0
	Creation of Crash Dump - Disable	Removes the creation of a Crash Dump file	0	0
	Customer experience improvement program - Disable	Disable customer experience improvement program	0	0
	Disk Timeout Value	How long the OS will wait for a disk write or read to take place on the SAN without throwing an error	200	200
	Do not buffer UDP packets less than 1500 Bytes	Improves high bandwidth video performance	1500	1500
	Enable Remote Desktop	Enables RDP	0	0
	Hide Fast User Switching	Hide Fast User Switching	1	1
	Hide Hard Error Messages	Hide Hard Error Messages	0	0

	Steps	Description	Expected Result	Actual Result
	IE Wizard - Disable	Removes the customization wizard upon first launch of Internet Explorer	1	1
	Image Revision	Image Revision	1.0	1.0
	Image Virtual	Registry Entry to identify if virtual machine	Yes	Yes
	Increase Service Startup Timeout	Allows up to 120 seconds before timing out waiting for a service	120000	120000
	IPv6 - Disable	Disable IPv6	255	255
	Machine Account Password Changes - Disable	Disable Machine Account Password Changes	0	0
	Network Location	Creates a blank key that disables the "Choose default network location" prompt.		
	Remote Desktop Authentication	Sets default authentication level.	0	
	Screen Saver at Logon/Welcome Screen - Disable	Making modifications to .DEFAULT	0	0
	Security Event Log Max Size	Set max size on Event Log to 1 MB	1048576	
	Security Event Log Retention	Sets no retention	0	
	Set Wallpaper to blank at Logon/Welcome Screen	Making modifications to .DEFAULT		

	Steps	Description	Expected Result	Actual Result
	Storing Recycle Bin Files - Disable	Deleting files will delete immediately instead of storing in the recycle bin. Same behavior as non persistent VM	1	1
	Superfetch (Registry) - Disable	Set Superfetch to boot files only.	0	0
	System Event Log Max Size	Set max size on Event Log to 1 MB	1048576	1048576
	System Event Log Retention	Set no retention	0	0
	System Restore - Disable	Disable System Restore. System Restore provides rollback capability that should not be leveraged in a VDI environment. Space and reliability are factors.	1	1
	TCP/IP Task Offload - Disable	Disable TCP/IP Task Offload	1	1
	UAC - Disable	Disables User Access Control. Use Group Policy to configure more granularly	0	0
	Windows Sideshow - Disable	Disable Windows Sideshow	1	1
	Windows Update - Disable	Disable Automatic Update - important for non persistent VMs	1	0
Disable Features				
	Boot GUI	Disable the graphic for the Windows 7 boot	N.A	N.A

	Steps	Description	Expected Result	Actual Result
	Delete Restore Points for System Restore	Removes all restore points if they exist	N.A	N.A
	Firewall (All Profiles)	Netsh to disable firewall on all profiles.	N.A	N.A
	Hibernation for Power Config	Disable Hibernation for Power Config	N.A	N.A
	Last Access Timestamp	Disable Last Access Timestamp	N.A	N.A
	Stop Superfetch Service	Stop Superfetch Service	N.A	N.A
	System Restore	Powershell command to immediately disable system restore	N.A	N.A
Disable Scheduled Tasks				
	Application Experience - AitAgent	Disable Application Experience - AitAgent	DISABLED	Disabled
	Application Experience - Program Data Updator	Disable Application Experience - Program Data Updator	DISABLED	Enabled
	CEIP Consolidator	Disable Customer Experience Improvement Program (CEIP) scheduled task	DISABLED	Disabled
	CEIP Kernel	Disable Customer Experience Improvement Program (CEIP) scheduled task	DISABLED	Disabled
	CEIP Usb	Disable Customer Experience Improvement Program (CEIP)	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
		scheduled task		
	Defrag Schedule	Disable Defrag Schedule	DISABLED	Disabled
	Registry Idle Backup Task	Disable Registry Idle Backup Task	DISABLED	Disabled
	System Restore Schedule	Disable System Restore Schedule	DISABLED	Disabled
	Windows Defender Idle Task	Disable Windows Defender Idle Task	DISABLED	
	Windows Defender Schedule	Disable Windows Defender Schedule	DISABLED	Disabled
	WinSAT	Measures performance of Windows 7 and provides an index number. Causes performance impact on VMs.	DISABLED	Disabled
Disable Services				
	Background Intelligent Transfer Service	Transfers files in the background using idle network bandwidth. If the service is disabled, Windows Update and MSN Explorer cannot automatically download programs and other information.	DISABLED	Manual
	Bitlocker Drive Encryption Service	Bitlocker service for drive encryption. Not recommended to encrypt VDI virtual machines.	DISABLED	Disabled
	Block Level Backup Engine Service	Used by Windows Backup	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
	BranchCache	Used for caching files on server in a branch office.	DISABLED	Disabled
	Change Group Policy Client start mode to manual	Responsible for applying settings configured by administrator for the computer and users through the Group Policy component.	MANUAL	Auto
	Computer Browser	Used for browsing computers on the same network.	DISABLED	Disabled
	Desktop Window Manager Session Manager	Used for Aero - disable if Aero is not desired. (VMware product compatibility: Do not disable if View 5.3 package will be installed.)	DISABLED	Auto
	Diagnostic Policy Service	Disable Diagnostic Policy Service	DISABLED	Disabled
	Diagnostic Service Host	Problem detection and troubleshooting resolution.	DISABLED	Disabled
	Diagnostic System Host	Problem detection and troubleshooting resolution.	DISABLED	Disabled
	Disk Defragmenter Service	Defrag can create unnecessary overhead on a virtual machine - the scheduled defrag has been set to disable below as well as disabling this service.	DISABLED	Disabled
	Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD providers supply network discovery services for the Simple Services Discovery Protocol (SSDP) and Web	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
		Services - Discovery (WS-D) protocol.		
	Function Discovery Resource Publication	Publishes his computer and resources attached to this computer so they can be discovered over the network.	DISABLED	Disabled
	HomeGroup Listener	Used for Homegroup services - N/A for VDI	DISABLED	Unknown
	HomeGroup Provider	Used for Homegroup services - N/A for VDI	DISABLED	Disabled
	Interactive Services Detection	Displays a dialog box when a service tries to send a message to the console.	DISABLED	Disabled
	IP Helper	Disable if IPv6 is not a factor in VDI	DISABLED	Disabled
	Media Center Extender	Allows Media Center Extenders to locate and connect to the computer.	DISABLED	
	Microsoft iSCSI Initiator Service	Not leveraged in a VDI	DISABLED	Disabled
	Microsoft Software Shadow Copy Provider	Leveraged by Windows Backup and System Restore.	DISABLED	Disabled
	Offline Files	Disable Offline Files	DISABLED	Disabled
	Reports and Solutions Control Panel Support	Provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports and Solutions control panel.	DISABLED	Disabled
	Secure Socket Tunneling	VPN tunneling service. Not likely leveraged in a	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
	Protocol Service	VDI environment.		
	Security Center	Remove the task tray regarding security center warnings	DISABLED	Disabled
	SSDP Discovery	Disable SSDP Discovery	DISABLED	Disabled
	Superfetch	Service is leveraged to optimize loading of applications over time. In a non persistent or commodity based VDI environment this service may impact performance. Depends on use and organization.	DISABLED	Disabled
	Tablet Services	Disable if you are not using Tablet PC functionality	DISABLED	Disabled
	Themes	Disable if you want to run "Classic" GUI	DISABLED	Disabled
	Universal PnP Host Service	Dependent on the SSDP Service.	DISABLED	Disabled
	Volume Shadow Copy Service	Used for System Restore and Backup Operations. (VMware product compatibility: Do not disable if Persona Management is in use.)	DISABLED	Disabled
	Windows Backup	Windows Backup service used by System Restore and Windows Backups.	DISABLED	Disabled
	Windows Defender Service	Windows Defender can be optionally disabled in a VDI environment especially for non persistent VMs where data will be purged. A scheduled task has also been marked to disable	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
		below.		
	Windows Error Reporting Service	Error reporting services leveraged by Applications when they crash to send reports to Microsoft. If using DER within VDI consider alternate configuration.	DISABLED	Disabled
	Windows Firewall	Recommended to customize instead of disable the firewall.	DISABLED	Auto
	Windows Media Center Network Sharing Service	Used by Media Center	DISABLED	Disabled
	Windows Media Center Receiver Service	Media Center Service Related	DISABLED	
	Windows Media Center Scheduler Service	Media Center Service Related	DISABLED	
	Windows Search	If you do a lot of searching on a VM, do not disable this service.	DISABLED	Disabled
	Windows Update	If this is a non persistent VM, Windows Update should be handled differently via standard image maintenance practices.	DISABLED	Disabled
	WLAN AutoConfig	Wireless LAN Configuration - N/A for VDI environments.	DISABLED	Disabled
	WWAN AutoConfig	Service related to Mobile Broadband Devices	DISABLED	Disabled
Disable Visual Effects				

	Steps	Description	Expected Result	Actual Result
	Aero Peek	Disable Desktop Window Manager Aero Peek Visual Effect	0	1
	Animate Min/Max Windows	Disable Animate Min/Max Windows Visual Effect	0	1
	ComboBox Animation	Disable ComboBox Animation Visual Effect	0	1
	Control Animations	Disable Control Animations Visual Effect	0	1
	Cursor Shadow	Disable Cursor Shadow Visual Effect	0	1
	Desktop Window Manager	Disable Desktop Window Manager Visual Effect	0	1
	Drag Full Windows	Disable Drag Full Windows Visual Effect	0	1
	Drop Shadow	Disable Drop Shadow Visual Effect	0	1
	Font Smoothing	Disable Font Smoothing Visual Effect	0	1
	ListBox Smooth Scrolling	Disable ListBox SmoothScrolling Visual Effect	0	1
	Listview Alpha Select	Disable Listview Alpha Select Visual Effect	0	1
	Listview Shadow	Disable Listview Shadow Visual Effect	0	1
	Menu Animation	Disable Menu Animation Visual Effect	0	1
	Save Thumbnail	Disable Save Thumbnail Visual Effect	0	0

	Steps	Description	Expected Result	Actual Result
	Selection Fade	Disable Selection Fade Visual Effect	0	1
	Taskbar Animations	Disable Taskbar Animations Visual Effect	0	1
	Thumbnails Or Icon	Disable ThumbnailsOrIcon Visual Effect	0	1
	Tooltip Animation	Disable Tooltip Animation Visual Effect	0	1
	Transparent Glass	Disable Transparent Glass Visual Effect	0	1
VMware Components				
	VMware Tools	VMware Tools		
	VMware View Agent	VMware View Agent.		Registry key not found.
	VMware View Agent Debug - Disable	VMware	False	False
	VMware View Agent Trace - Disable	VMware	False	False

5.2 End User Persona

End user profile management is achieved using Liquidware Labs Profile Unity. It is recommended to engage Liquidware Labs in order to gather all necessary configurations to optimize the login process and deliver the best experience to the end users.

6. Recommendations

6.1 vSphere Recommendations

- Review above observations and make configuration enhancements based on business need
- Use resource pools for workload grouping
- Enable syslog collecting of ESXi environment (Configured, not enabled)

- Move vSphere Database to a dedicated SQL server (presently co-installed on the vSphere server)
- Set a max memory allocation for SQL server
- Increase size of Microsoft Event Log and collect a regular bundle for future analysis
- Discussed the importance of monitoring and root cause identification
- Leverage out of box monitoring and alerting in vSphere and View for regular review

6.2 Horizon View Recommendations

- Continue using the VMware OS Optimization tool for virtual desktops
- GPOs for PCoIP optimization (build to lossless, max image size, copy/paste and resolution for desktops, etc.)
- Using multiple datastores in more than one array for redundancy of View desktops
- Using connection server tags to provide explicit paths to users desktops
- Deploying cloud pod architecture for Horizon View redundancy and potential disaster recovery
- Providing connection server redundancy (load balancing) for high availability desktops
- Investigate the View Administrators Toolbox (located in labs.vmware.com/flings) for the ability to use more Horizon View metrics
- Discussions around some issues they have been experiencing within their View desktop environment
  - Cursor disappearing in View sessions (registry key, *kb.vmware.com/kb/2081495*)
  - KMS activation for Office (Use Office customization tool and check box activate with KMS and provide KMS server FQDN)
  - Typing lag on office applications in View sessions (Group Policy setting for View Agent)
  - Allowing larger screen resolutions (Group Policy setting for View Agent)
  - Printing issues (garbled text) when printing from a View session (usually caused by firmware/driver mismatch or older version of VMware tools. Will need to investigate as to which component is causing the issue)
  - Unlocking multiple desktops while using Horizon View client (Will need to investigate pass thru options)

6.3 Operational Recommendations

- Use the Liquidware Labs Stratusphere product (already own licensing and Profile Unity) to maintain higher visibility within the Virtual Machines and applications and the resources they consume.
- Use the Nutanix dashboard that was included in the host and storage solution for identifying metrics from physical components.
- Discussed vRealize Operations Manager and its ability to add value for maintaining a proactive environment.
- Develop regular habits to check dashboards and messages generated by infrastructure

6.4 Additional Recommendations

- Recommend advanced training on products for support personnel
- Enlisting a VMware resource while planning and preparing for product upgrades
- Annual Health Checks for the environment

Appendix A: References

Item	URL
Documentation	http://www.vmware.com/support/pubs
VMTN Technology information	http://www.vmware.com/vcommunity/technology
VMTN Knowledge Base	http://kb.vmware.com
Discussion forums	http://www.vmware.com/community
User groups	http://www.vmware.com/vcommunity/usergroups.html
Online support	http://www.vmware.com/support
Telephone support	http://www.vmware.com/support/phone_support.html
Education services	http://mylearn.vmware.com/mgrreg/index.cfm
Certification	http://mylearn.vmware.com/portals/certification/
Technical papers	http://www.vmware.com/vmtn/resources

U.S. Merit Systems Protection Board (MSPB) IT Assessment Project

Prepared For:

MSPB
1615 M St, NW, Suite 500
Washington, D.C. 20036

Final Report
MSP-MSP-15-K-00044

Prepared By:

Cask, LLC
1940 Duke Street
Alexandria, VA 22314

October 30, 2015

October 30, 2015

US Merit Systems Protection Board (MSPB)
1615 M St, NW, Suite 500
Washington, D.C. 20036

Attention: (b) (6) [redacted], Contracting Officer

Subject: Final Report

Reference: Contract MSP-MSP-15-K-00044 MSPB IT Assessment Project

Dear (b) (6) [redacted]:

Cask is very pleased to deliver this Final Report in support of the MSPB IT Assessment project. If you have any questions please contact myself at (b) (6) [redacted], or electronically at (b) (6) [redacted].

Sincerely,

(b) (6) [redacted]

(b) (6) [redacted]
Cask, LLC

Enclosures:
Final Report

Executive Summary

Goals

The Merit Systems Protection Board (MSPB) is seeking to shift from paper-based work processes and products to automated, electronic adjudication and convert to 100% electronic case processing to substantially improve the delivery and efficiency of adjudication services. This strategy is called e-Adjudication.

Objective

In addition to conducting other technical assessments of the VMWare and Oracle infrastructure, MSPB engaged Cask to conduct "an independent review of existing IT infrastructure, virtualization strategy and operational processes and procedures to identify areas where improvements can be made as well as recommend changes that will benefit the quality, efficiency and/or effectiveness of MSPB's IT-related products and services. This will include taking a holistic approach to make certain that MSPB's IT systems are effectively and efficiently designed to meet an organization of its size, budget and scope of business.

Observations

The catastrophic failure of the entire virtual environment on 30 June 2015, a key component to the e-Adjudication strategy, and the resulting loss of data, configuration and confidence of the user community has halted much of the e-Adjudication strategy in the near term. Cask assessed the operation processes and technical capabilities in Information Resource Management (IRM) and made numerous observations. Nearly every interview that Cask conducted with MSPB personnel traced back to the question:

"Can the goals of e-Adjudication be enabled by IRM?"

Our analysis and recommendations are detailed in this report. We grouped our findings into three broad IT goals:

Goal	Definition
Manage technology acquisition within organization in support of business objectives	This includes managing the process of translating business requirements into technical requirements as well as scoping, prioritizing, and managing resultant projects to achieve the technical requirements and enable the business objectives holistically across the enterprise.
Attain and maintain repeatable processes	This includes establishing and maintaining operational processes that can provide common and repeatable methodologies to reduce reliance on the availability of specific personnel.
Manage technology in accordance with best industry practices	This includes the use of tools and practices as recommended by Original Equipment Manufacturers (OEM) to provide technical management of IT infrastructure.

In addition, we conducted interviews across IRM to assess organizational competencies and skills as well as customer interviews to better understand the environment. Cask firmly believes that of the three legs of any IT capability (people, process, and technology) it is the people (or organization) that lies at the heart of demonstrated capability. What we saw with the operation is mostly symptomatic of answers to the following questions:

- Are there any missing roles?
- Are the significant gaps between the criticality of any role and IRM's ability to perform that role?
- Are there significant competency rating deficiencies within any roles?
- Are there significant skill rating deficiencies within any roles?

Our analysis identified the following answers to these questions aligned to the three IT goals:

Organizational Skills Finding Category	**Goal**		
	Manage Technology Acquisition within Organization ISO Business Objectives	**Attain and Maintain Repeatable Processes**	**Manage Technology IAW Best Industry Practices**
Missing Roles	*Service Manager*	*IT Security Manager*	*IT Security Specialist*
Gap Between Role Criticality and Ability	*Enterprise Architect*	*QA Manager*	*Network Specialist*
Low Competency Ratings	*IT Consultant* *Systems Analyst*	*IT Operations Manager*	*Network Specialist*
Low Technical Skills Rating			*Systems Administrator* *Network Specialist*

In concert with the organizational skills assessment, Cask conducted a process and technology assessment within IRM. We made 42 specific observations with recommendations. The following table provides a summary of the process and technology assessment by priority within each of the IT goals. It should be noted that there are positive comments in this summary. Of particular note are the robust network and virtual environment infrastructures that MSPB have implemented.

IT Goal	**Category**	**Priority**			**Summary**
		High	**Med**	**Low**	
Manage technology acquisition within organization in support of business objectives	Tech Acq	4	2	1	» There are significant technical obstacles to VDI enablement and acceptance; outside professional services is probably necessary » There are also significant organizational acceptance obstacles; a deliberate Organizational Change Management (OCM) effort may be necessary » Documentation of requirements and technical instantiation of key systems supporting core business functionality is lacking
Attain and maintain repeatable processes	Network	3	0	0	» Key network security and management processes are not in place and must be implemented
	Service Mgmt	3	3	0	» Operational processes are not documented leaving the infrastructure vulnerable to failures and maintaining continuity » The lack of documentation and independent configuration backups prior to the virtual environment failure set back the VDI implementation a number of months

IT Goal	Category	Priority			Summary
		High	Med	Low	
Manage technology in accordance with best industry practices	Data Protection	4	2	2	» Disaster Recovery Planning must be conducted, implemented, and maintained » Ongoing data backup of all systems should be reviewed for completeness, capability, and tested
	Infra-structure	5	1	1	» Core business applications require upgrading so they are capable of running with supported hardware and software » An adequate Development/Test environment and promotion procedures must be established
	Virtual	0	2	5	» Ironically, despite the historical failure event of the virtual environment, the virtual infrastructure is pretty solid
	Network	1	1	0	» Network infrastructure at MSPB headquarters is robust » Network monitoring tools need to be implemented » Network cabling standards are not utilized and can lead to failures
	Data Center	1	1	0	» The data center infrastructure is inadequate and cost/effort prohibitive to fix » However, there are some relatively simple actions that can be taken to improve the DC
	Total	**21**	**12**	**9**	» **42 Total Observations**

Conclusion

Upon consideration of all of the organizational, process and technology assessment observations, we conclude that although there are significant obstacles, with sufficient resourcing IRM can meet the vast majority of e-Adjudication goals. We couch this statement because prioritization of requirements must take place as there is rarely unlimited funding to solve all technical issues or personnel resourcing. In the next section we will present a number of overarching recommendations for consideration to effect this conclusion.

Overarching Recommendations

We have synthesized the organizational, process and technology observations and recommendations into five (5) overarching recommended courses of action. They are presented within their broad IT Goal.

Within the Manage Technology Acquisition goal, there is really an overarching recommended course of action to formalize the entire process of developing and managing business requirements through their enablement as IT capabilities and operations. There are four parts of Rec #1(a – d) to achieving this as depicted in Figure (i). The Process and Technology IT Goals include Rec #2 - #5 that are operational in nature.

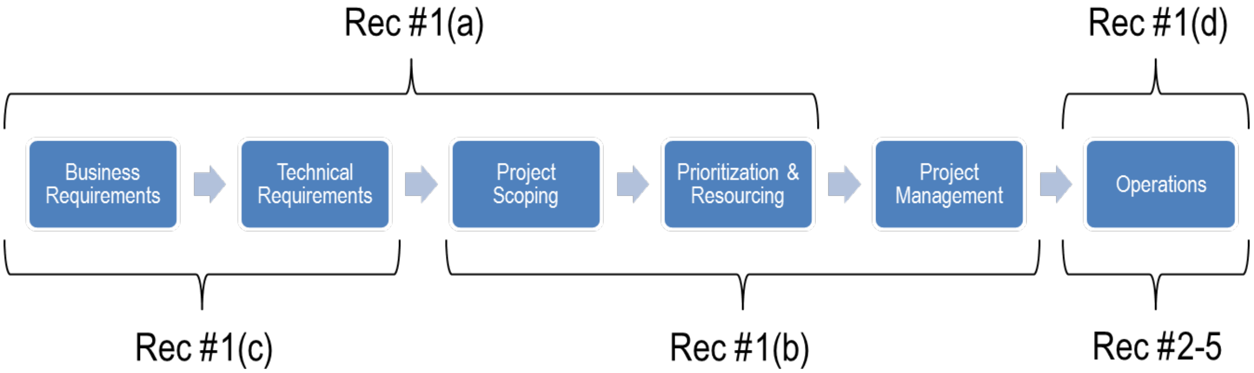


Figure i: Technology Acquisition to Operations Sequence

A. Manage Technology Acquisition

Rec #1(a).	Review the relationship between Clerk of the Board (CoB) and IRM
Rec #1(b).	Develop a transition plan for the IT infrastructure
Rec #1(c).	Update core business applications
Rec #1(d).	Assign a Service Manager

B. Repeatable Operational Processes

Rec #2.	Invest in a prioritized and systematic development and implementation of operational processes and tools to manage IT infrastructure

C. Manage Technology

Rec #3(a).	Continue to use virtualization services to consolidate IT footprint
Rec #3(b).	Continue to pursue VDI as the correct path for client services
Rec #4.	Invest in a dedicated network administrator
Rec #5.	Conduct a Business Case Analysis (BCA) and Analysis of Alternatives (AoA) for a hosting solution

Cask believes that all of the overarching recommendations are of a high priority and should be considered for implementation. However, they have different resourcing and schedule requirements and may not be considered of equal priority by MSPB. Cask understands that it is not feasible with a small organization like MSPB to launch multiple efforts simultaneously with equal attention. This is why we have recommended the use of a third-party or hiring action with a number of these recommendations to provide particular expertise that we feel MSPB may not have and/or provide the extra hands and feet to more efficiently accomplish tasks without diluting internal MSPB resources beyond their effectiveness. However, this approach takes commitment and funding resourcing from management.

TABLE OF CONTENTS

Introduction

Purpose

MSPB required an independent review of existing IT infrastructure, virtualization strategy and operational processes and procedures to identify areas where improvements can be made as well as recommend changes that will benefit the quality, efficiency and/or effectiveness of MSPB's IT related products and services. This included taking a holistic approach to make certain that MSPB's IT systems are effectively and efficiently designed to meet an organization of its size, budget and scope of business. More specifically MSPB requested the following assessments:

- Perform an assessment on MSPB's entire virtual infrastructure
- Perform an assessment on all of MSPB's major business applications
- Perform an assessment on MSPB's network infrastructure (LAN and WAN)
- Perform an assessment on all computer operational processes

In addition, Cask offered two additional assessments in order to provide a truly holistic baseline assessment of the People, Process and Technology associated with information systems operation with MSPB.

- Perform an assessment on MSPB's data center facility infrastructure; i.e. architectural, electrical, mechanical, fire suppression, and physical security
- Perform an assessment on MSPB's data center operations staff organizational management

Background

MSPB Mission

The mission of MSPB is to protect Federal merit systems and the rights of individuals within those systems. The Board carries out its statutory responsibilities and authorities primarily by adjudicating individual employee appeals and by conducting merit system studies.

MSPB headquarters located in Washington, DC, has eight offices that are responsible for conducting its statutory and support functions. The Directors of these eight offices report to the Chairman through the Executive Director. MSPB also has six regional and two field offices located throughout the United States.

Information Technology

The MSPB's primary mission is to provide for independent adjudication of appeals of personnel actions for Federal employees. Many of the appeals filed with the agency are from *pro se* appellants -- employees representing themselves. Pro se appellants do not generally have equal knowledge of the case filing process or equal access to the information available, especially if they are stationed overseas. Yet, they are expected to file an appeal and to respond to orders in a timely manner or risk having their cases dismissed.

MSPB is looking to shift from paper-based work processes and products to automated, electronic adjudication and convert to 100% electronic case processing to substantially improve the delivery and efficiency of their adjudication services. The MSPB's electronic filing system, e-Appeal Online, allows Federal agencies and employees instant access to filings and issuances through the internet as soon as they are uploaded. It also provides the pro se appellants relevant information at each step of the filing process to assist them in submitting material and correct answers to the questions on the automated appeal form. Parties who file electronically can also receive acknowledgement orders from the agency by e-mail instantaneously, rather than through the regular mail.

The agency has also implemented an agency-wide, electronic Case Management System (CMS). The system is used to process and track each initial appeal and Petition for Review filed with the agency. CMS has also been integrated with the MSPB's e-Appeal, document management, and document assembly systems to allow our Administrative Judges and Attorneys to more efficiently create legal documents that are pre-populated with case data. In addition, MSPB has implemented an agency-wide, web-based office calendar system to make staff aware of scheduled events, such as hearings, leave, and outreach. In FY 2014, MSPB piloted the Virtual Desktop Infrastructure (VDI) technology, which allows MSPB employees easy and efficient access to their desktop while working at home or on travel. In FY 2015, VDI was implemented agency-wide.

Methodology

Cask conducted a baseline assessment of MSPB. The baseline assessment included interviews and a review of the documentation provided by MSPB. As part of the engagement, Cask used a customized version of the Tudor ITSM Process Assessment (TIPA) methodology (www.tipaonline.org) to provide a standardized and repeatable assessment and report results (Figure 1). The assessment leveraged Information Technology Infrastructure Library (ITIL®) v3, the European e-Competence Framework v3.0, Original Equipment Manufacturer (OEM), and Building Industry Consulting Services International (BICSI) Data Center and Network Design and Implementation Best Practices. Cask utilized our assessment methodology to identify areas where improvements can be made as well as recommend changes that will benefit the quality, efficiency and/or effectiveness of MSPB's IT related People, Process and Technology.

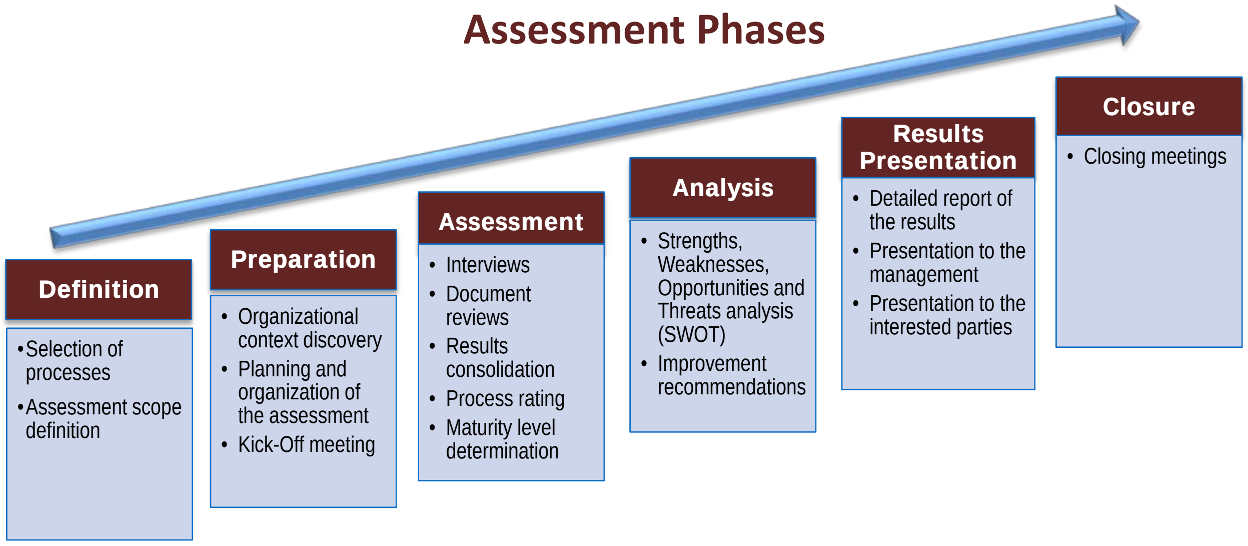

Assessment Phases
Definition
•Selection of processes
•Assessment scope definition
Preparation
• Organizational context discovery
• Planning and organization of the assessment
• Kick-Off meeting
Assessment
• Interviews
• Document reviews
• Results consolidation
• Process rating
• Maturity level determination
Analysis
• Strengths, Weaknesses, Opportunities and Threats analysis (SWOT)
• Improvement recommendations
Results Presentation
• Detailed report of the results
• Presentation to the management
• Presentation to the interested parties
Closure
• Closing meetings

Figure 1: Assessment Methodology

References

Cask utilized the following references as a means of evaluating the MSPB IRM operations (people, process and technology) against industry recognized best practices. These references can provide clarity and guidance of how to best align existing and proposed IRM operations. Cask has also provided a list of acronyms and their definitions used in this report in Appendix (E).

ANSI/BICSI 002-2011, *Data Center Design and Implementation Best Practices*
ANSI/BICSI TDMM, *Building Industry Consulting Service International Telecommunications Distribution Methods Manual (TDMM)*
ANSI/NFPA 70, *National Fire Protection Association standard for electrical code, i.e., the National Electrical Code (NEC)*
ANSI/TIA/EIA-568-C Set, *TIA commercial building cabling standard, defines a generic cabling system for a multiproduct, multivendor environment*
ANSI/TIA/EIA-569-B, *TIA commercial building standard for telecommunications pathways and spaces, defines the minimum requirements for both pathways for telecommunications cabling and spaces for telecommunications equipment*
ANSI/TIA/EIA-606-B, *TIA administrative standard for the telecommunications infrastructure of commercial buildings*
ANSI/TIA/EIA-607, *TIA grounding and bonding standard for commercial buildings*
ANSI/TIA/EIA-758, *TIA customer-owned outside plant standard*
ANSI/TIA/EIA-942, *Telecommunications Infrastructure Standard for Data Centers*
ASHRAE TC 9.9, *Mission Critical Facilities, Data Centers, Technology Spaces and Electronic Equipment – HVAC guidelines for mission critical facilities*
Commvault CommCell Disaster Recovery Guide
Control Objects for Information Technology 5.0
European e-Competence Framework v3.0
EIA/TIA TSB 72, *Centralized Optical Fiber Cabling Guidelines*
IBC 2012/09/06, *International Building Code, Seismic Guidelines*
ICT Professional Profiles e-CF version 3.0
Information Systems Audit and Control Association's Database Backup and Recovery Best Practices
Information Technology Infrastructure Library (ITIL) v3
Microsoft TechNet Library
NIST Special Publication 800-137 *Information Security Continuous Monitoring*
NIST Special Publication 800-34 *Contingency Planning Guide for Information Technology Systems*
OMB Circular A-130 *Management of Federal Information Resources*
Uptime Institute's Data Center Site Infrastructure, *Tier Standard: Topology*
VMware Knowledge Base

Organizational Skills Assessment

Technique and Findings

The organizational skills assessment used the e-Competence Framework v3.0. This framework establishes competencies across 23 roles found within IT organizations (Figure 2). This is further defined in Appendix (A). These roles cover the IT lifecycle from the inception of a capability, through operation, and retirement. It's important to note that a role does not necessarily equal one or more individuals. In small organizations, like MSPB, a single individual will fulfill multiple roles. Missing roles may mean that several critical tasks are not routinely completed. When critical tasks are not routinely completed, risks may linger in the IT operation that are only realized when the organization is under stress.

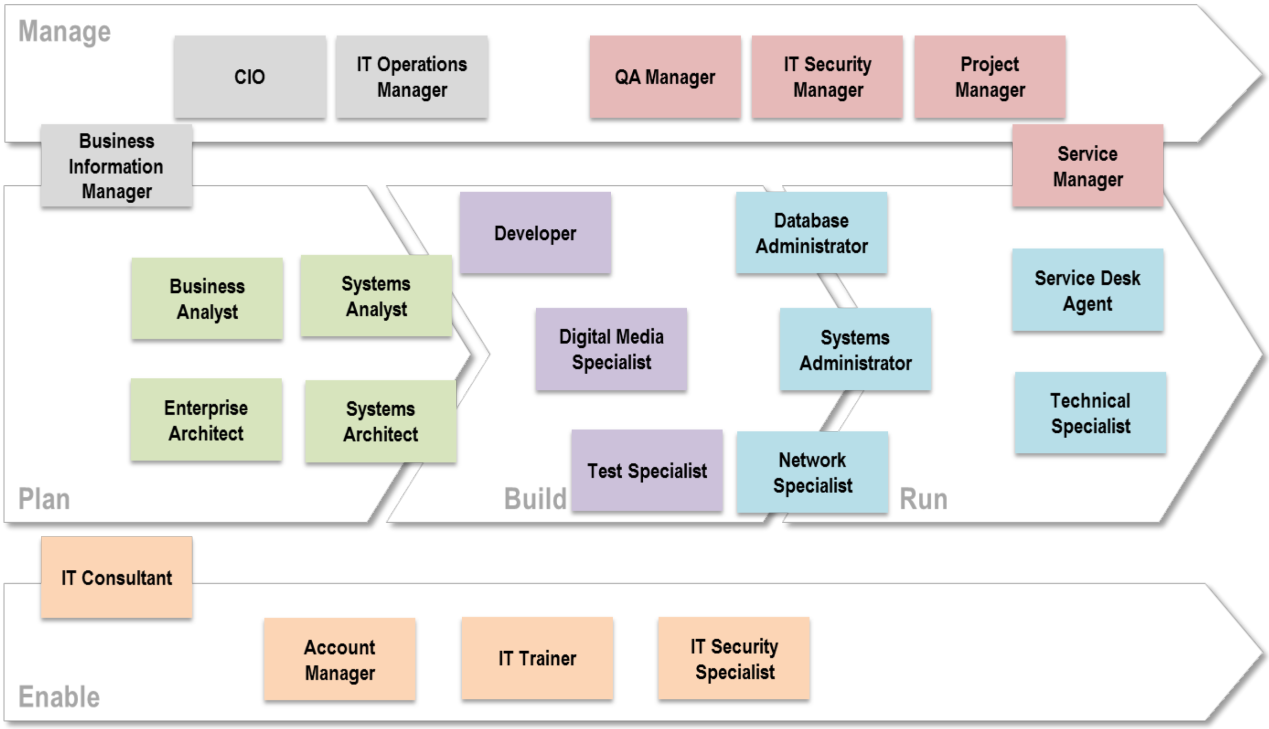


Figure 2: e-Competence Framework v3.0 Roles

The Cask team interviewed the MSPB IRM managers. Although our methodology was limited to the manager's self-reporting, we believe that it is predominately consistent found it viable. We wanted to identify the criticality of each role to the organization and then the manager's ratings of the organization's ability to perform each role. The ability to perform any particular role encompasses several items including commitment from the organization to perform each role, the availability of the competencies and skills required to perform each role and the availability of adequate resources to perform each role. Later we would ask each manager to rate the competence of their organization in performing each role. The following table is provided to clarify the difference between "Ability to Perform" and "Competence."

Term	Description
Ability to Perform	*Describes the preconditions that must exist in the project or organization to implement the software process competently. Ability to Perform involves resources, organizational structures, and training.*
Competence	*Ability to apply knowledge, skills and attitudes to achieve an observable result.*

We didn’t ask each manager directly to respond to a role. We have found that oftentimes a role can be variously defined and realized in different organizations and this can lead to miscommunication. However, the definition of each role includes between 4-8 specific tasks. So, we asked managers identify specific tasks associated with their group and to rate the criticality of these tasks on a scale of 1 (basic) to 5 (critical). They were also asked to rate the ability to perform the task on a scale of 1 (fails to meet our needs) to 5 (exceeds our needs). Then we calculated the mean for the tasks associated with particular roles to develop a single overall rating for each role (Figure 3).

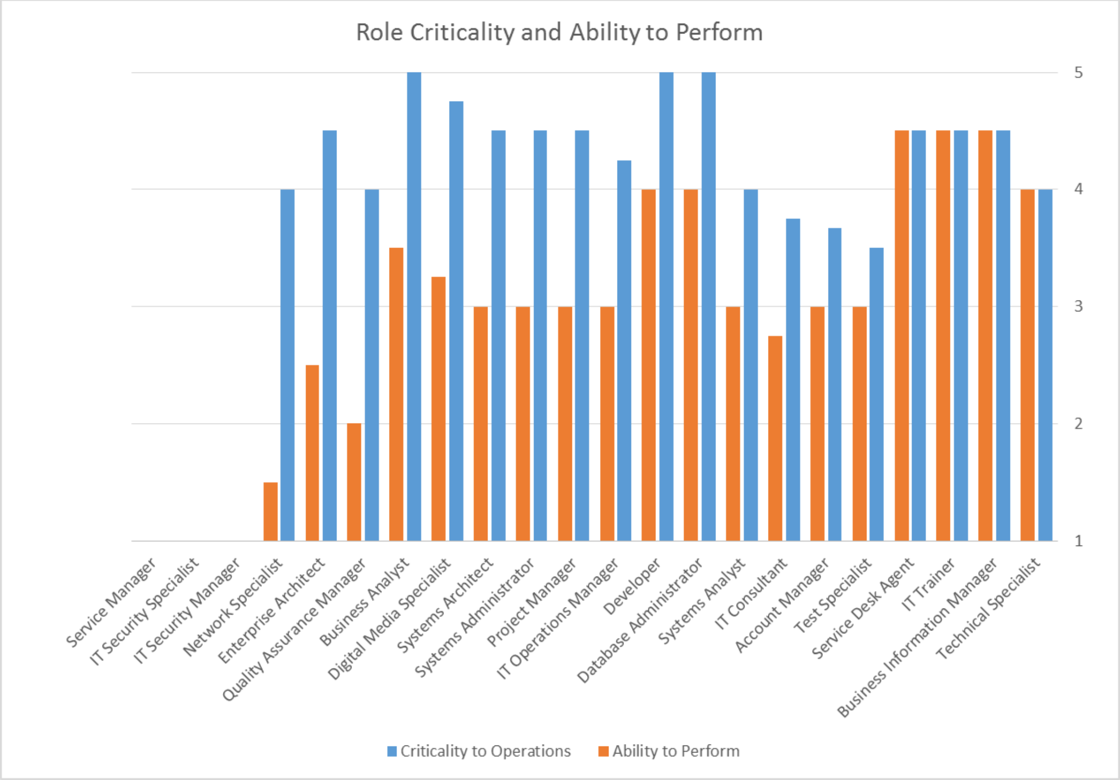


Figure 3: Role Criticality vs Ability to Perform

The roles in Figure 3 have been sorted to reflect the largest gap between criticality and ability to perform from left to right. There are two observations that we captured from these results. The first is that three roles were not identified by any of the IRM managers as being part of their responsibility. We understand that there is a formal assignment within IRM of an IT Security Manager and Specialist. However, within our methodology, the tasks associated with these roles were not identified as well as a third role:

Role	Description
Service Manager	*Plans, implements and manages solution provision*
IT Security Specialist	*Ensures the implementation of the organizations security policy*
IT Security Manager	*Manages the Information System security policy*

Secondly, our analysis shows that the following roles contain the biggest gap between criticality and ability to perform:

Role	Description
Network Specialist	*Ensures the alignment of the network, including telecommunication and/or computer infrastructure to meet the organization's communication needs*
Enterprise Architect	*Designs and maintains the Enterprise Architecture*
Quality Assurance Manager	*Guarantees that Information Systems are delivered according to organization policies (quality, risks, Service Level Agreement)*

The IRM managers rated two dimensions within each role – competencies and technical skills. We previously defined competency as "a demonstrated ability to apply knowledge, skills and attitudes for achieving observable results". Each manager was asked to rate each competency on a scale of 1 (fails to meet our needs) to 5 (exceeds our needs). Figure 4 depicts the results.

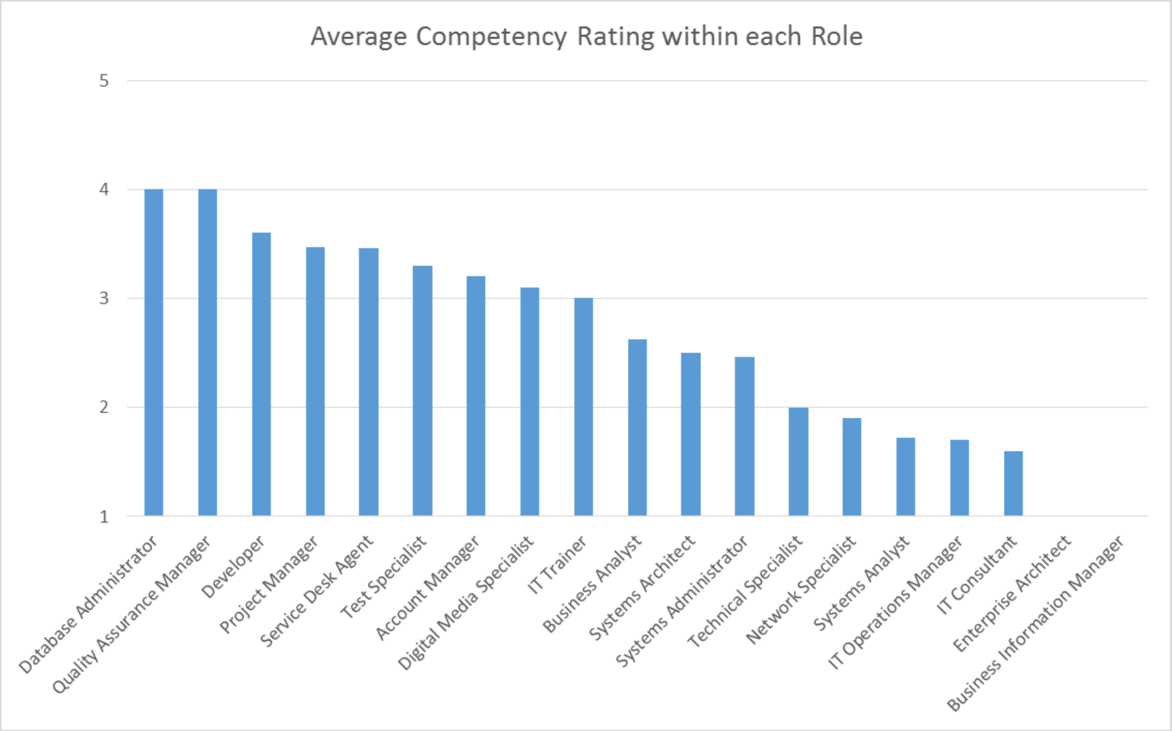


Figure 4: Average Competency Rating by Role

Our analysis shows that the following roles scored lowest:

Role	Description
Systems Analyst	*Analyses requirements and specifies software and systems.*
IT Consultant	*Supports understanding of how new IT technologies add value to a business.*
IT Operations Manager	*Manages operations, people and further resources for the IT activity.*
Network Specialist	*Ensures the alignment of the network, including telecommunication and/or computer infrastructure to meet the organization's communication needs.*

From the definition, you can see that skills are a component of a competency. For the purposes of this assessment, we collected data at the competency level for each role and additionally at the technical skill level for the roles to which those technical skills apply. The technical skills requirements were collected through analysis of the MSPB infrastructure. Each manager was asked to rate the each technical skill on a scale of 1 (fails to meet our needs) to 5 (exceeds our needs). Figure 5 depicts the results of these ratings.

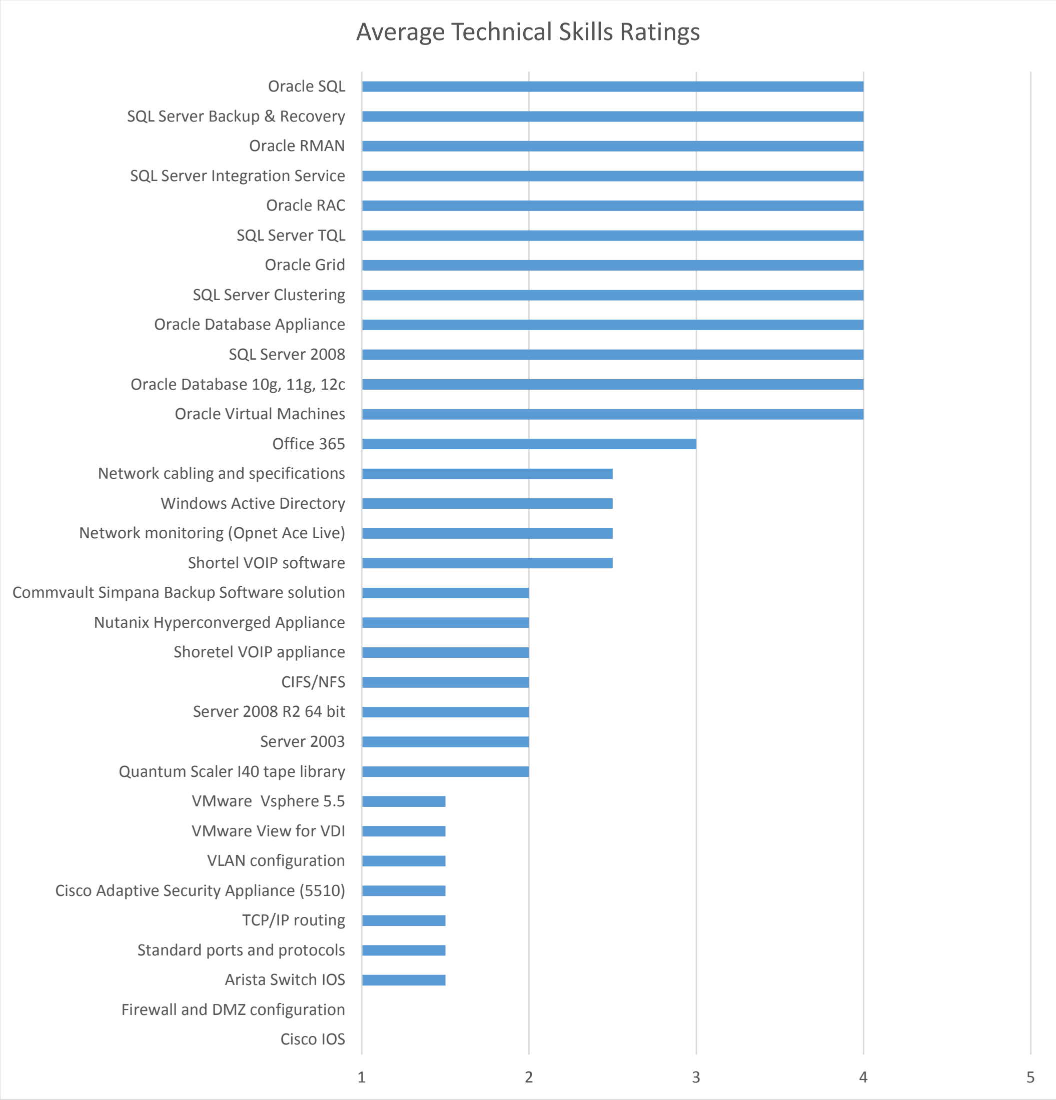


Figure 5: Technical Skill Ratings

An additional view of this data is provided in Figure 6. This view depicts the technical skills ratings for each role to which those technical skills apply. You can see that Network Specialist rated exceptionally low.

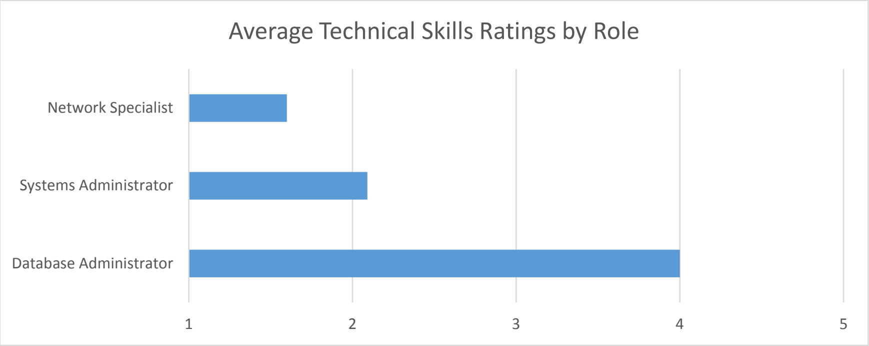


Figure 6: Average Technical Skill Ratings by Role

Summary of Organization Skills Assessment

We have identified three broad goals that IT organizations typically have:

Goal	Definition
Manage technology acquisition within organization in support of business objectives	This includes managing the process of translating business requirements into technical requirements as well as scoping, prioritizing, and managing resultant projects to achieve the technical requirements and enable the business objectives holistically across the enterprise.
Attain and maintain repeatable processes	This includes establishing and maintaining operational processes that can provide common and repeatable methodologies to reduce reliance on the availability of specific personnel.
Manage technology in accordance with best industry practices	This includes the use of tools and practices as recommended by Original Equipment Manufacturers (OEM) to provide technical management of IT infrastructure.

In our organizational skills analysis we identified various possible short comings within IRM. In the following summary, we group these findings into these IT goals:

Organizational Skills Finding Category	Goal		
	Manage Technology Acquisition within Organization ISO Business Objectives	Attain and Maintain Repeatable Processes	Manage Technology IAW Best Industry Practices
Missing Roles	*Service Manager*	*IT Security Manager*	*IT Security Specialist*
Gap Between Role Criticality and Ability	*Enterprise Architect*	*QA Manager*	*Network Specialist*
Low Competency Ratings	*IT Consultant* *Systems Analyst*	*IT Operations Manager*	*Network Specialist*
Low Technical Skills Rating			*Systems Administrator* *Network Specialist*

Process and Technology Assessment

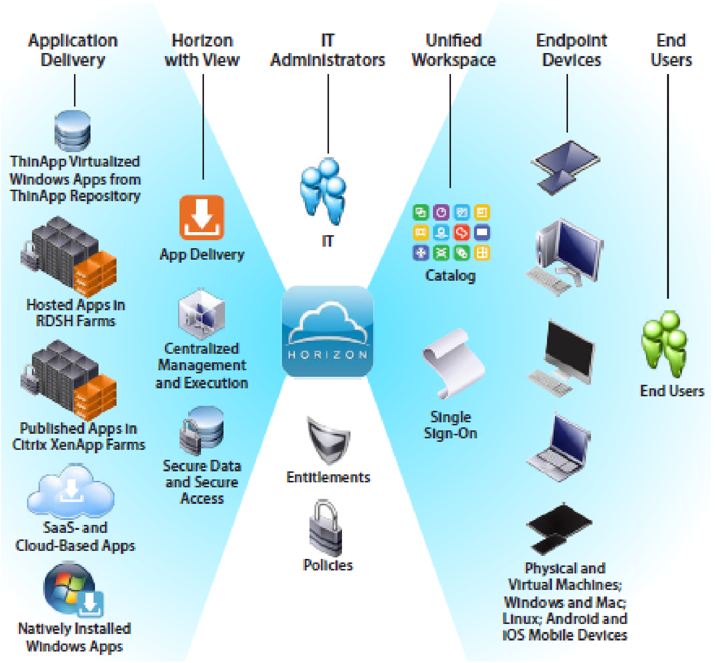
Manage Technology Acquisition within Organization ISO Business Objectives

Category:	Technology Acquisition	ID:	TA-1	Severity:	High
Observation: User Loss of Confidence in VDI					
Discussion: The VDI failure of 30 June 2015 has caused significant loss of trust and confidence in IRM that impedes moving forward with goals of e-Adjudication.					
Recommendation: Champion a communication plan which links the goals of e-Adjudication and IRM set within a schedule that emphasizes user roles and concerns within business goals.					

Category:	Technology Acquisition	ID:	TA-2	Severity:	High
Observation: User Experience with VDI					
Discussion: Users report that changes to the VDI are frequent and oftentimes not communicated adequately. This lack of useful communication through notifications, including newly added capabilities, creates user disorientation and inability to appropriately manage information assets.					
Recommendation: Establish a standard means to communicate information about VDI changes and capabilities with the users on the portal.					

<table>
<tr><th>Category:</th><th>Technology Acquisition</th><th>ID:</th><th>TA-3</th><th>Severity:</th><th>High</th></tr>
<tr><td colspan="6"><b><i>Observation:</i></b> VDI Adoption Hampered</td></tr>
<tr><td colspan="6"><b><i>Discussion:</i></b> Lack of VDI ability to support unique user tasks such as Kofax scanner (into DMS) and other client specialty software applications impedes enterprise adoption of VDI and loss of productivity. For example, the Office of Policy and Evaluation utilizes SAS and other data tools that are not currently available to them with VDI.

All three editions of Horizon 6 include View, one of the main platforms in Horizon 6 for delivering applications to users. VMware Horizon View offers several application delivery solutions such as ThinApp, App Volumes, and Cloud based applications such as Office 365. Native applications and support for USB and Scanners is also now available with Horizon 6. In addition to being able to delivery applications to end-users, you can also set policies in View to control who has access to the applications.


Application Delivery
Horizon with View
IT Administrators
Unified Workspace
Endpoint Devices
End Users
ThinApp Virtualized Windows Apps from ThinApp Repository
Hosted Apps in RDSH Farms
Published Apps in Citrix XenApp Farms
SaaS- and Cloud-Based Apps
Natively Installed Windows Apps
App Delivery
Centralized Management and Execution
Secure Data and Secure Access
IT
HORIZON
Entitlements
Policies
Catalog
Single Sign-On
Physical and Virtual Machines; Windows and Mac; Linux; Android and iOS Mobile Devices
End Users

</td></tr>
</table>

http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-workspace-application-delivery-options.pdf

Having multiple remote offices is one of the top use cases for a Virtual Desktop infrastructure, but in many cases a standard implementation of a virtual desktop isn't always enough. For MSPB to be able to take full advantage of the benefits of VDI, there must be some advanced designing to be performed. One of the key designs would be application delivery. This would allow MSPB to have greater benefits from their virtual desktop solution. Some key benefits are:

- Reduction in operational cost through better utilization of limited resources (smaller staff can manage more desktops)
- Increased security. All data resides in a single location and allows MSPB support staff to controlled organizational policies to ensure security compliance. This is especially important for remote users.
- Improved end-user experience. This user experience is key and why we suggest investing in VMware Professional Services.
- Improved Business Continuity and Disaster Recovery by protecting data locally and not being dependent on the end-user.

VMware Horizon View Use Case for Remote Offices:
http://www.vmware.com/files/pdf/customers/VMware-Telus-14Q1-Case-Study.pdf?src=WWW_customers_VMware-Telus-14Q1-Case-Study.pdf

Recommendation: Recommend MSPB to utilize VMware's Professional Services to provide a comprehensive architectural design and implementation of an application delivery solution that meets their needs.

<table>
<tr><th>Category:</th><th>Technology Acquisition</th><th>ID:</th><th>TA-4</th><th>Severity:</th><th>Low</th></tr>
<tr><td colspan="6"><b><i>Observation:</i></b> Help Desk Hours Insufficient</td></tr>
<tr><td colspan="6"><b><i>Discussion:</i></b> The IRM SLA sets the Help Desk hours as 0800 – 1700 EST. However, MSPB users are located across a number of time zones. IRM staff cell phone numbers are also published for emergency off-hours support. Users report that they experience productivity issues with insufficient hours of support. There also appears to be a trend that some users have gotten into the habit of bypassing the Help Desk and calling technicians directly. This is not best practice and reduces visibility across the enterprise.</td></tr>
<tr><td colspan="6"><b><i>Recommendation:</i></b> Consider committing additional resources toward extending the hours for the Help Desk.</td></tr>
</table>

<table>
<tr><th>Category:</th><th>Technology Acquisition</th><th>ID:</th><th>TA-5</th><th>Severity:</th><th>Medium</th></tr>
<tr><td colspan="6"><b><i>Observation:</i></b> Law Manager Functionality</td></tr>
<tr><td colspan="6"><b><i>Discussion:</i></b> Lack of transparency and auditing capability within Law Manager impairs compliance with recordkeeping requirements.</td></tr>
<tr><td colspan="6"><b><i>Recommendation:</i></b> This business capability should be included as a requirement for Law Manager. The technical requirements should be defined as a potential project and be included within the IT planning process to be prioritized and considered for funding.</td></tr>
</table>

<table>
<tr><th>Category:</th><th>Technology Acquisition</th><th>ID:</th><th>TA-6</th><th>Severity:</th><th>High</th></tr>
<tr><td colspan="6"><b><i>Observation:</i></b> User Data Storage Policy</td></tr>
<tr><td colspan="6"><b><i>Discussion:</i></b> User lack of understanding and confidence in the interim user storage policy and capability (particularly with VDI) reduces productivity.</td></tr>
<tr><td colspan="6"><b><i>Recommendation:</i></b> Press forward with establishing a secure and resilient data storage capability that can be communicated to users and restore confidence.</td></tr>
</table>

<table>
<tr><th>Category:</th><th>Technology Acquisition</th><th>ID:</th><th>TA-7</th><th>Severity:</th><th>Medium</th></tr>
<tr><td colspan="6"><b><i>Observation:</i></b> DMS Documentation</td></tr>
<tr><td colspan="6"><b><i>Discussion:</i></b> Lack of documentation on the DMS architecture impedes the ability to explore its full capability in supporting records and content management functionality.</td></tr>
<tr><td colspan="6"><b><i>Recommendation:</i></b> Work collaboratively with key records user community to identify priorities for establishing documentation.</td></tr>
</table>

Attain and Maintain Repeatable Processes

Network Processes

<table>
<tr><th>Category:</th><th>Network</th><th>ID:</th><th>N-1</th><th>Severity:</th><th>High</th></tr>
<tr><td colspan="6"><b><i>Observation:</i></b> Network Security Practices</td></tr>
<tr><td colspan="6"><b><i>Discussion:</i></b> Basic system and network security practices have not been implemented leaving the organization open to multiple vulnerabilities. MSPB has no safeguards in place to prevent an unauthorized user from plugging a random laptop or other device into the network. The “guest” Wi-Fi access point is actually tied into the MSPB Headquarters production network allowing anyone with the proper tools on their laptop to get an accurate map of all devices on the network, opening up the organization for further malicious intrusions. The password on the guest Wi-Fi is easily guessed and provides no security against a determined adversary.
Industry best practices recommend implementing port locking that will only allow a specific computer to connect to the network at a specified network drop. Guest Wi-Fi access should be connected to the Internet through the DMZ at a minimum. Passwords for guest Wi-Fi access should meet a minimum complexity utilizing upper and lower case letters, number, and special characters. The password should be changed on a regular basis as well.</td></tr>
<tr><td colspan="6"><b><i>Recommendation:</i></b> As the changes are made to the MSPB network, specifically the upgrade of the Cisco 6500 to the Arista switches, port locking should be implemented to prevent unauthorized network access. In addition, the guest Wi-Fi access should be hardened with a more secure password and the connection to the network relocated to the DMZ or directly to the Internet.
» http://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html
» https://www.uninett.no/webfm_send/730</td></tr>
</table>

<table>
<tr><th>Category:</th><th>Network</th><th>ID:</th><th>N-2</th><th>Severity:</th><th>High</th></tr>
<tr><td colspan="6"><b><i>Observation:</i></b> Vulnerability Scanning</td></tr>
<tr><td colspan="6"><b><i>Discussion:</i></b> Vulnerability scans are not routinely performed on the servers leaving systems with possible vulnerabilities that would be open to exploitation. New vulnerabilities are</td></tr>
</table>

discovered in operating systems and commercial off the shelf software daily. Running routine system scans with an updated tool allows the IT staff to address these vulnerabilities before they are exploited.

MSPB currently receives alerts from US-CERT concerning new vulnerabilities, but only takes action on those marked as critical. The scan utilities can be used to verify that all critical vulnerabilities are addressed and identify lower priority vulnerabilities. The organization can then make a fully informed decision on which vulnerabilities need to be addressed and which can be deferred.

Recommendation: MSPB should renew the subscription for the Nessus scan software and implement procedures to ensure regular scanning of all systems.

Category:	**Network**	**ID:**	**N-3**	**Severity:**	**High**

Observation: Administrator Password Policy

Discussion: (b) (5), (b) (7)(E) [redacted]

[redacted]

[redacted]

[redacted]

Recommendation: (b) (5) [redacted]

IT Service Management Processes

Category:	Service Management	ID:	SM-1	Severity:	High

Observation: ITSM Process Implementation

Discussion: Core IT Service Management processes are not in place to manage the technology stack. The following core set of processes as defined by ITIL are critical to management of the technology stack (the technology stack comprises the layers of components or services that are used to provide a software solution or application):

- Configuration Management (CM) comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.
- Change Management helps organizations understand and work to minimize risks of changes to the IT environment. It is essentially a process for managing the people-side of change.
- Release Management encompasses the planning, design, build, configuration and testing of hardware and software releases to create a defined set of release components.

Recommendation: To reduce risk, recommend developing processes based off ITSM/ITIL. Processes documentation and training available at link below.

- https://www.axelos.com/best-practice-solutions/itil/what-is-itil
- http://www.best-management-practice.com/gempdf/itsmf_an_introductory_overview_of_itil_v3.pdf

Category:	Service Management	ID:	SM-2	Severity:	High

Observation: Continuity Planning

Discussion: The MSPB Continuity Plan (CP) is not up to date and is lacking in critical information. Continuity plans provide a coordinated strategy to identify technical procedures and methods that will prevent most service disruptions and enable quick recovery should any disruptions occur. Having no continuity plan or an outdated plan exposes the organization to the risk that it will not be able to recover its systems and operations in a timely manner after any kind of failure, not only disaster situations. Note that a business continuity plan contains the disaster recovery plan as well as containing contingency procedures that cover less severe levels of outages.

A continuity plan allows organizations to have an organized and consistent response to any kind of service disruption. The heart of any continuity plan is the organization's detailed network, system, and application documentation. Management should keep in mind that continuity plans should include sufficient detail to allow IT professionals that are not familiar with the organization's system to be able to restore service or rebuild the IT environment if necessary.

- Examples of details that are necessary would be configuration information for each server, minimum hardware and software requirements for the applications, ports and protocols used for communication, etc. If this information is already documented in sufficient detail elsewhere, then references to those documents should be included.
- Each organization has to determine their requirements for time of recovery in the event of a disaster/system failure and tailor its continuity plan accordingly. It was discovered during the interviews that MSPB does not have any Recovery Point Objectives (RPO)

or Recovery Time Objectives (RTO) established for is systems. Those objectives are an important part of the continuity plan since they set priorities for recovery.

- Industry best practices call for continuity plans to be tested annually. In the case of organizations that have a critical mission, the continuity plans should be tested more frequently. Each test should be documented and evaluated to identify lessons learned with the continuity plan being updated with those lessons. A continuity plan is a living document that must be kept up to date as an organization's systems change or new IT systems are added.

Continuity planning generally includes one or more of the following approaches to restore disrupted services:

- Restoring information systems using alternate equipment.
- Performing some or all of the affected business processes using alternate processing (manual) means.
- Recovering information systems operations at an alternate location.
- Implementing of appropriate continuity planning controls based on the information system’s security impact level.

Recommendation: Because of the changes that MSPB has in process and in planning, it is recommended that the IT systems that are the highest priority to the function of the organization be identified and a detailed continuity plan be created for those systems.

- This will help protect MSPB in the short term without utilizing a great deal of staff resources in the creation of the plan. As the changes and upgrades are made to the MSPB system, the continuity plans for the essential systems can be combined and expanded to eventually become the master continuity plan for the entire IT system.
- It is also recommended that there be two members of the IT staff, a primary and a backup, designated to keep the continuity plan up to date. The continuity plan and other system documentation should be stored in a centralized repository with copies kept off site.

Suggest updating continuity plan in accordance to NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

- http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
- http://www.forbes.com/sites/sungardas/2014/11/19/business-continuity-and-disaster-recovery-best-practices-from-the-availability-trenches/
- http://tabbforum.com/opinions/6-disaster-recovery-best-practices-as-defined-by-regulators
- http://www.zetta.net/blog/practices-building-disaster-recovery-plan/

Category:	Service Management	ID:	SM-3	Severity:	High

Observation: Technical Baseline

Discussion: No technical baseline is in place. The technical baseline is an agreed-to description of the attributes of a product, at a point in time, which serves as a basis for defining change. Without an accurate baseline, risk and issues pertaining to reliability, supportability, and maintainability increase. Most of the systems/applications have outdated documentation if any documentation exists at all.

This issue could be considered a continuation of the continuity plan discussion. Industry best practices call for having highly detailed documentation on the technical base-lines of all systems. This includes physical servers, virtual servers, database appliances, network appliances, network switches and routers. Two immediate advantages to having a technical baseline available are: having the baseline makes troubleshooting network and systems issues easier, and the baseline also makes it easier to identify systems that need to have security flaws corrected.

As changes are made to any of the systems or the network, the baseline configuration documentation must be updated. It is a common shortcoming in many organizations to allow documentation to become outdated, often because there is little priority placed on documenting changes and most IT shops have a heavy workload.

When everything is running well there are no consequences to that practice. When a systems failure or disaster situation occurs, the organizations in that situation find themselves unable to recover their systems in the desired time frame. In the case of older systems that were set up by vendors that are no longer available it can be almost impossible to recover.

Recommendation: MSPB has plans for performing upgrades to their network and systems as well as possibly migrating to a different data center. It is recommended that as the upgrades and migration are done, each system be examined carefully and documentation created or updated. This documentation should then be stored in the central configuration management repository.

Additionally, for each document an "owner" should be identified who will be responsible for maintaining the document. A process should be put in place that emphasizes maintaining the documentation any time changes are made to the systems. In this context, "systems" refers to servers (virtual and physical), applications, databases, database appliances, network appliances, network cabling, network switches, and routers.

Category:	**Service Management**	**ID:**	**SM-4**	**Severity:**	**Medium**

Observation: CM Documentation Storage

Discussion: There is no centralized storage location for the configuration management documentation. This can lead to time wasted searching to find the technical documentation needed to correct a system failure or, worse, having a technician use an outdated version of the configuration documents that result in a system being misconfigured.

Configuration documentation for the applications, servers, databases, and network is essential for understanding how the applications function, understanding how they are inter-connected with and affect other systems and applications, prevention of vulnerabilities due to security flaws, and timely recovery of the systems and network.

- This documentation should be stored in a centralized repository. This repository could be one of the commercially available configuration management utilities or simply a designated location on the network.
- To provide redundancy, there should also be copies of all the documentation stored off site. This permits the documentation to be available should it be necessary to recover from a disaster when the primary office is not available.

» All IT staff should know the location of these documents, however there should be a limited number of people that have the rights to make changes to the documents.
Recommendation: It is recommended that MSPB designate an on-site and an off-site storage location for all of the configuration documents. A primary and backup staff member should be identified that will be the owner of the documents. These individuals would be responsible for saving updated copies of the documentation to the centralized storage locations. They would not necessarily be the ones responsible for making the updates to the documentation.

Category:	**Service Management**	**ID:**	**SM-5**	**Severity:**	**Medium**
Observation: Help Desk Incident Processing					
Discussion: Users report a significant disparity with satisfaction of ticket processing. If the issue is of a fairly routine nature the general consensus is that the tickets are promptly addressed, communicated to the user and closed. It is likely that these are tickets being handled by Tier I support. However, for more complex incidents that are probably being routed to Tier II support the users repeatedly report a lack of visibility into the status of their incident, slow response times, and a lack of communication. The Service Level Agreement (SLA) that IRM has established and disseminated to MSPB Employees is a good working document and communicates expectations well. However, the Incident Management process within the Help Desk is not functioning to uniformly achieve these SLA.					
Recommendation: Recommend establishing an Incident Management process for the Help Desk based off ITSM/ITIL. Processes documentation and training available at link below. » https://www.axelos.com/best-practice-solutions/itil/what-is-itil » http://www.best-management-practice.com/gempdf/itsmf_an_introductory_overview_of_itil_v3.pdf					

Category:	**Service Management**	**ID:**	**SM-6**	**Severity:**	**Medium**
Observation: VDI Recovery Hampered					
Discussion: The VDI recovery from the failure of 30 June 2015 has been hampered by a lack of VDI configuration documentation and back-up outside of virtual infrastructure. This impedes moving forward with goals of e-Adjudication and impairs user experience and productivity. Recovery actions are ongoing.					
Recommendation: Document and back-up VDI configuration IAW best practices as well as address user concerns in the communication plan.					

Manage Technology IAW Best Industry Practices

Data Protection

Category:	**Data Protection**	**ID:**	**DP-1**	**Severity:**	**High**
Observation: Disaster Recovery Planning					
Discussion: The disaster recovery plan should be specific processes to CommServe disaster recovery, which is a set of procedures that are used to prepare for and recover from a CommServe disaster. This Disaster recovery plan should not take the place of the Continuity plan but be a part.					
Recommendation: Recommend creating a Disaster recovery plan or adding to Continuity plan by following CommServe Disaster Recovery Solution.					

- » http://docs.commvault.com/commvault/v10/article?p=features/disaster_recovery/c_cs_dr_overview.htm

Category:	Data Protection	ID:	DP-2	Severity:	Low

Observation: Commvault_Disk E:\ low on space

Discussion: There is only 1.9gb of disk space remaining. High disk utilization may cause failed backups, poor drive performance and data corruption. However, (b) (6) reports that this disk is on an unused HP storage unit that is scheduled to be disconnected and retired.

Recommendation: Recommend retirement if it is no longer in service. Otherwise, expand the drive or clearing unnecessary files from drive if it is to remain in service as best practice is to keep drives to a maximum of 80% capacity.

Category:	Data Protection	ID:	DP-3	Severity:	High

Observation: Host System Backup (b)(7)

Discussion: This applies to

Server Name	Service
(b) (7)(E)	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

These systems are either not on the Commvault backup schedule or do not have any backup agents installed on the system. Possibly some applications do their own backup (Oracle RMAN, SQL), or per your recovery strategy, they may not need to be backed up.

Recommendation: Recommend reviewing host systems to identify backup requirements are being met.

Category:	**Data Protection**	**ID:**	**DP-4**	**Severity:**	**High**

Observation: Data Backup Testing

Discussion: MSPB's policy is that the restoration data from backups shall be tested twice a year. Currently no testing of the ability to recover from backups is being performed. During the interview process it was discovered that no full system or database restorations have been performed. With most applications the database is the heart of the application. Without the data stored in the database, the application is of little to no use to an organization. Because of this it is essential to protect the database and the data. One part of this protection is regular database backups. Having the backups is only the first step, however. Those backups must be tested to verify that they can be used to restore the database as well.

- Database failures typically occur in one of two categories: data corruption and drive media failure. MSPB's Oracle databases are configured in archive log mode to allow hot backups by the Commvault software. This use of archive logs also allows for recovery of the database in the event of data corruption provided the point in time of the data corruption can be reliably determined. Archive logs are a proven method for point in time recovery of the database, though Oracle does have a recommended configuration for the log files. Verifying that configuration was not part of the evaluation performed by Cask.
- The hot backups performed by Commvault are a mitigation against media failure provided the backups are good. There has been no test of the backups which leaves MSPB vulnerable since there is no level of confidence that recovery from media failure is possible.
- The staff DBA also routinely performs database exports using the provided Oracle utilities. This technology is also proven and does provide a method for recovery from media failure provided the export files are maintained in a separate location where they would not also be lost in the event of media failure.
- Backups for the application servers are being performed, but have not been tested. These backups should be regularly be tested as well since any server can be restored much faster than it can be rebuilt. Performing a full system restore also eliminates the possibility that when a server is rebuilt it may not be configured correctly.
- MSPB has successfully tested that individual files can be restored from the backup solution.

Recommendation: Recommend performing recovery testing in accordance to MSPB's policy. There is sufficient hardware available to allow the creation of an environment for the purpose of testing these backups.

- Backups of the servers should also be tested to verify that they can be restored successfully.
- Detailed instructions for the backups and restores should be included in the organization's Continuity plan. This will allow a timely recovery of the systems and database under any circumstances.
- http://www.practicepro.ca/Technology/pdf/Backup-Best-Practices-and-Strategies.pdf
- http://www.isaca.org/Journal/archives/2012/Volume-1/Pages/Database-Backup-and-Recovery-Best-Practices.aspx

Category:	**Data Protection**	**ID:**	**DP-5**	**Severity:**	**Medium**
Observation: System State Errors					
Discussion: Errors in backing up system state on the following serves. (b) (7)(E), (b) (7)(E), and (b) (7)(E). System State backup creates a backup file for critical system related components. This backup file can be used to recover critical system components in case of a crash.					
Recommendation: Recommend reviewing Commvault logs and server logs to identify and resolve backup issues and ensure successful recovery.					

Category:	**Data Protection**	**ID:**	**DP-6**	**Severity:**	**Medium**
Observation: Commvault License					
Discussion: The MSPB Commvault is licensed for 5 Terabytes. System utilizing 10.3 Terabytes. In August, a change to the primary and secondary copies from 4 days 2 cycles to a 14 day and 1 cycle retention increased the amount of data retained on disk.					
Recommendation: Expand the license to meet your capacity requirements or reduce the amount of data retained on disk.					

Category:	**Data Protection**	**ID:**	**DP-7**	**Severity:**	**High**
Observation: Backup SOP					
Discussion: No Standard Operating Procedures (SOP) are established for monitoring and administering Backup solution. Without SOP's, MSPB risks ensuring proper backup and recovery capabilities.					
Recommendation: Recommend documenting Standard Operating Procedures for Daily, Weekly and Monthly activities.					

Category:	**Data Protection**	**ID:**	**DP-8**	**Severity:**	**Low**
Observation: Commvault Deduplication					
Discussion: Deduplication provides an efficient method to transmit and store data by identifying and eliminating duplicate blocks of data during backups. All data types from Windows, Linux, UNIX operating systems and multiple platforms can be deduplicated when data is copied to secondary storage.					
Recommendation: Recommend enabling deduplication to optimize use of storage media by eliminating duplicate blocks of data and reducing network traffic by sending only unique data during backup operations. » http://documentation.commvault.com/hds/release_8_0_0/books_online_1/english_us/features/single_instance/single_instance_how_to.htm					

Infrastructure

Category:	**Infrastructure**	**ID:**	**I-1**	**Severity:**	**High**
Observation: No Anti-Virus (b) (7)(E)					
Discussion: There is out of date or no Anti-Virus installed on (b) (7)(E) ystems					

Server Name	Servic
(b) (7)(E)	(b) (7)(E)
[redacted]	[redacted]
[redacted]	[redacted]

(b) (7)(E)	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Antivirus software is one of the most important tools for safe-guarding systems information from malicious viruses and worms. Without antivirus protection, your systems may be left unsecure.

Recommendation: Ensure systems have Anti-Virus installed with the latest definition.

Category:	Infrastructure	ID:	I-2	Severity:	High

Observation: Unsupported Windows 2003

Discussion: There are (b) (7)(E) ervers running unsupported Windows 2003 32-bit Operating System. This applies to:

Server Name	Service
(b)	[redacted]
(7)(E)	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

The Windows 2003 32-bit Operating system Extended Support End Date was 7/14/2015. Continuing to use Windows 2003 increases the risk of security vulnerabilities as well as lack of support.

Recommendation: Recommend updating these systems to the latest Server Operating System.

Category:	Infrastructure	ID:	I-3	Severity:	High

Observation: Unsupported Servers

Discussion: There are (b)(7)(E) Physical servers running on unsupported hardware.

Hardware Make	Server Name	Service
(b) (7)(E)	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	(b) (7)(E)
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

End of Support has been reached for HP ProLiant DL360 and DL380 (G5 and below). The biggest risks of running end of service equipment are lack of support, scalability, and reliability. With no support available from the Vendor in the event of hardware failure, parts may not be available. Additionally, end of service life hardware may not be able to handle more load when upgrading other portions of the infrastructure.

Recommendation: Recommend upgrading hardware or converting to virtual machines.

Category:	Infrastructure	ID:	I-4	Severity:	High

Observation: Java Ou[redacted]f Date

Discussion: There ar (b)(7)(E) servers Java(TM) and Java(TM) SE Development Kit out of date. This applies to

Server Name	Service
(b)(7)(E)	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Java needs frequent maintenance with security patches needing to be rolled out regularly. Java is one of the top security vulnerabilities.

Recommendation: Recommend updating Java on all systems.

Category:	Infrastructure	ID:	I-5	Severity:	Medium

Observation: Test/Dev Mirroring Prod

Discussion: The existing Test/Dev environments do not mirror the configuration of the production environment. Without a mirrored test environment, it is not possible to fully test the impact of patches and upgrades except on production which is a major risk.

Having an environment that is essentially a mirror of the production environment that can be used for the testing of patches and upgrades is highly recommended as an industry best practice. Developers very rarely have the systems they use for developing code changes configured to match the production environment and never are able to fully reproduce the interactions that occur on the production systems/network. Because of this it is essential to have a test environment that is configured as closely as possible to match the production environment as possible.

- In that environment thorough testing can be done to ensure that patches and upgrades work properly. This also prevents issues with bad code changes from possibly affecting the production system causing unplanned outages.
- MSPB has test servers for some of their critical applications. However, these environments are connected to the production network and it is not known if the systems are configured to match the production servers. In the case of operating system security patches, these are applied directly to the production systems without having any testing done at all. Considering that there are multiple versions of .Net running on the MSPB systems, this practice presents a serious risk of an outage caused by a security update.

Recommendation: Discussions with the MSPB IT staff indicated that hardware is already available for implementing a test environment. It is recommended that dedicated test environments, completely separate from the production network, be created as soon as possible for the critical MSPB applications. This will provide a starting point for creating a full test environment as MSPB moves forward with the planned data center changes.

Category:	Infrastructure	ID:	I-6	Severity:	Medium

Observation: Developer Segregation

Discussion: Segregation/separation of duties and environments does not exist in the MSPB environment. This presents a risk that developers will make changes directly in the production environment that are not properly tested and documented resulting in outdated configuration management documents in the best case, and system outages as a worst case. Segregation/separation of test and production environments has been discussed previously. Industry best practices call for separation of staff member's duties as well.

» The biggest threat to any organization's network and systems is from an inside threat. In many cases there is no malice intended, but inadvertent changes can cause system failures and un-planned outages just as serious as deliberate attacks. Developers should not be granted privileged access to the production systems that would allow them to make configuration changes to the servers or deploy any code changes themselves.

» The best process for ensuring separation of duties is to have the developers create changes on their development systems, install the changes on a separate test system and conduct thorough testing while documenting the changes made and installation process for the code changes.

» The new code and installation documentation is then turned over to the production administrative staff for deployment to the production servers. The production administrators would then work with the developers to update the system configuration documents in the central storage repository.

Recommendation: It is recommended that MSPB implement a process to ensure separation of duties. This increases security, reduces the risk of system down time, and ties in with the change and configuration management processes since it ensures creation of the proper installation documents and the updating of system configuration documents. The websites below provide additional details and best practices concerning separation of duties:

» http://www.sans.edu/research/security-laboratory/article/it-separation-duties

» http://www.giac.org/paper/gsec/261/segregating-technology-personnel/100853

» http://demo.protocolpolicy.com/ISO27002index.html#12.1.4

Category:	Infrastructure	ID:	I-7	Severity:	Low

Observation: High UPS Utilization

Discussion: 9 APC UPS running at 75% or higher utilization.

Recommendation: Informational only at this time. When consolidation of rack begin, this may be a concern. Verify power availability prior to migration.

Virtualization

Category:	Virtualization	ID:	V-1	Severity:	Medium

Observation: Dual Path vNICs

Discussion: Not all vNICs on Virtual Machines are dual pathed. Lack of dual path vNICs present risks with no failover path available.

Recommendation: Recommend reviewing and modifying all vNICs to ensure they are dual pathed for high availability.

Category:	**Virtualization**	**ID:**	**V-2**	**Severity:**	**Medium**

Observation: VM Symantec Endpoint

Discussion: Symantec Endpoint software is supposed to be installed on all servers, but there is no baseline template in use for the virtual servers so they may or may not have the anti-virus software installed. A base virtual server template with all required software already installed is not used for creating Virtual Machines. Combined with the lack of documented server baselines, this results in servers that are missing essential security software such as Symantec anti-virus. The use of a partially pre-hardened base template allows for a consistent starting point when deploying new servers as well as saving time for the IT staff since much of the hardening only has to be performed one time. This builds on the configuration management process. Since each server's base configuration is known from the start, so it is only necessary to document customizations to each server.

Recommendation: It is recommended that MSPB create a base template for VM's prior to any architecture changes. This will tie in with the creation of the configuration management process, save time on future deployments, and ensure that the base protection software and settings are already configured.

Category:	**Virtualization**	**ID:**	**V-3**	**Severity:**	**Low**

Observation: VMware Tools

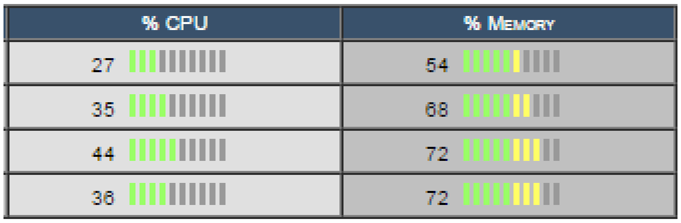
Discussion: VMware Tools on Several VMware guest operating system either not running or not installed. VMware Tools is a suite of utilities that enhances the performance of the virtual machines guest operating system and improves management of the virtual machine. Without VMware Tools installed in your guest operating system, guest performance lacks important functionality.

Recommendation: Ensure VMware tools are installed, updated and running on all VMware Guest Operating Systems.

Category:	**Virtualization**	**ID:**	**V-4**	**Severity:**	**Low**

Observation: VDI Infrastructure Memory Utilization

Discussion: There is High Memory utilization on VDI host (b)(7) and (b)(7). This may cause performance issues during boot storms or Scans/Patching.



% CPU	% Memory
27	54
35	68
44	72
36	72

Recommendation: Informational only at this time. System is running high but no ballooning is occurring. Recommend continuous monitoring.

Category:	**Virtualization**	**ID:**	**V-5**	**Severity:**	**Low**
Observation: VDI Host Overcommit Ratio					
Discussion: There is a 7.25 Overcommit ratio on VDI Host. This is a good ratio for Medium users. Heavy user overcommit ratio is roughly 3.75. A good, conservative starting point in the design is 6 vCPUs per pCPU when calculating density.					
Recommendation: Informational only at this time. If performance becomes an issues with VDI, recommend reviewing VMware's Server sizing guide for VDI. » http://www.vmware.com/files/pdf/view/Server-Storage-Sizing-Guide-Windows-7-TN.pdf					

Category:	**Virtualization**	**ID:**	**V-6**	**Severity:**	**Low**
Observation: VM Hardware Discrepancies					
Discussion: VM hardware discrepancies on infrastructure VMware Guest Operating systems. Virtual hardware versions introduce new functionality, extend limits and may have performance implications. Virtual Machine hardware discrepancies may have been brought on by performing P2V migration of systems.					
Recommendation: Recommend reviewing virtual hardware settings on each Virtual Machine and removing any unnecessary hardware and updating systems. Recommend following VMware's Knowledge base regarding Upgrading a virtual machine to the latest hardware version (multiple versions) (1010675). » http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1010675					

Category:	**Virtualization**	**ID:**	**V-7**	**Severity:**	**Low**
Observation: VMware Licensing					
Discussion: The VCenter is being shared between VDI infrastructure and Virtual Server Infrastructure. VCenter/VSphere should have a separate infrastructure for View environment. This is a licensing issue. Even though the two Nutanix appliances are clustered, under the VMware EULA, you are not licensed to fail-over the VSphere Infrastructure to the View infrastructure.					
Recommendation: Recommend contacting VMware to discuss license requirements.					

Network

Category:	**Network**	**ID:**	**N-4**	**Severity:**	**High**
Observation: Network Monitoring					
Discussion: MSPB has a number of network and system monitoring tools available, but they are not being used in a regular and proactive manner. Some of these tools are: • OpNet Ace Live/SteelCentral • Stratusphere • NetIQ • Spotlight • Oracle Grid/Enterprise Manager » Each of these tools allow comprehensive monitoring of the network, servers, or databases, providing information that could be used to improve system and network					

performance as well as prevent issues. Other tools had been in use previously, but the licenses were not renewed.

- Industry best practice calls for utilizing network monitoring tools to establish a performance baseline that will allow IT staff to identify trends over time requiring expansion of network capabilities and quickly identify when problems are occurring on the network. This baselining should be done to a granular level (tracking the amount of traffic on each segment, the processor utilization on servers and appliances, and even the temperature of the processors in the network switches) in order to allow IT staff members to identify at a glance when any component is out of normal range. Caution should be used to ensure that too much data is not collected since this can mask problems because the amount of data is overwhelming.
- In some cases the same tools that monitor the network can monitor the health of the servers, applications, databases, and services, a practice that is also recommended. Many of the tools include the means to automatically send alerts to the IT staff any time issues are detected. The monitoring can be finely tuned to screen out false positives to prevent adding unnecessary administrative overhead to the staff.
- During the assessment, the Stratusphere tool was deployed and used to gather configuration information on the servers. MSPB staff has been using Quest Foglight to monitor the databases. However, that product does not offer the same range of functionality as Oracle Enterprise Manager.

Recommendation: It is recommended that MSPB leverage the tools that are available and implement processes that will result in proactive monitoring of the network and systems rather than reactive monitoring. This would be something that could be presented to the user community as an indication that the IT staff is listening to their concerns about system and network performance. Enabling the out of the box system alerts will provide a basic level of automated alerts that can be fine-tuned over time.

- If MSPB intends to migrate to a hosted data center, it is recommended that one of the items provided by the host facility be automatic monitoring of the network and systems.
- Additional information on network and system monitoring best practices can be found at the websites below. The references to specific monitoring applications can be ignored since MSPB already owns excellent monitoring tools:
- http://www.solarwinds.com/network-monitoring-best-practices.aspx
- https://www.sqa.its.state.nc.us/library/pdf/HP%20Performance%20Monitoring%20Best%20Practices.pdf

Category:	**Network**	**ID:**	**N-5**	**Severity:**	**Medium**

Observation: Network Cabling Standards

Discussion: The network cabling in the server room is not done to industry standard. Cables are lacking in labels, not run neatly, separated in bundles for each rack, etc. Substandard cabling increases the time it takes to troubleshoot network faults and can cause faults due to the poor cable routing.

Industry best practices call for network cabling to be run neatly either in over-head trays or under a raised floor to allow easy tracing of cables and access to equipment. MSPB currently uses overhead trays for the cables in the data center, however the cabling configurations at the patch panels and server racks is not up to standard. Much of the MSPB cabling in the data center is cluttered and interferes with access to the patch panels and servers in the racks.

- Cables going from the main patch panel to each server rack should be organized into separate bundles with one bundle per rack. Network cables should not be run parallel with any power cables. Where power cables must be crossed, the recommended practice is for the network and power cables to cross at right angles.
- At no time should network cables be run along to floor or dangle down to floor level. Cables in this configuration present a tripping hazard to personnel as well as opening the possibility that cables could be inadvertently pulled out of the servers or patch panels and/or damaged.
- On the server racks, the cables should be run and organized in such a manner as to allow easy access to the equipment, both front and back. This includes providing sufficient length of the cable to allow the servers to be slid out of the racks for servicing without disconnecting any cables. In all cases, cables should be kept to the minimum necessary length. The use of switches on each rack is encouraged where network traffic permits. This allows for fewer cables to be run between the racks and the patch panels.

Recommendation: As MSPB implements the changes to the data center architecture and infrastructure, the cabling for each rack should be cleaned up to meet industry best practices. The patch panel cabling should be cleaned up during the migration from the Cisco 6500 to the Arista switches.

- https://www.brocade.com/content/dam/common/documents/content-types/product-design-guide/cabling-best-practices-ga-bp-036-02.pdf
- http://www.techrepublic.com/blog/10-things/10-cabling-tips-to-keep-your-data-center-manageable/
- http://www.datacenterknowledge.com/archives/2013/10/09/cable-pathways-a-data-center-design-guide-and-best-practices/

Data Center

Category:	**Data Center**	**ID:**	**DC-1**	**Severity:**	**High**

Observation: Data Center Infrastructure Risks

Discussion: The data center infrastructure has significant limitations, which collectively may pose unacceptable risks to consistently meet the goals of e-Adjudication without mission limiting planned and unplanned outages. The following specific observations apply:

- Lack of redundant and backup electrical service in the Data Center makes the IT susceptible for extended (days) outages. This would be very costly and difficult to implement; particularly in a commercial (vice government owned) building.
- Inefficient cooling methodology increases management burden and offsite monitoring requirements to ensure sufficient cooling is available for Data Center. It is possible to realign this capability with some moderate investment.
- Wet pipe sprinkler system increases risk of catastrophic IT loss in case of fire in the Data Center. It is possible to mitigate this with a moderate investment.
- Lack of cooling and ventilation in the mechanical room containing the electrical transformers powering the data center create an environment where the ambient temperature exceeds IEEE recommendations. Sustained temperatures greater than 86

deg F which may cause reduction in life cycle and loss of data center power. This can be mitigated with a small capital investment.

This building was not designed to house a data center. A rough order of magnitude (ROM) cost estimate for the non-electrical mitigations is about $300K. Since getting a second (independent) power service into the building would be very challenging, the introduction of a backup power source (diesel or natural gas generator) would be the most logical means to prevent electrical outages. This would have to be supported by the building owner and involve permitting process with the City. A ROM for this project to include some best practice transfer switching, electrical conditioning and panel upgrades is about $1M and is expected to take at least a year to achieve.

Recommendation: The President's Federal Data Center Consolidation Initiative (FDDCI) has goals to close approximately 800 data centers much like this one. Recommend that MSPB seek to migrate their technology to either a public or private data center that is certified to meet their requisite physical and network security requirements.

Category:	**Data Center**	**ID:**	**DC-2**	**Severity:**	**Medium**

Observation: Data Center Configuration Risks

Discussion: Observation "Data Center Infrastructure Risks" highlighted capital data center infrastructure limitations. This observation highlights other risks present in the data center which also pose risks to meet the goals of e-Adjudication. However, they are more so associated with housekeeping and can be mitigated with labor and little funding. The following specific observations apply:

- Presence of extraneous equipment and cardboard boxes in Data Center increases fire risk and increases wear and tear on IT equipment due to airborne particulate matter.
- Lack of UPS on network main distribution frame increases risk of unconditioned power or power loss causing intermittent and possibly untraceable network outages.
- Use of rack mounted UPS is inconsistent, not all IT equipment in racks are connected to UPS, increasing risk that small power fluctuations may cause intermittent outages or damage to unprotected IT equipment. Systematically ensuring that electrical connections are proper and documented is further impaired by clutter in the racks.
- Hot and cold aisle mechanical efficiencies are impaired by IT equipment being deployed (backwards) with air flow running toward the cold aisle.

Recommendation: Recommend that these observations be mitigated through mostly labor, but there may be a requirement to obtain a handful of additional rack mounted UPS.

Summary of Process and Technical Assessment

Cask has made 42 specific process and technical observations with recommendations. The following table lists the observations organized by the previously identified IT goals.

Manage Technology Acquisition within Organization ISO Business Objectives	**Manage Technology IAW Best Industry Practices**
TA-1 (High) User Loss of Confidence in VDI	DP-1 (High) Disaster Recovery Planning
TA-2 (High) User Experience with VDI	DP-2 (Low) Commvault_Disk E:\ low on space
TA-3 (High) VDI Adoption Hampered	DP-3 (High) Host System Backup (b) (7)(E)
TA-4 (Low) Help Desk Hours Insufficient	DP-4 (High) Data Backup Testing
TA-5 (Med) Law Manager Functionality	DP-5 (Med) System State Errors
TA-6 (High) User Data Storage Policy	DP-6 (Med) Commvault License
TA-7 (Med) DMS Documentation	DP-7 (High) Backup SOP
	DP-8 (Low) Commvault Deduplication
Attain and Maintain Repeatable Processes	I-1 (High) No Anti-Virus (b) (7)(E)
N-1 (High) Network Security Practices	I-2 (High) Unsupported Windows 2003
N-2 (High) Vulnerability Scanning	I-3 (High) Unsupported Servers
N-3 (High) Administrator Password Policy	I-4 (High) Java Out of Date
SM-1 (High) ITSM Process Implementation	I-5 (Med) Test/Dev Mirroring Prod
SM-2 (High) Continuity Planning	I-6 (High) Developer Segregation
SM-3 (High) Technical Baseline	I-7 (Low) High UPS Utilization
SM-4 (Med) CM Documentation Storage	V-1 (Med) Dual Path vNICs
SM-5 (Med) Help Desk Incident Processing	V-2 (Med) VM Symantec Endpoint
SM-6 (Med) VDI Recovery Hampered	V-3 (Low) VMware Tools
	V-4 (Low) VDI Infrastructure Memory Utilization
	V-5 (Low) VDI Host Overcommit Ratio
	V-6 (Low) VM Hardware Discrepancies
	V-7 (Low) VMware Licensing
	N-4 (High) Network Monitoring
	N-5 (Med) Network Cabling Standards
	DC-1 (High) Data Center Infrastructure Risks
	DC-2 (Med) Data Center Configuration Risks

The following table provides a summary of the process and technology assessment by priority within each of the IT goals.

IT Goal	**Category**	**Priority**			**Summary**
		High	**Med**	**Low**	
Manage technology acquisition within organization in support of business objectives	Tech Acq	4	2	1	» There are significant technical obstacles to VDI enablement and acceptance; outside professional services is probably necessary » There are also significant organizational acceptance obstacles; a deliberate Organizational Change Management (OCM) effort may be necessary

IT Goal	Category	Priority			Summary
		High	Med	Low	
					» Documentation of requirements and technical instantiation of key systems supporting core business functionality is lacking
Attain and maintain repeatable processes	Network	3	0	0	» Key network security and management processes are not in place and must be implemented
	Service Mgmt	3	3	0	» Operational processes are not documented leaving the infrastructure vulnerable to failures and maintaining continuity » The lack of documentation and independent configuration backups prior to the virtual environment failure set back the VDI implementation a number of months
Manage technology in accordance with best industry practices	Data Protection	4	2	2	» Disaster Recovery Planning must be conducted, implemented, and maintained » Ongoing data backup of all systems should be reviewed for completeness, capability, and tested
	Infra-structure	5	1	1	» Core business applications require upgrading so they are capable of running with supported hardware and software » An adequate Development/Test environment and promotion procedures must be established
	Virtual	0	2	5	» Ironically, despite the historical failure event of the virtual environment, the virtual infrastructure is pretty solid
	Network	1	1	0	» Network monitoring tools need to be implemented » Network cabling standards are not utilized and can lead to failures
	Data Center	1	1	0	» The data center infrastructure is inadequate and cost/effort prohibitive to fix » However, there are some relatively simple actions that can be taken to improve the DC
	Total	**21**	**12**	**9**	» **42 Total Observations**

Conclusion

Upon consideration of all of the organizational, process and technology assessment observations, we conclude that although there are significant obstacles, with sufficient resourcing IRM can meet the vast majority of e-Adjudication goals. We couch this statement because prioritization of requirements must take place as there is rarely unlimited funding to solve all technical issues or personnel resourcing. In the next section we will present a number of overarching recommendations for consideration to effect this conclusion.

Overarching Recommendations

We have synthesized the organizational, process and technology observations and recommendations into five (5) overarching recommended courses of action. They are presented within their broad IT Goal. Within the Manage Technology Acquisition goal, there is really one overarching recommended course of action to formalize the entire process of developing and managing business requirements through their enablement as IT capabilities and into operation. There are four parts of Rec #1(a – d) to achieving this as depicted in Figure (7). The Process and Technology IT Goals include Rec #2 - #5 that are operational in nature.

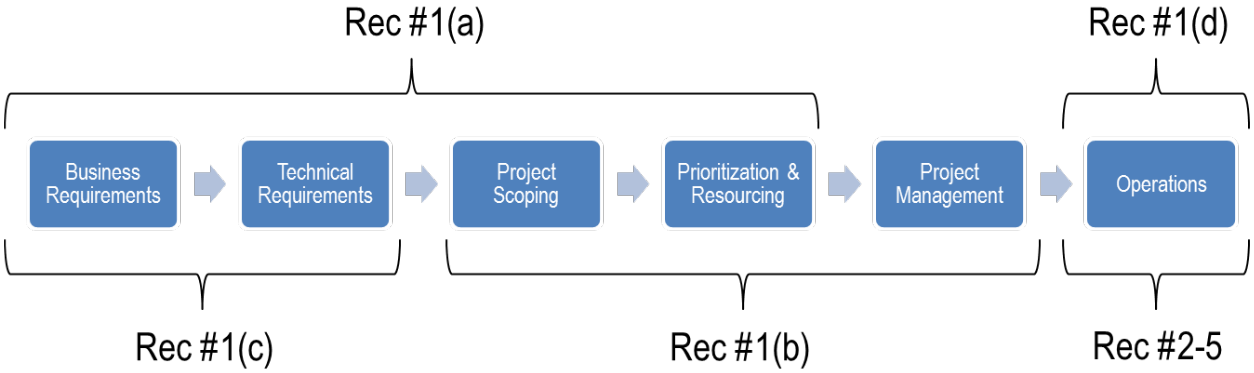


Figure 7: Technology Acquisition to Operations Sequence

A. Manage Technology Acquisition

Rec #1(a). Review the relationship between Clerk of the Board (CoB) and IRM

a. We feel that ‘missing’ roles of Enterprise Architect and IT Consultant combined with the lack of business and technical requirements documentation of core business applications is an indicator of a systemic problem with planning for the business and technology architecture. The e-Adjudication effort provides the impetus and necessity to reevaluate how requirements are developed, documented and enabled by IT.

b. Recommend that MSPB review the relationship between Clerk of the Board (CoB) and IRM, focusing on responsibilities and roles associated with management of the business and technology architecture. This relationship would be best supported by someone placed in the role to liaison role between CoB driven requirements and IRM Development technical evaluation and implementation.

Rec #1(b). Develop a transition plan for the IT infrastructure

a. A transition plan can serve as a roadmap establishing expectations for the achievement of business and technical objectives as well as depicting resourcing and schedule constraints. Oftentimes, the transition plan stems from a gap analysis of the baseline architecture (Status Quo) and the target architecture (To-Be). During the course of the assessment, Cask worked with MSPB to implement existing tools that can baseline the infrastructure (Appendix (B)). Then, we documented the intent for the virtualization and consolidation of the infrastructure as a form of Target Architecture (Appendix (C)). Finally, we provide some considerations for the development of a Transition Plan (Appendix (D)).

b. Recommend that MSPB leverage this beginning to develop a Transition Plan to guide and communicate intent within the organization for the transition.

Rec #1(c). Update core business applications

a. A small number of core business applications were identified to us that provide the greater part of the functionality foundation in the enterprise. This includes Law Manager, eAppeal and Document Management System (DMS). We understand that these applications were either custom coded or heavily configured commercial applications that have not been updated for some time.

b. Recommend that MSPB:

   i. Validate the business and technical requirements for these applications to support e-Adjudication

   ii. Perform such updates as necessary to bring these applications to supported hardware and software while also developing a prioritized path for functional capability upgrades are necessary to support the business

   iii. Develop system documentation

Rec #1(d). Assign a Service Manager

a. The role of Service Manager is to manage the relationship between IRM and their customers. This role is primary responsible for service delivery and management of customer expectations. We found this role 'missing' from IRM during our organizational assessment. Particularly with issues surrounding customer adoption of VDI, this role is critical.

b. Recommend that MSPB consider assigning a Service Manager. There could be synergies if this role was combined with the liaison role mentioned in Recommendation #7. This would require a dedicated resource to handle both roles.

c. Also, MSPB should consider engaging an Organizational Change Management (OCM) consultant to provide expert assistance with customer adoption of e-Adjudication.

B. Repeatable Operational Processes

Rec #2. Invest in a prioritized and systematic development and implementation of operational processes and tools to manage IT infrastructure

a. Core IT Service Management, continuity/disaster recovery planning and data backup testing are the backbone for IRM to provide repeatable consistent support across the MSPB enterprise with limited personnel resources. Development of the various processes and tool implementations can be a daunting endeavor, particularly with providing ongoing support to the enterprise.

b. Recommend that MSPB consider engaging an ITSM provider to assist in the process development and tool evaluation (as required).

C. Manage Technology

Rec #3(a). Continue to use virtualization services to consolidate IT footprint

a. The VMWare health check as well as our assessment indicate that the virtualization approach utilized by MSPB is generally sound. The previous failure of the virtual environment was an anomaly that was compounded by the lack of an effective data backup schema that made restoration impossible.

b. Recommend that the virtualization course be maintained. In particular, the use of the Nutanix appliances works to mitigate server administrator technical skill limitations and makes the environment more repeatable.

Rec #3(b). Continue to pursue VDI as the correct path for client services

a. Having multiple remote offices is one of the top use cases for a Virtual Desktop infrastructure, but in many cases a standard implementation of a virtual desktop isn’t always enough. For MSPB to be able to take full advantage of the benefits of VDI, there must be some advanced designing to be performed. One of the key designs would be application delivery. This would allow MSPB to have greater benefits from their virtual desktop solution. Some key benefits are:

   i. Reduction in operational cost through better utilization of limited resources (Smaller staff can manage more desktops)

   ii. Increased security. All data resides in a single location and allows MSPB support staff to controlled organizational policies to ensure security compliance. This is especially important for remote users.

   iii. Improved end-user experience. This user experience is key and why we suggest investing in VMware Professional Services.

   iv. Improved Business Continuity and Disaster Recovery by protecting data locally and not being dependent on the end-user.

b. Recommend MSPB utilize VMware’s Professional Services to provide a comprehensive architectural design and implementation of an application delivery solution that meets their needs.

Rec #4. Invest in a dedicated network administrator

a. Although the network itself is solid at MSPB HQ. The management of the network is hampered by a lack of dedicated support to implement and utilize process and tools to ensure adherence to security and best business practices as well as monitor the entire network outside of MSPB HQ.

b. Recommend that MSPB hire a dedicated Network Administrator empowered with the requisite authority and responsibility for the network.

Rec #5. Conduct a Business Case Analysis (BCA) and Analysis of Alternatives (AoA) for a hosting solution

a. The data center infrastructure has significant limitations, which collectively may pose unacceptable risks to consistently meet the goals of e-Adjudication without mission limiting planned and unplanned outages.

b. The President’s Federal Data Center Consolidation Initiative (FDDCI) has goals to close approximately 800 data centers much like this one. Recommend that

MSPB seek to migrate their technology to either a public or private data center that is certified to meet their requisite physical and network security requirements.

Cask believes that all of the overarching recommendations are of a high priority and should be considered for implementation. However, they have different resourcing and schedule requirements and may not be considered of equal priority by MSPB. Cask understands that it is not feasible with a small organization like MSPB to launch multiple efforts simultaneously with equal attention. This is why we have recommended the use of a third-party or hiring action with a number of these recommendations to provide particular expertise that we feel MSPB may not have and/or provide the extra hands and feet to more efficiently accomplish tasks without diluting internal MSPB resources beyond their effectiveness. However, this approach takes commitment and funding resourcing from management.

It is difficult to provide MSPB a firm timeline and cost for these recommendations with the information that we now possess. For example, we have little insight into the code base of MSPB core business applications. So, scoping what modifications may need to be conducted to achieve supportability (and possibly enable new functionality (see T-5) and providing a timeline and cost is not feasible. However, we look forward to discussing these recommendations with MSPB and through that dialogue will seek to provide any additional insight we can for the conduct of these recommendations within MSPB resourcing and contracting particulars.

Appendixes

Appendixes are provided in the following pages.

Remainder of Page Blank

Appendix (A) European e-Competence Framework v3.0

Cask utilized the European e-Competence Framework as the primary tool to conduct our organizational skills assessment. This framework establishes competencies across 23 roles found within IT organizations. These 23 roles cover the IT lifecycle from the inception of a product or service through its operation and retirement. Figure 8 below depicts the 23 roles in the context of the lifecycle.

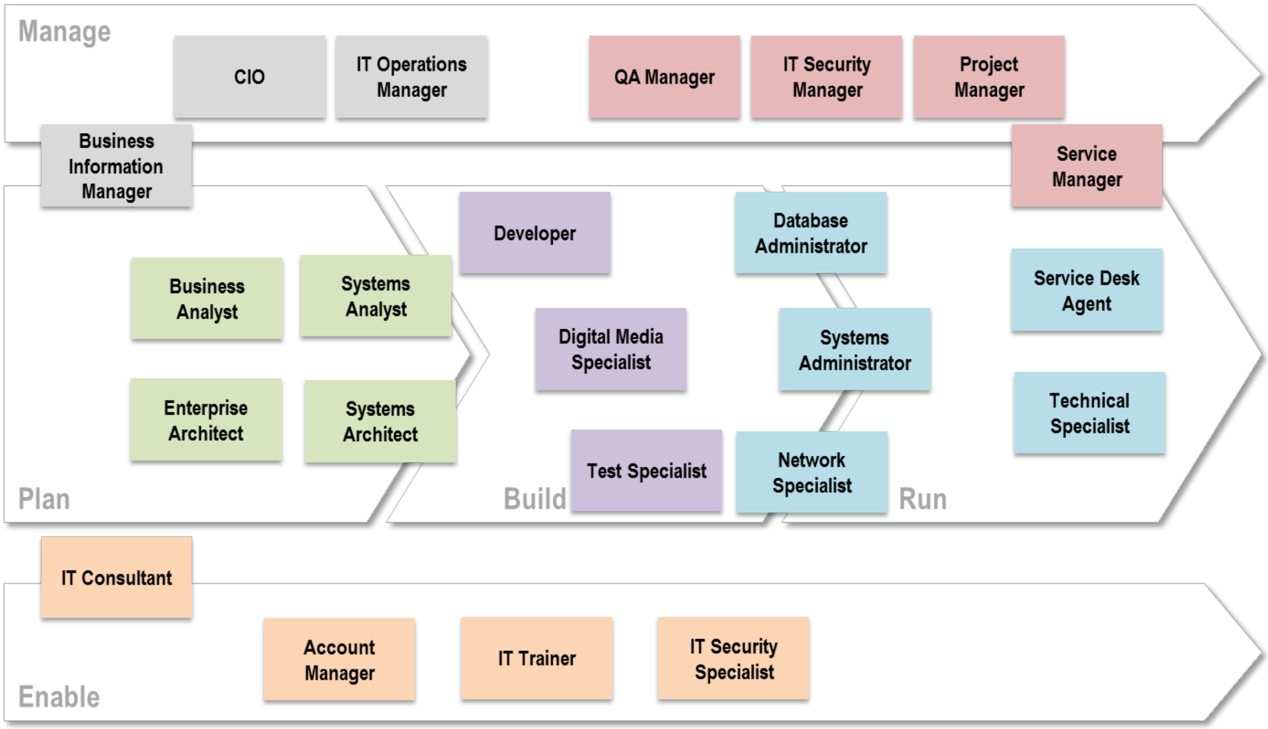


Figure 8: e-Competence Framework v3.0 Roles

It's important to note that a role does not necessarily equal one or more individuals. In small organizations, like MSPB, a single individual will fulfill multiple roles. It is important to note that each role is critical. The following table describes the roles as well as listing its' main tasks and competencies.

Role	Description	Main Tasks	Competencies
Account Manager	Senior focal point for client sales and customer satisfaction	» Maintain overall customer satisfaction with products and/or services » Identify opportunities to propose new products or services to client(s) » Be the primary contact point for client executive management » Deliver value added presentations related to products and services to customer executive management » Lead negotiations to establish profitable contracts with client(s) » Maintain and enhance business relationships	» Sales Proposal Development » Sales Management » Forecast Development » Relationship Management » Channel Management

Role	Description	Main Tasks	Competencies
Business Analyst	Analyses Information System for improving business performance	» Contribute to the preparation of the business plan of the organization » Identify areas for improvement in business processes providing possible IT solutions compliant with the IT strategy » Build requirements, specifications, business processes and the business case related to the proposed solutions » Analyze required information and documents	» IT and Business Strategy Alignment » Business Plan Development » Process Improvement » Needs Identification
Business Information Manager	Proposes plans and manages functional and technical evolutions of the Information System within the relevant business domain	» Responsible for managing the information technology development within the business domain » Anticipate changes to the Information System and the business impact and vice versa » Formalize, consolidate and drive the development of the configuration of the information system » Evaluate the relevance of the Information systems to the business domain » Build a knowledge base through understanding the organization's information system	» IT and Business Strategy Alignment » Business Plan Development » Project and Portfolio Management » Business Change Management » Information and Knowledge Management
Chief Information Officer	Develops and maintains Information Systems compliant to business and organization's needs	» Define the company's strategy for IT Manage all IT department activity » Responsible for the quality and management of customer-supplier relationships » Define and ensure compliance with Service Level Agreements » Negotiate and implement complex contracts » Make recommendations to senior general management » Ensure that change management processes are implemented » Ensure the reliability, confidentiality, security and integrity of Information Systems	» IT and Business Strategy Alignment » Business Plan Development » Project and Portfolio Management » Relationship Management » IT Governance

Role	Description	Main Tasks	Competencies
Database Administrator	Designs and implements, or monitors and maintains databases	» Define/ build/optimize database models and schemas » Apply standards methods and tools for measuring and reporting on wide set of relevant performance indicators (response time, availability, safety, integrity …) » Produce database procedures and instructions for other analysts or administrators » Monitor and maintain databases » Identify, investigate and correct problems or incidents related to databases » Provide training, support, advice and guidance on database issues to other information system practitioners	» Application Design » Application Development » Component Integration » Problem Management » Information and Knowledge Management
Developer	Builds/codes IT solutions and specifies IT products according to the customer needs	» Develop component » Engineer component » Shape documentation » Provide component support beyond the first level » Supply 3rd level support	» Application Development » Component Integration » Testing » Documentation Production » Problem Management
Digital Media Specialist	Creates websites and multimedia applications combining the power of digital technology with effective use of graphics, audio, photographic and video images	» Design web and multimedia content to provide clear and visually attractive solution in line with customer needs » Test and resolve any technical issues » Ensure accessibility for disabled users and for accessibility via a range of browsers » Ensure compliance with privacy, legal requirements and environmental constraints	» Application Design » Application Development » Testing » Solution Deployment » Digital Marketing
Enterprise Architect	Designs and maintains the Enterprise Architecture	» Devise business improvement opportunities and create proposals » Align IT strategy and planning with the organization’s business goals » Streamline business processes, functions, procedures and workflows and apply a consistent implementation approach » Manage stakeholder engagement in the development of new processes and systems and verifies feasibility » Conduct post-implementation reviews to evaluate benefits accrued from new processes and systems	» IT and Business Strategy Alignment » Business Plan Development » Architecture Design » Technology Trend Monitoring » Business Change Management

Role	Description	Main Tasks	Competencies
IT Consultant	Supports understanding of how new IT technologies add value to a business	» Provide advice on how to optimize the use of existing tools and systems » Raise awareness of information technology innovations and potential value to a business » Make recommendations for the development and implementation of a business project or technological solution » Participate in the definition of general project specifications » Participate in the assessment and choice of IT solutions	» Technology Trend Monitoring » Business Change Management » Needs Identification » Product or Project Planning » Risk Management
IT Operations Manager	Manages operations, people and further resources for the IT activity	» Coordinate and manage staff » Direct, organize, plan and monitor activities » Negotiate the objectives and resources » Manage the departmental budget » Establish and monitor management information » Analyze and propose solutions for the continuous productivity improvement » Manage the implementation and monitoring of IS quality assurance and security » Communicate with internal business departments and project owners	» Personnel Development » Risk Management » IT Quality Management » Business Change Management » Information Security Management
IT Security Manager	Manages the Information System security policy	» Define and implement procedures linked to IS security » Contribute to the development of the organization's security policy » Establish the prevention plan » Inform and raise awareness among general management » Ensure the promotion of the IT security charter among users » Inspect and ensure that principles and rules for IS security are applied	» Technology Trend Monitoring » Information Security Strategy Development » Risk Management » IT Governance » Information Security Management
IT Security Specialist	Ensures the implementation of the organizations security policy	» Ensure security and appropriate use of IT resources » Evaluate risks, threats and consequences » Provide security training and education » Provide technical validation of security tools » Contribute to definition of security standards » Audit security vulnerability » Monitor security developments to ensure data and physical security of the IT resources	» Change Support » Service Delivery » Personnel Development » Information and Knowledge Management » Information Security Management

Role	Description	Main Tasks	Competencies
IT Trainer	Educates and trains IT professionals and practitioners to reach predefined standards of IT technical /business competence	» Conduct training needs analyses » Design programs to meet needs » Produce and/or update existing training materials (content and method) » Deliver effective training in classroom, on-line or informally » Monitor, evaluate and report effectiveness of training » Maintain currency of expertise on specialist subject » Evaluate and report student performance	» Education and Training Provision » Personnel Development
Network Specialist	Ensures the alignment of the network, including telecommunication and/or computer infrastructure to meet the organization's communication needs	» Ensure that communication performance, recovery, and security needs meet agreed service agreement standards » Contribute to define network design policies, philosophies and criteria » Investigate, diagnose and solve network problems » Use network management system tools to determine network load and model performance statistics » Maintain awareness of relevant legislation affecting network security	» Application Design » Component Integration » Solution Deployment » Problem Management » Information Security Management
Project Manager	Manages project to achieve optimal performance that conforms to original specifications	» Organize, coordinate and lead the project team » Supervise project progress » Coordinate, record and ensure quality compliance » Circulate and distribute information from the project owner » Implement the new application or service » Plan maintenance and user support » Ensure specification compliance » Comply with budgets and delivery times » Update the project according to changing circumstances	» Product/Service Planning » Project and Portfolio Management » Risk Management » Relationship Management » Business Change Management
Quality Assurance Manager	Guarantees that Information Systems are delivered according to organization policies (quality, risks, Service Level Agreement)	» Establish and deploy the IT quality policy » Organize and provide quality training » Provide IT managers with quality performance indicators » Perform quality audits » Organize customer satisfaction surveys » Assist project team members to build and perform project quality plans	» IT Quality Strategy Development » Risk Management » Process Improvement » IT Quality Management

Role	Description	Main Tasks	Competencies
Service Desk Agent	Provides first line telephone or e-mail support to clients with technical issues	» Identify and diagnose issues and problems » Categorize and record reported queries and provide solutions » Support problem identification » Advise users on appropriate course of action » Monitor issues from start to resolution » Escalate unresolved problems to higher levels of support	» User Support » Service Delivery » Problem Management
Service Manager	Plans, implements and manages solution provision.	» Define Service requirements » Negotiate SLA / OLA » Manage solution operation » Provide service delivery	» Service Level Management » Service Delivery » Problem Management » Contract Management » Personnel Development
Systems Administrator	Administers IT System components to meet service requirements.	» Investigate, diagnose and solve system related problems » Install and upgrades software » Schedule installation work, liaising with all concerned to ensure that installation priorities are met and disruption to the organization is minimized » Diagnose and solve problems and faults occurring in the operation of hardware and software » Comply with organization procedures to ensure integrity of the system	» Component Integration » Testing » User Support » Problem Management » Information Security Management
Systems Analyst	Analyses requirements and specifies software and systems.	» Recommend resolutions and improvements » Provide integrated solutions » Provide consolidate findings on components or processes	» Architecture Design » Process Improvement » Systems Engineering
Systems Architect	Plans and is accountable for the implementation and integration of software and/ or IT systems.	» Analyze technology, business and technical requirements » Specify and implement complex IT solutions » Lead development and integration of components » Lead and/ or conduct system integration	» Architecture Design » Technology Trend Monitoring » Systems Engineering » Component Integration » Innovating

Role	Description	Main Tasks	Competencies
Technical Specialist	Maintains and repairs hardware and software.	» Identify software and hardware problems and repair » Perform regular maintenance on hardware and software components » Install cables and configures hardware and software » Document system addresses and configurations » Run diagnostic programs or use test equipment to locate source of problems » Communicate effectively with end users and customer management » Maintain security and functionality through application of program temporary fixes	» Change Support » Service Delivery » Problem Management
Test Specialist	Designs and performs testing plans.	» Select and develop integration testing techniques to ensure the system meets requirements » Design and customize integration tests, identify open issues » Develop test plans and procedures for white and black box testing at unit, module, system and integration levels » Establish procedures for result analysis and reporting » Design and implement defect tracking and correction procedures » Write test program to assess software quality » Develop tools to increase test effectiveness	» Application Development » Component Integration » Testing » Solution Deployment » Problem Management

Remainder of Page Blank

Appendix (B) Baseline Architecture

One of the most important documents that all IT organization should have is a baseline of all their systems. The main purpose of baseline information is to serve as a point of reference and to be able to compare what happens before and after changes has been implemented to a system. Without an accurate baseline, it's difficult to estimate the impact of changes, or to demonstrate progress.

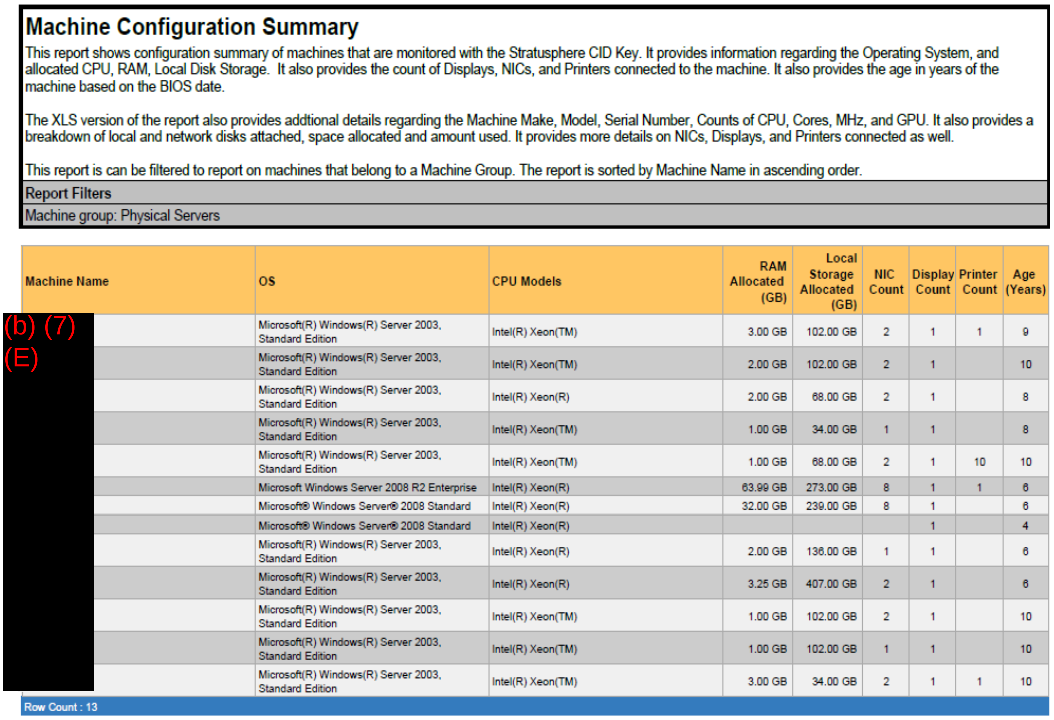
From our discussions with the MSPB leadership, Cask has identified two projects on the Roadmap for MSPB. First a datacenter modernization where MSPB looks to convert the remaining physical system to a virtual platform as well as an update their Network infrastructure. The second project is more of a transformational project on how MSPB operates. MSPB is looking to shift from paper-based work processes and products to automated, electronic adjudication (e-Adjudication) and move to 100% electronic case processing to substantially improve the delivery and efficiency of adjudication services.

Cask suggest following the ITIL methodology of system baselines. This methodology groups baselines into three categories (ITSM, Performance and Configuration Management Baselines).

- The ITSM Baseline can be used as a starting point to measure the effect of a Service Improvement Plan.
- A Performance Baseline can be used to measure changes in Performance over the lifetime of an IT Service.
- A Configuration Management Baseline can be used to enable the IT Infrastructure to be restored to a known Configuration if a Change or Release fails.

Upon reviewing MSPB documentation we determined that there was no completed baseline documentation on any of the systems. For MSPB to have a successful modernization of their datacenter, it is vital for them to have at a minimum a Configuration Management Baseline in place. This baseline will serves as a point of reference going forward. Cask engineers suggested developing a simple CM baseline utilizing an excel spreadsheet and working with the stakeholders on data collection. During this process we discovered that MSPB has a tool called Liquidware Labs Stratusphere that although not fully deployed, could be used to capture and maintain a CM Baseline. Upon request, MSPB's (b) (6) [redacted] has fully deployed Liquidware Labs Stratosphere agents to all hosts. With this MSPB is now able to capture hardware and software baselines (See Figures 9 & 10).

Remainder of Page Blank



Machine Configuration Summary

This report shows configuration summary of machines that are monitored with the Stratusphere CID Key. It provides information regarding the Operating System, and allocated CPU, RAM, Local Disk Storage. It also provides the count of Displays, NICs, and Printers connected to the machine. It also provides the age in years of the machine based on the BIOS date.

The XLS version of the report also provides addtional details regarding the Machine Make, Model, Serial Number, Counts of CPU, Cores, MHz, and GPU. It also provides a breakdown of local and network disks attached, space allocated and amount used. It provides more details on NICs, Displays, and Printers connected as well.

This report is can be filtered to report on machines that belong to a Machine Group. The report is sorted by Machine Name in ascending order.

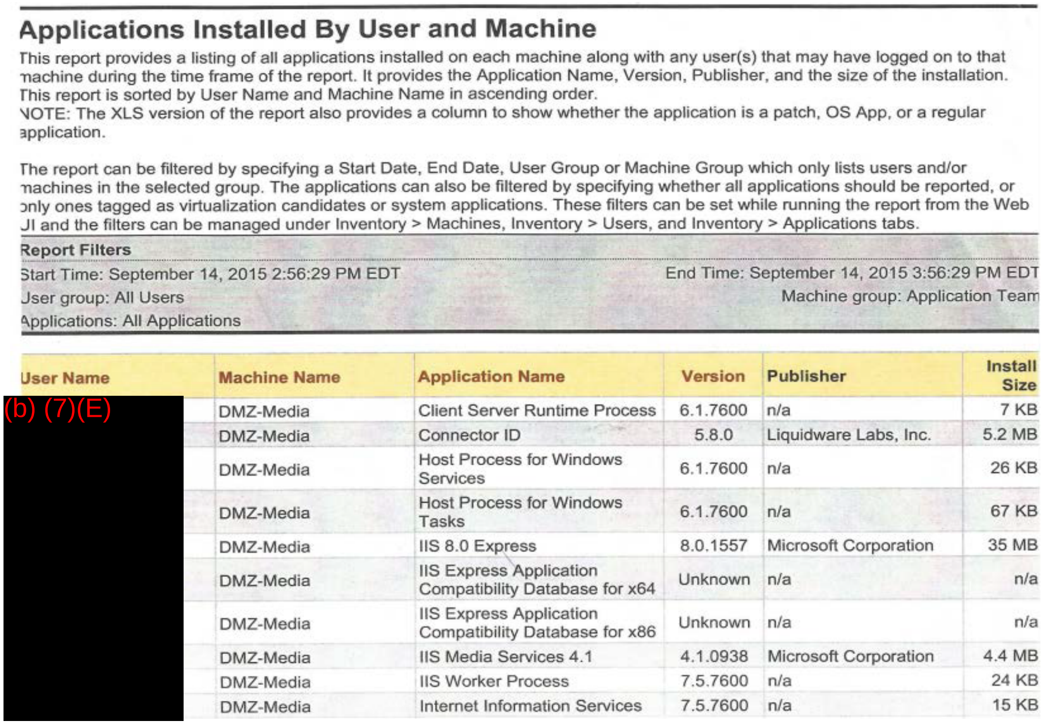
Report Filters

Machine group: Physical Servers

Machine Name	OS	CPU Models	RAM Allocated (GB)	Local Storage Allocated (GB)	NIC Count	Display Count	Printer Count	Age (Years)
(b) (7) (E) [redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(TM)	3.00 GB	102.00 GB	2	1	1	9
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(TM)	2.00 GB	102.00 GB	2	1		10
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(R)	2.00 GB	68.00 GB	2	1		8
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(TM)	1.00 GB	34.00 GB	1	1		8
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(TM)	1.00 GB	68.00 GB	2	1	10	10
[redacted]	Microsoft Windows Server 2008 R2 Enterprise	Intel(R) Xeon(R)	63.99 GB	273.00 GB	8	1	1	6
[redacted]	Microsoft® Windows Server® 2008 Standard	Intel(R) Xeon(R)	32.00 GB	239.00 GB	8	1		6
[redacted]	Microsoft® Windows Server® 2008 Standard	Intel(R) Xeon(R)				1		4
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(R)	2.00 GB	136.00 GB	1	1		6
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(R)	3.25 GB	407.00 GB	2	1		6
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(TM)	1.00 GB	102.00 GB	2	1		10
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(TM)	1.00 GB	102.00 GB	1	1		10
[redacted]	Microsoft(R) Windows(R) Server 2003, Standard Edition	Intel(R) Xeon(TM)	3.00 GB	34.00 GB	2	1	1	10

Row Count : 13

Figure 9: Sample System Hardware Baseline exported from Stratusphere



Applications Installed By User and Machine

This report provides a listing of all applications installed on each machine along with any user(s) that may have logged on to that nachine during the time frame of the report. It provides the Application Name, Version, Publisher, and the size of the installation. This report is sorted by User Name and Machine Name in ascending order.
NOTE: The XLS version of the report also provides a column to show whether the application is a patch, OS App, or a regular application.

The report can be filtered by specifying a Start Date, End Date, User Group or Machine Group which only lists users and/or nachines in the selected group. The applications can also be filtered by specifying whether all applications should be reported, or only ones tagged as virtualization candidates or system applications. These filters can be set while running the report from the Web JI and the filters can be managed under Inventory > Machines, Inventory > Users, and Inventory > Applications tabs.

Report Filters

Start Time: September 14, 2015 2:56:29 PM EDT
End Time: September 14, 2015 3:56:29 PM EDT
Jser group: All Users
Machine group: Application Team
Applications: All Applications

User Name	Machine Name	Application Name	Version	Publisher	Install Size
(b) (7)(E) [redacted]	DMZ-Media	Client Server Runtime Process	6.1.7600	n/a	7 KB
[redacted]	DMZ-Media	Connector ID	5.8.0	Liquidware Labs, Inc.	5.2 MB
[redacted]	DMZ-Media	Host Process for Windows Services	6.1.7600	n/a	26 KB
[redacted]	DMZ-Media	Host Process for Windows Tasks	6.1.7600	n/a	67 KB
[redacted]	DMZ-Media	IIS 8.0 Express	8.0.1557	Microsoft Corporation	35 MB
[redacted]	DMZ-Media	IIS Express Application Compatibility Database for x64	Unknown	n/a	n/a
[redacted]	DMZ-Media	IIS Express Application Compatibility Database for x86	Unknown	n/a	n/a
[redacted]	DMZ-Media	IIS Media Services 4.1	4.1.0938	Microsoft Corporation	4.4 MB
[redacted]	DMZ-Media	IIS Worker Process	7.5.7600	n/a	24 KB
[redacted]	DMZ-Media	Internet Information Services	7.5.7600	n/a	15 KB

Figure 10: Sample System Software Baseline exported from Stratusphere

Appendix (C) Target Architecture

IRM has been planning to virtualize and consolidate services from legacy equipment in order to reduce the rack footprint ultimately to three racks. We found no documentation available to support this effort. We developed the following high level summary of tasks as described to us by (b) (6) [redacted] in order to more fully understand the plan. In Appendix (D) we analyze the plan and provide some key considerations and recommendations for execution.

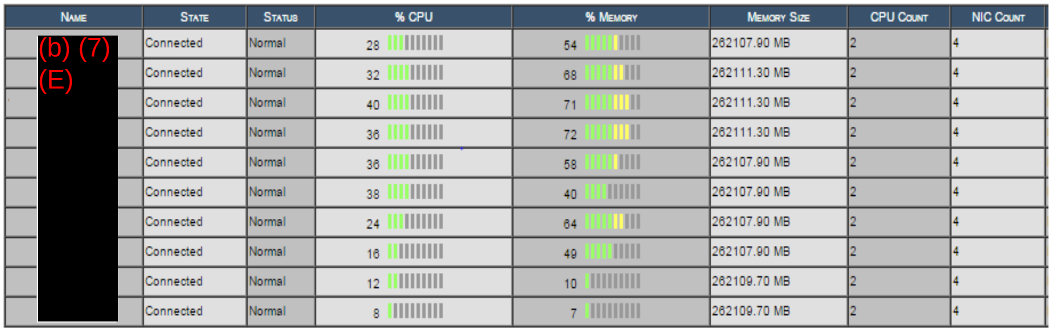
(b) (5) [redacted]

(b) (5) [redacted].

Appendix (D) Transition Planning Considerations

We understand that MSPB is still in the process of learning about everything that is in place in the server room, and thus have not been able to come up with concrete plans. A detailed transition plan is vital to a successful modernization. Cask strongly recommends utilizing the data output from Liquidware Labs Stratusphere to reduce risk in planning and execution.

- (b) (5) [redacted]



Name	State	Status	% CPU	% Memory	Memory Size	CPU Count	NIC Count
(b) (7) (E) [redacted]	Connected	Normal	28	54	262107.90 MB	2	4
[redacted]	Connected	Normal	32	68	262111.30 MB	2	4
[redacted]	Connected	Normal	40	71	262111.30 MB	2	4
[redacted]	Connected	Normal	36	72	262111.30 MB	2	4
[redacted]	Connected	Normal	36	58	262107.90 MB	2	4
[redacted]	Connected	Normal	38	40	262107.90 MB	2	4
[redacted]	Connected	Normal	24	64	262107.90 MB	2	4
[redacted]	Connected	Normal	16	49	262107.90 MB	2	4
[redacted]	Connected	Normal	12	10	262109.70 MB	2	4
[redacted]	Connected	Normal	8	7	262109.70 MB	2	4

Figure 11: VMware Infrastructure Farm

- (b) (5) [redacted]
- (b) (5), (b) (7)(E) [redacted]

Appendix (E) Acronyms

Acronym	Definition
ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigerating, and Air Conditioning Engineers
BICSI	Building Industry Consulting Services International
CIO	Chief Information Officer
CM	Configuration Management
CoB	Clerk of the Board
COOP	Continuity of Operations Plan
CP	Continuity Plan
CMS	Case Management System
DBA	Database Administrator
DMZ	De-Militarized Zone
e-CF	European Competency Framework
EIA	Electronic Industries Alliance
EST	Eastern Standard Time
EULA	End User License Agreement
FDDCI	Federal Data Center Consolidation Initiative
IAW	In Accordance With
IBC	International Building Code
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronic Engineers
IRM	Information Resource Management
ISO	In Support Of (non-standard usage of this acronym)
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
LAN	Local Area Network
MSPB	Merit Systems Protection Board
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
ODA	Oracle Database Appliance
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
P2V	Physical To Virtual
pCPU	Physical Central Processing Unit
QA	Quality Assurance
QOS	Quality of Service
RMAN	Recovery Manager
ROM	Rough Order of Magnitude
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SQL	Structured Query Language

Acronym	Definition
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TC	Technical Committee
TDMM	Telecommunications Distribution Methods Manual
TIA	Telecommunications Industry Association
TIPA	Tudor ITSM Process Assessment
TSB	Telecommunications Systems Bulletin
UPS	Uninterruptable Power Supply
US-CERT	United States Computer Emergency Readiness Team
vCPU	Virtual Central Processing Unit
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
vNIC	Virtual Network Interface Card
VPN	Virtual Private Network
WAN	Wide Area Network