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

Cask
STRATEGY. SOLUTIONS. SUCCESS.

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.

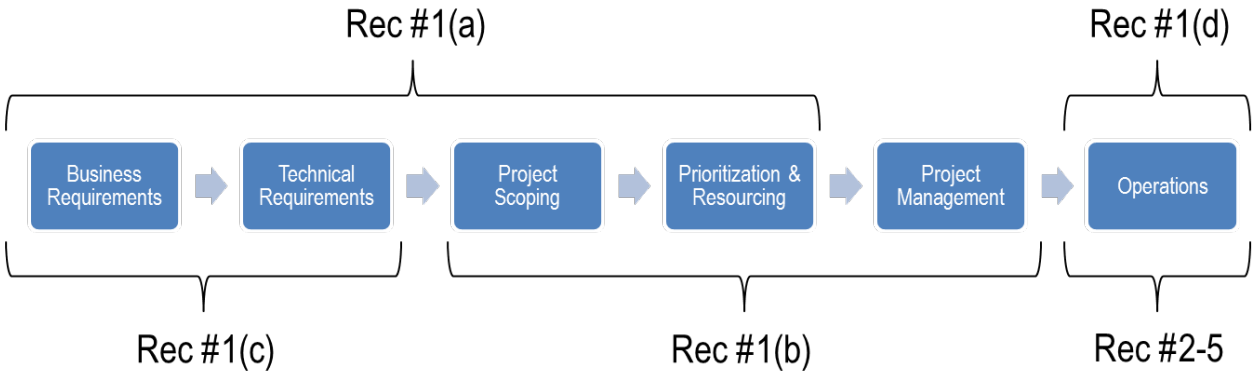


Figure i: Technology Acquisition to Operations Sequence

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

Executive Summary ..... **ii**
Introduction **1**
Purpose 1
Background 1
MSPB Mission 1
Information Technology 1
Methodology 2
References 3
Organizational Skills Assessment **4**
Technique and Observations 4
Summary of Organization Skills Assessment 8
Process and Technology Assessment **9**
Manage Technology Acquisition within Organization ISO Business Objectives 9
Attain and Maintain Repeatable Processes 11
Network Processes 11
IT Service Management Processes 13
Manage Technology IAW Best Industry Practices 16
Data Protection 16
Infrastructure 19
Virtualization 23
Network 25
Data Center 27
Summary of Process and Technical Assessment 29
Conclusion **30**
Overarching Recommendations **31**
Appendixes **34**
Appendix (A) European e-Competance Framework v3.0 ..... A-1
Appendix (B) Baseline Architecture B-1
Appendix (C) Target Architecture C-1
Appendix (D) Transition Planning Considerations D-1
Appendix (E) Acronyms E-1

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.

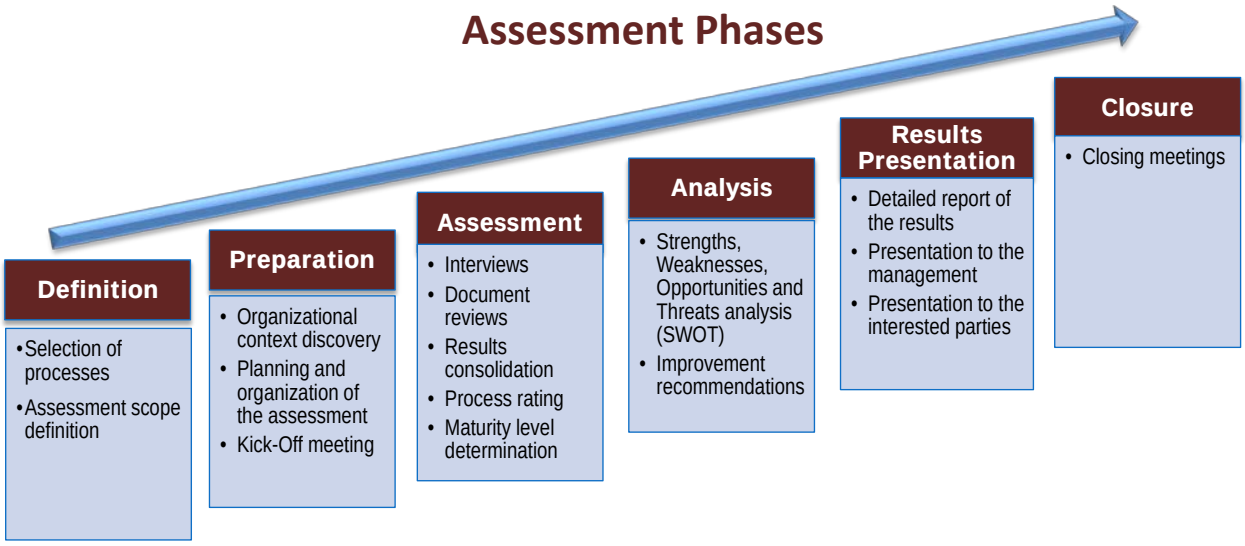


Figure 1: Assessment Methodology

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.

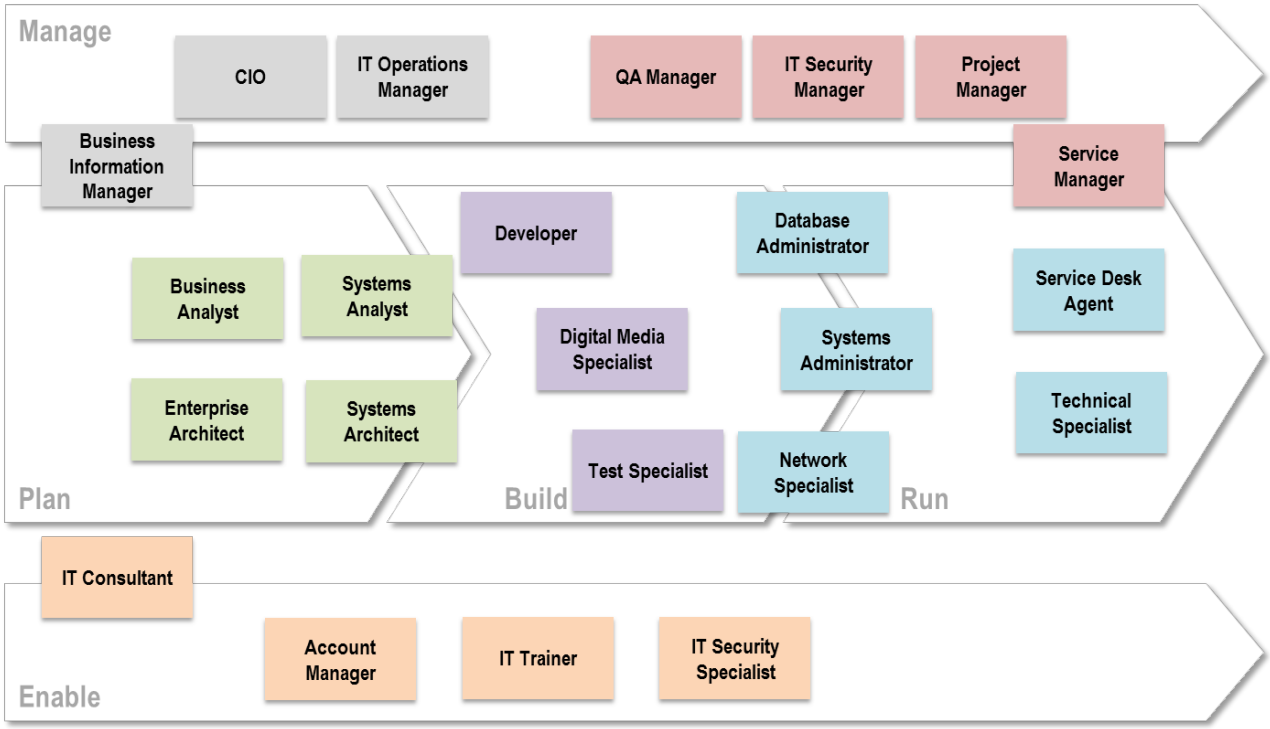


Figure 2: e-Competence Framework v3.0 Roles

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).

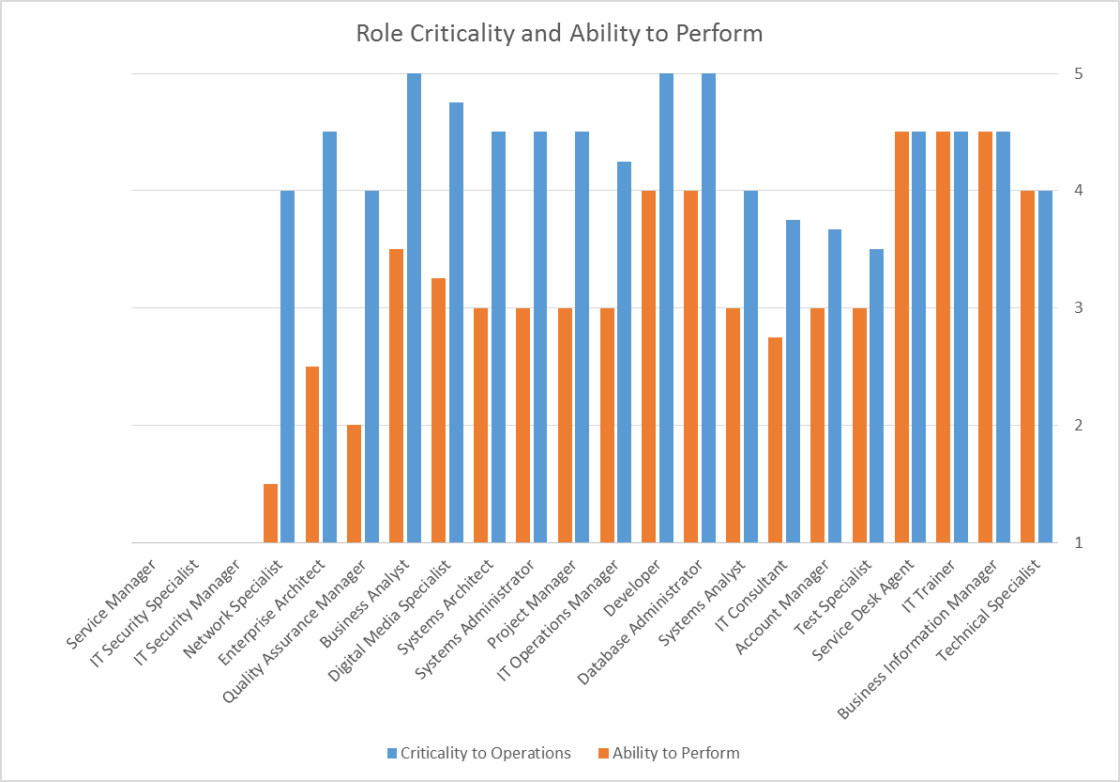


Figure 3: Role Criticality vs Ability to Perform

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.

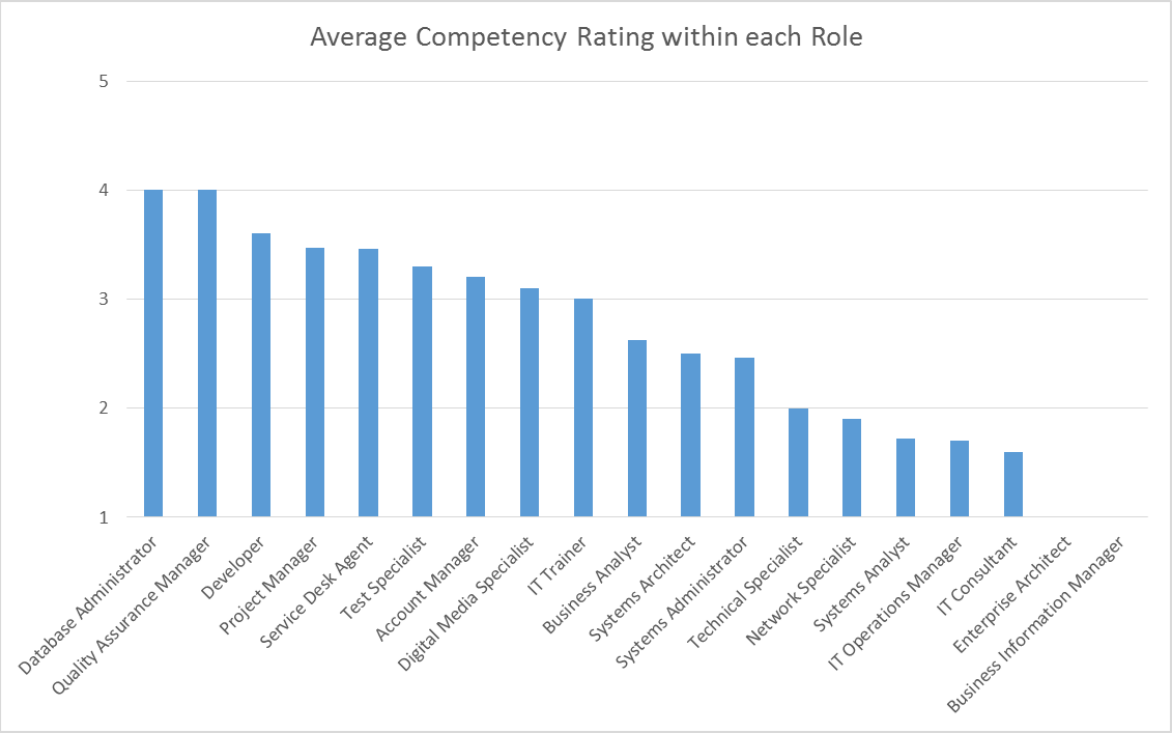


Figure 4: Average Competency Rating by Role

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.

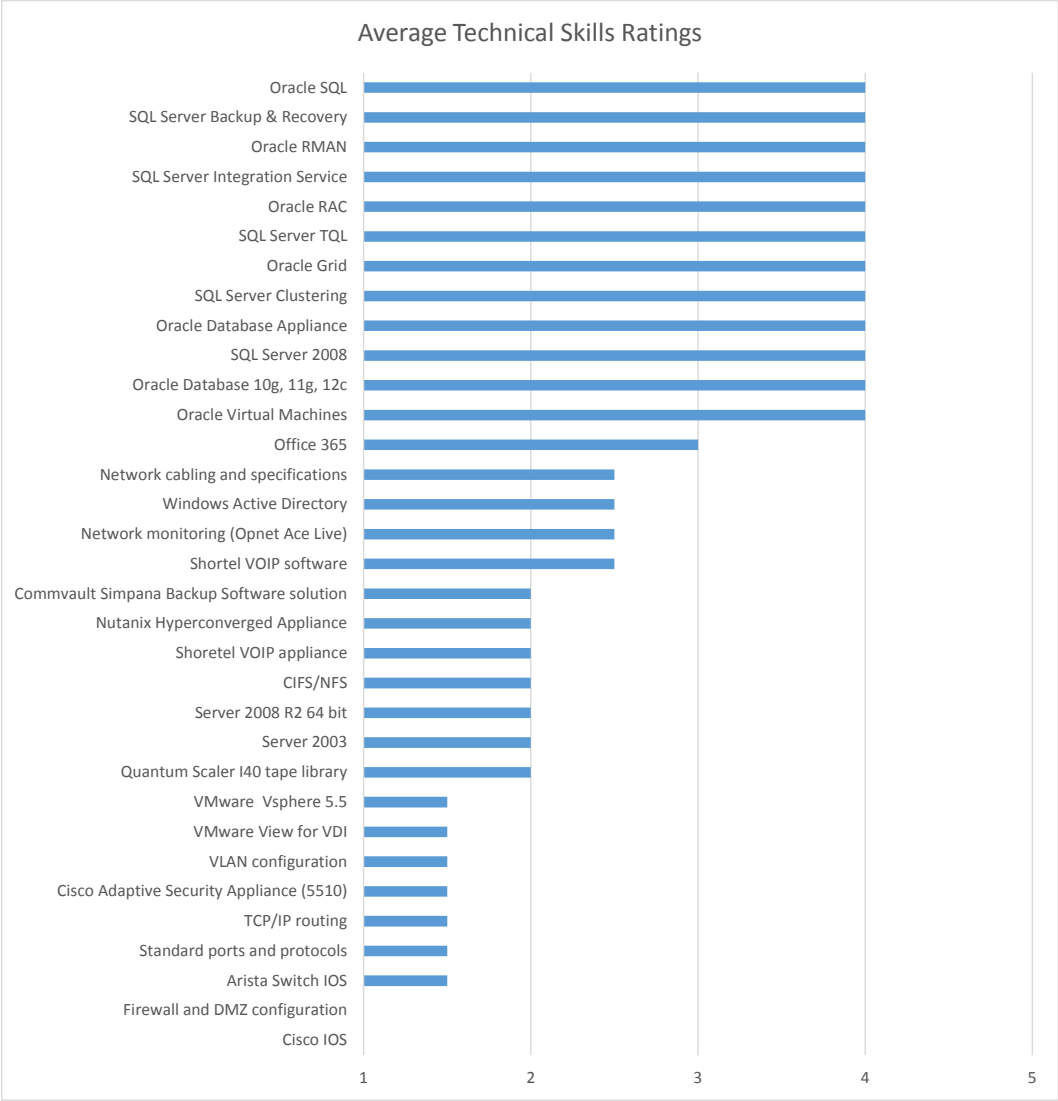


Figure 5: Technical Skill Ratings

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.

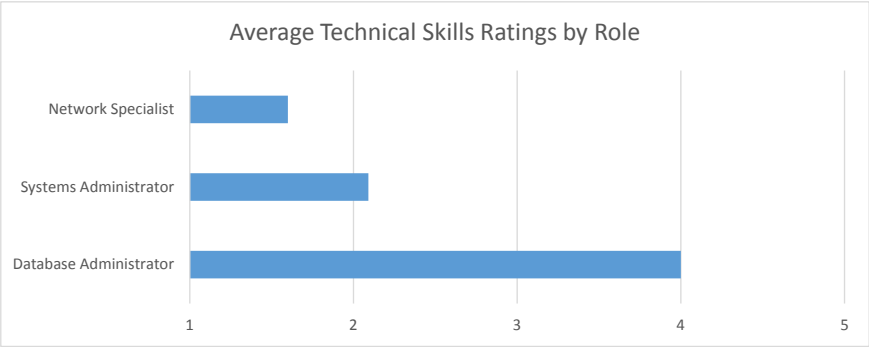


Figure 6: Average Technical Skill Ratings by Role

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

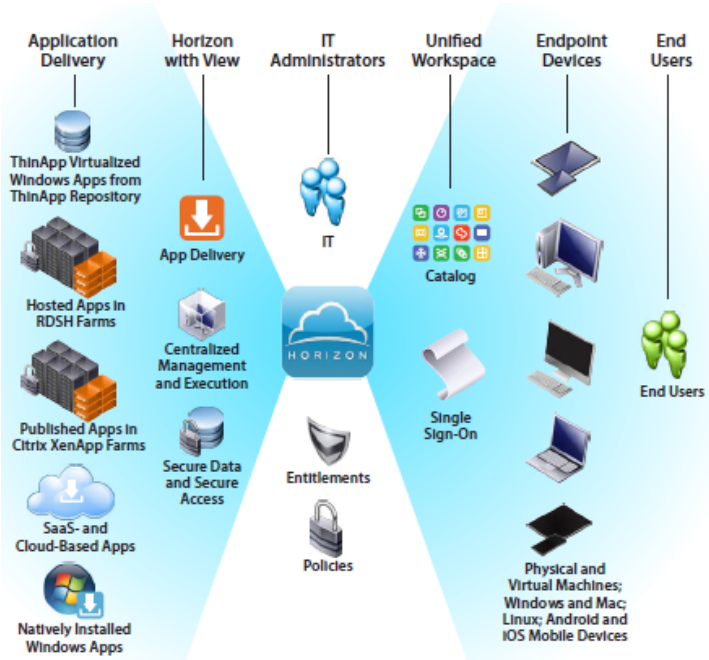
Manage Technology Acquisition within Organization ISO Business Objectives

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.					

Category:	Technology Acquisition	ID:	TA-3	Severity:	High
Observation: VDI Adoption Hampered					
Discussion: 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.



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.

Category:	Technology Acquisition	ID:	TA-4	Severity:	Low
Observation: Help Desk Hours Insufficient					
Discussion: 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.					
Recommendation: Consider committing additional resources toward extending the hours for the Help Desk.					

Category:	Technology Acquisition	ID:	TA-5	Severity:	Medium
Observation: Law Manager Functionality					
Discussion: Lack of transparency and auditing capability within Law Manager impairs compliance with recordkeeping requirements.					
Recommendation: 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.					

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

Category:	Technology Acquisition	ID:	TA-7	Severity:	Medium
Observation: DMS Documentation					
Discussion: Lack of documentation on the DMS architecture impedes the ability to explore its full capability in supporting records and content management functionality.					
Recommendation: Work collaboratively with key records user community to identify priorities for establishing documentation.					

Attain and Maintain Repeatable Processes

Network Processes

Category:	Network	ID:	N-1	Severity:	High
Observation: Network Security Practices					
Discussion: 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.					
Recommendation: 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					

Category:	Network	ID:	N-2	Severity:	High
Observation: Vulnerability Scanning					
Discussion: Vulnerability scans are not routinely performed on the servers leaving systems with possible vulnerabilities that would be open to exploitation. New vulnerabilities are					

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]

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) [redacted] 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) [redacted]

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]

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)

(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) (7)(E)	[redacted]
[redacted]	[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]	[redacted]	(b) (7)(E) [redacted]
[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[redacted]servers Java(TM) and Java(TM) SE Development Kit out of date. This applies to

Server Name	Service
[redacted]	[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.

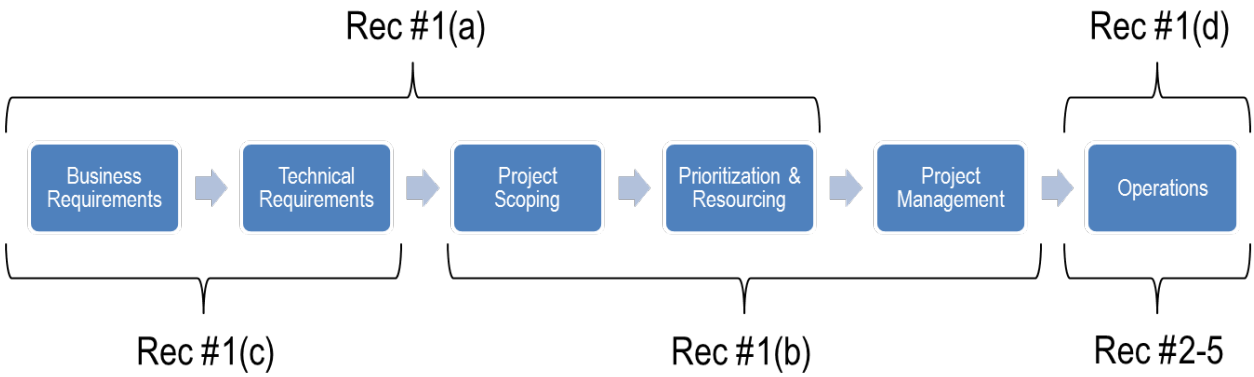


Figure 7: Technology Acquisition to Operations Sequence

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.

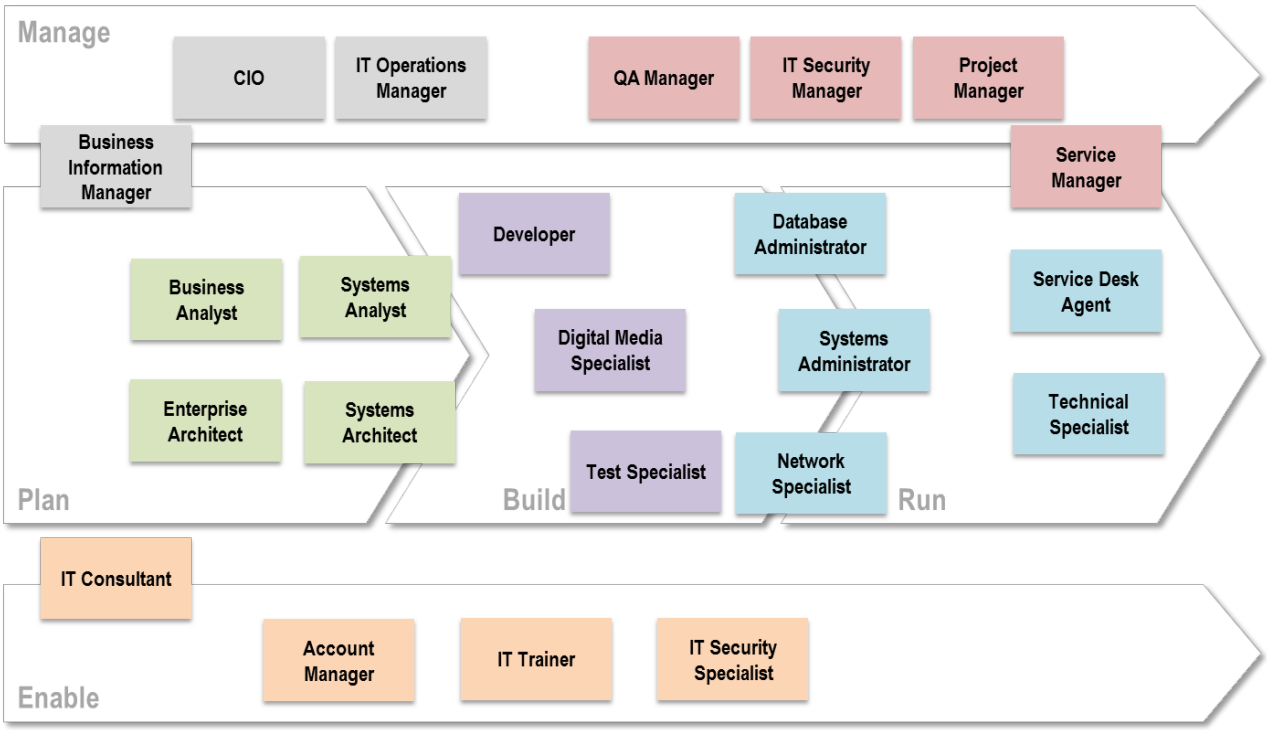


Figure 8: e-Competence Framework v3.0 Roles

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

(b) (7)(E)

Machine Name	OS	CPU Models	RAM Allocated (GB)	Local Storage Allocated (GB)	NIC Count	Display Count	Printer Count	Age (Years)
[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 machine 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 machines 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 UI 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
User group: All Users
Machine group: Application Team
Applications: All Applications

(b) (7)(E)

User Name	Machine Name	Application Name	Version	Publisher	Install Size
[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
	Connected	Normal	32	68	262111.30 MB	2	4
	Connected	Normal	40	71	262111.30 MB	2	4
	Connected	Normal	36	72	262111.30 MB	2	4
	Connected	Normal	36	58	262107.90 MB	2	4
	Connected	Normal	38	40	262107.90 MB	2	4
	Connected	Normal	24	64	262107.90 MB	2	4
	Connected	Normal	16	49	262107.90 MB	2	4
	Connected	Normal	12	10	262109.70 MB	2	4
	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