smarter solutions. **better outcomes.**

Pierce College Infrastructure Assessment

Proposed Remediation Timelines

Document Overview

Pierce College engaged Burwood Group in an assessment of campus infrastructure and operations to gather information and feedback on the current state and to begin steps towards establishing better alignment between the business and technology teams.

This document combines the highlights of each of the work stream deliverables and discusses the key findings of the Burwood Group.

Assessment of LA Pierce College IT Services

Capture Business Requirements, Objectives, and Guiding Principles

Review LA Pierce College IT Services

Assessment of Subcomponents

Service Desk | Incident Mgmt. | Problem Mgmt. | Config. Mgmt. | Change Mgmt. | Release Mgmt. | Service Level | Capacity Mgmt. | Availability Mgmt. | Business Cont.

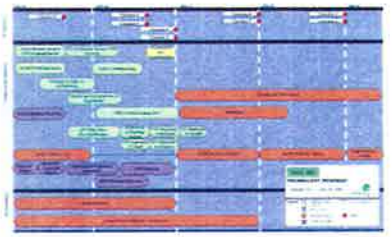
Assessment Findings

Observations and Recommendations

Assessment Recommendations

Improvements | Investments | Roadmap

Deliverables



Methodology

Data Gathering

- Understand Pierce College use cases and end user needs
- Understand IT and Administration position on subject area
- Understand current process and what works and what is broken

Review

- Review current state configuration with Pierce College IT
- Understand device capabilities and limitations
- Review current codes, versions, and patch levels

Recommend

- Provide recommendations to Pierce College on best practices for each area reviewed
- Provide feedback on operational improvements
- Facilitate further discussions on how to implement recommendations

Burwood Group Project Team

Erick Lee
VP, Western Region
Executive Sponsor

Aaron Wu
Sr. Project Manager
Project Leadership

Lauren Dunnevant
Sr. Consultant
Technical Leadership

Tom Howard
Account Executive
Client Engagement Manager

Mark Pingry
Managing Consultant, Managed Services
Processes SME

Larry Metzger
Managing Consultant, Western Region
Physical/Network SME

Melissa Baker
Principal Consultant
Staffing SME

Shaun Neal
Solution Architect
Client Champion

Scott Rohrer
Consultant
Security SME

Justin Smith
Solution Architect
Storage SME

Steve Bunnell
Consultant
Wireless SME

Work Stream	Burwood SME
Physical	Larry Metzger
Security	Scott Rohrer
Wireless	Steve Bunnell
Virtualization	Lauren Dunnevant
Systems and Services	Lauren Dunnevant
Active Directory	Lauren Dunnevant
Storage	Justin Smith
VDI and Thin Clients	Lauren Dunnevant
Email	Lauren Dunnevant
Disaster Recovery	Lauren Dunnevant
IT Process	Mark Pingry & Melissa Baker

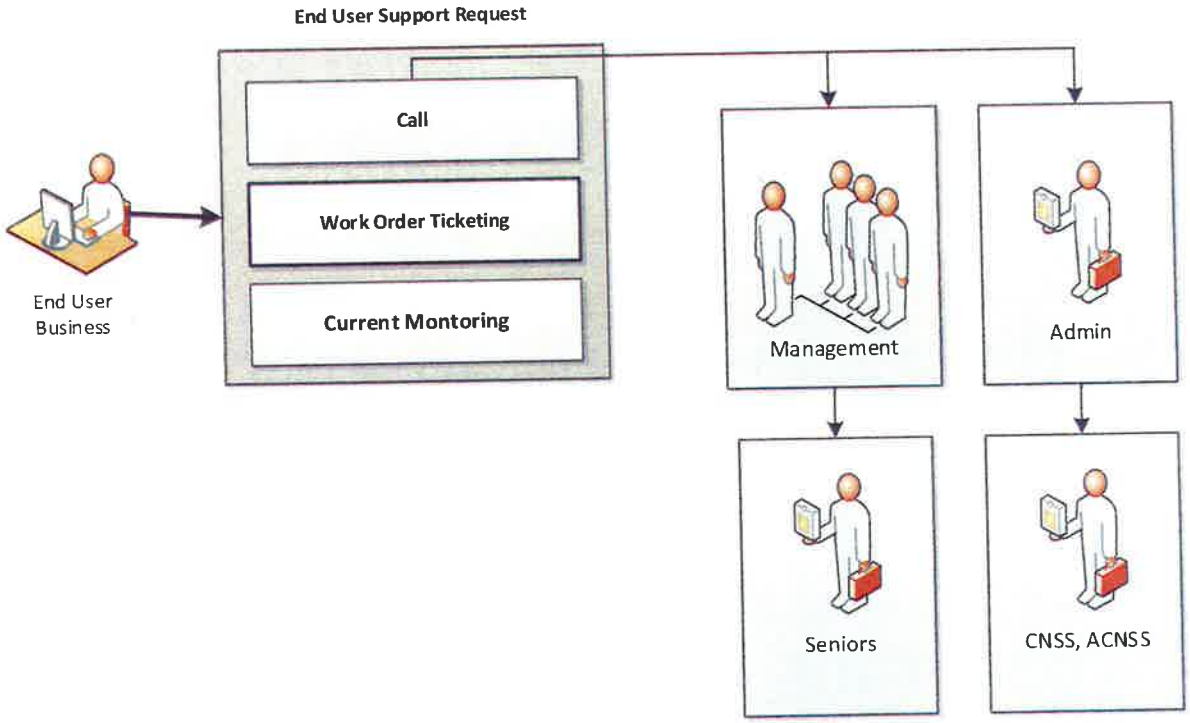
Summary of Findings

Operations

Top 10 Positive Findings

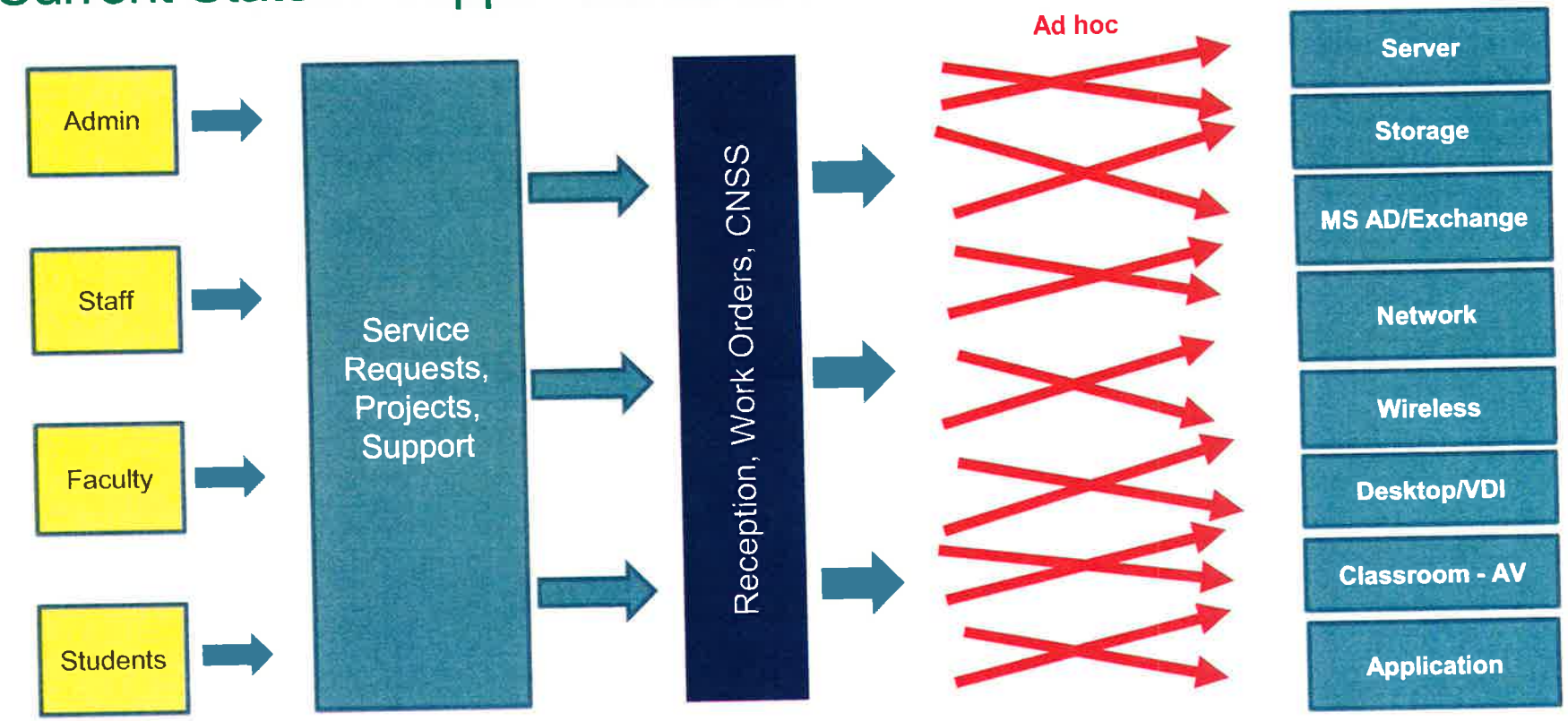
1. Entire IT Team, Union and Faculty provided open and candid responses during the assessment
1. IT team has adequate skill and experience to provide required IT support services
2. IT team is reviewing options to improve system tools, operations and services
3. IT identified operational improvements and have reported them to the Tech Advisory Committee
4. IT team does provide a high level of service resolving issues and requests once engaged
5. IT team regularly provides services after hours to address IT operational issues and outages
6. Faculty and Staff are aware of the infrastructure concerns and engaged with IT to develop resolution
7. Faculty indicated willingness to participate in improving IT services and support
8. Underlying IT organizational framework in place
9. IT and Faculty willing to participate in technical committees, planning sessions to improve services
10. IT willing to invest to improve services and operations

Current IT System Design

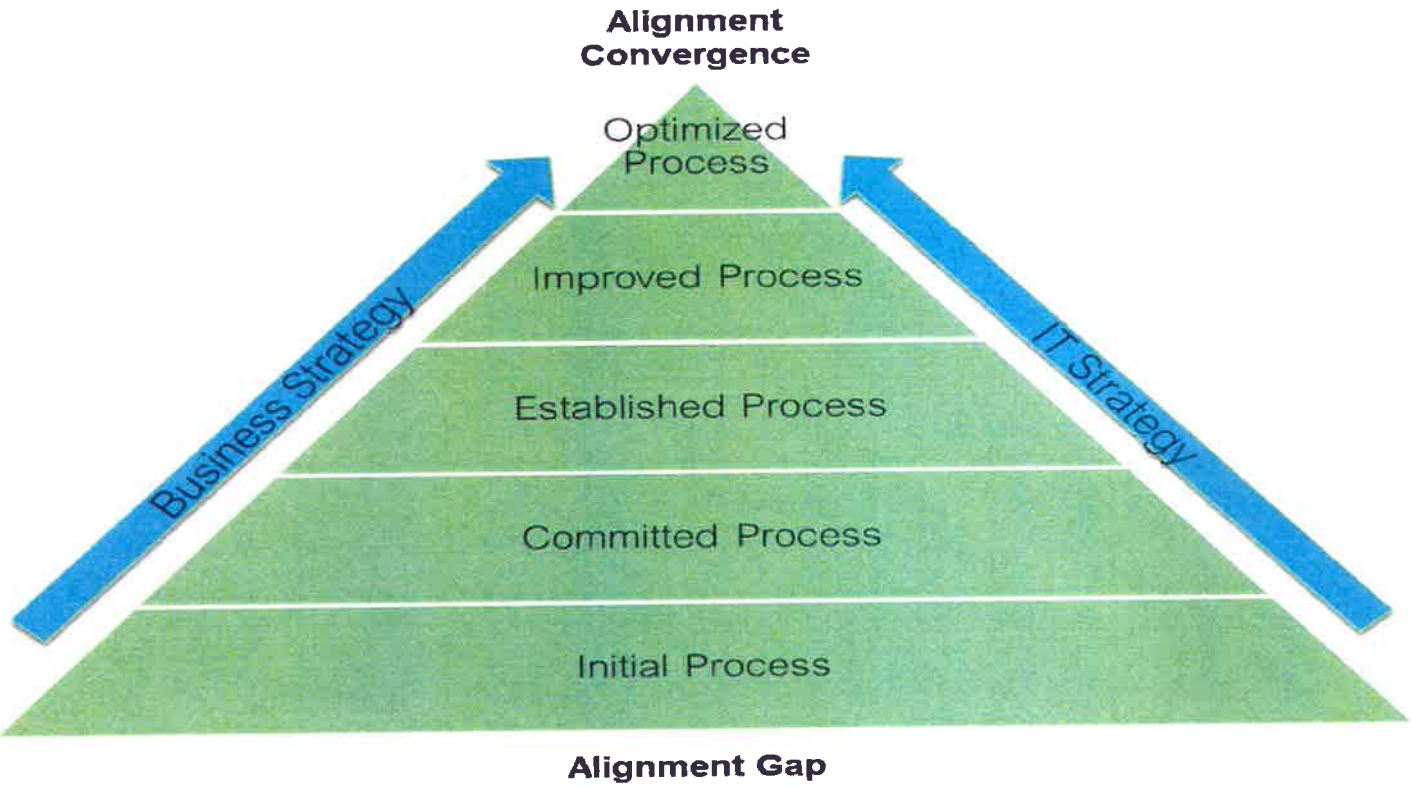


- Numerous inputs to IT to request support. (Call and Ticketing)
- Manual notification and escalation of infrastructure issues and outages.
- Limited Monitoring – Limited visibility of infrastructure performance issues or outages – reactive state
- Limited IT staff to respond and manage volume of calls and requests
- No documented process or procedures, support documentation for training and reference.

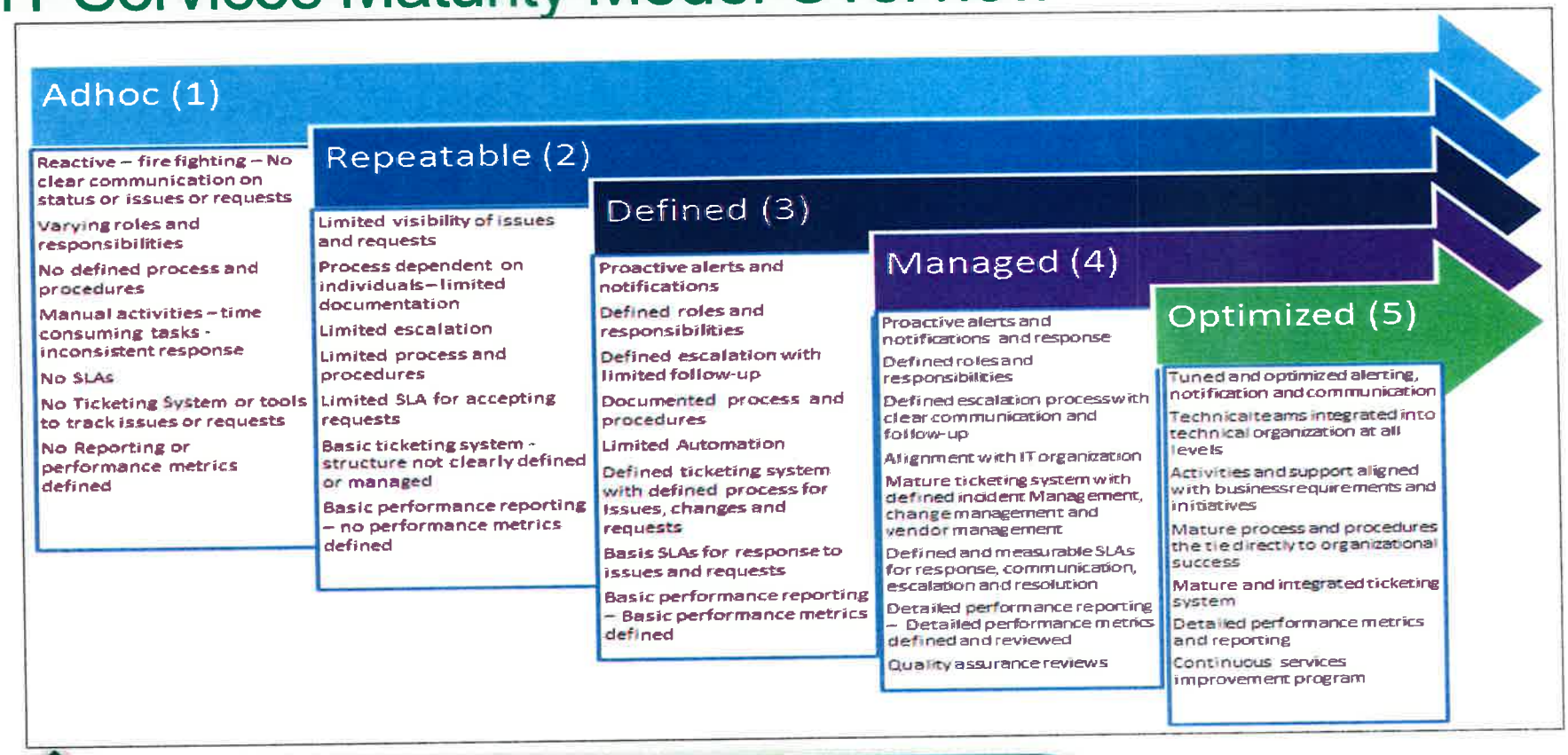
Current State IT Support and Services Workflow



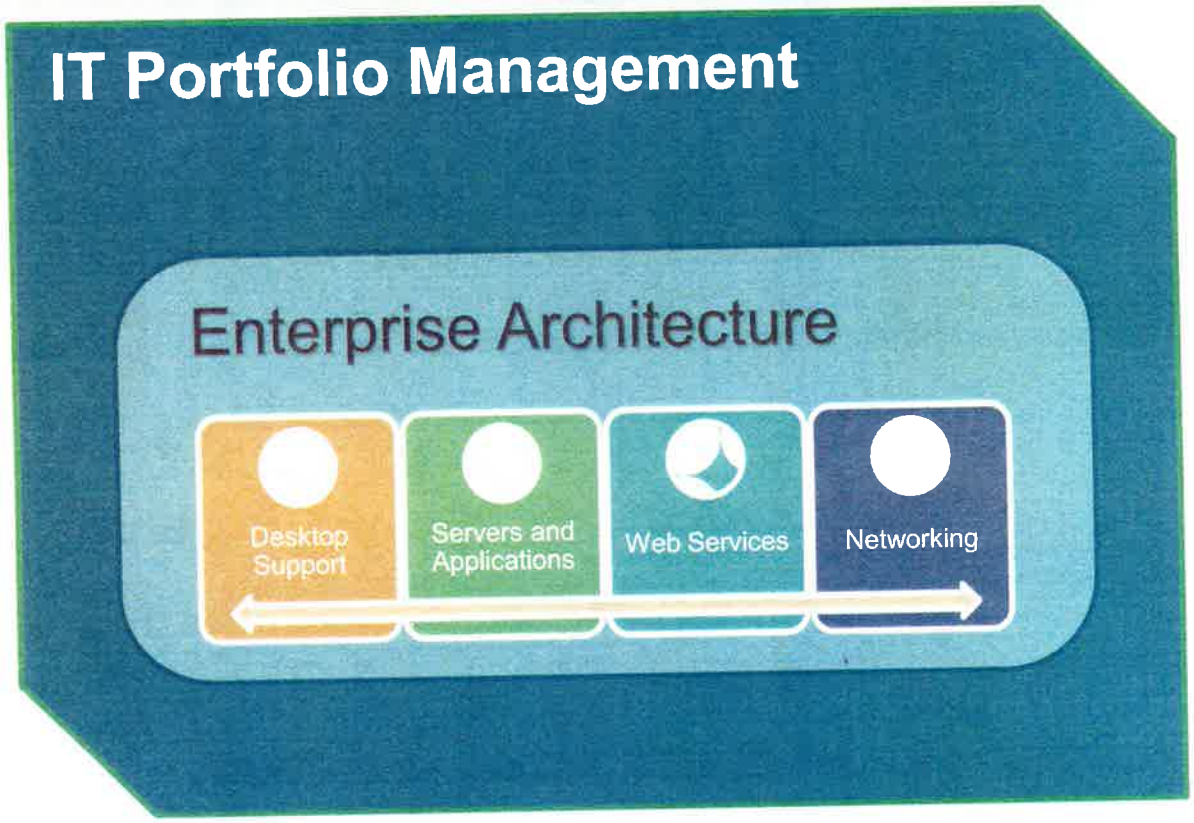
IT Alignment Maturity



IT Services Maturity Model Overview



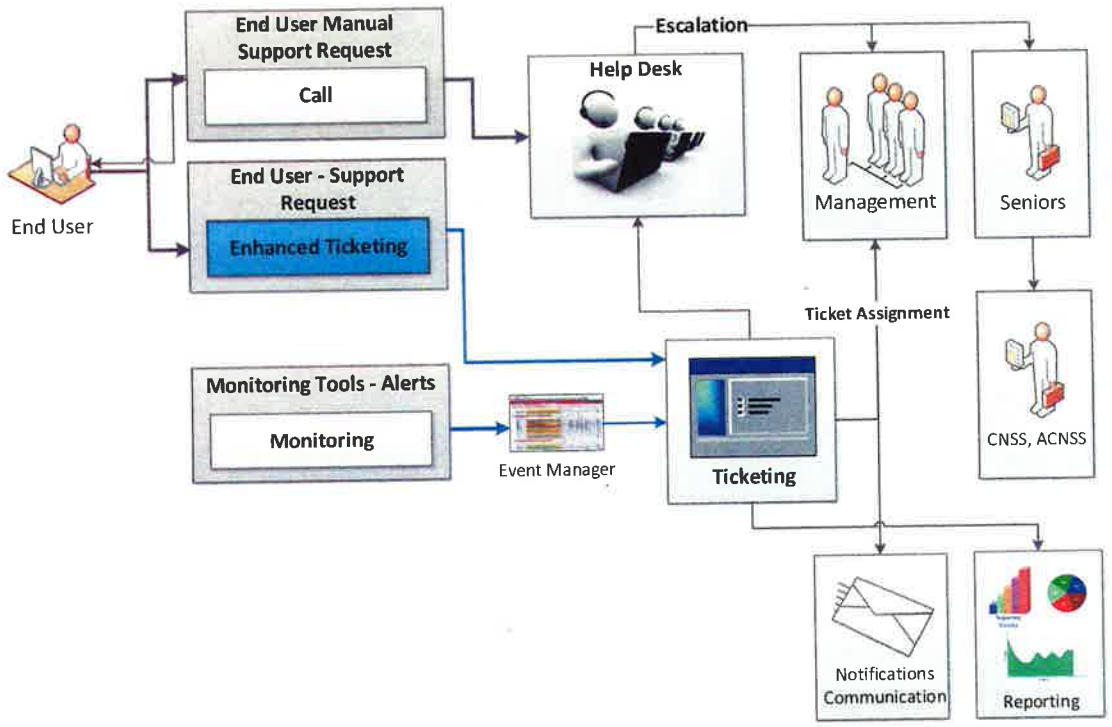
IT Portfolio Management



Functional Recommendations

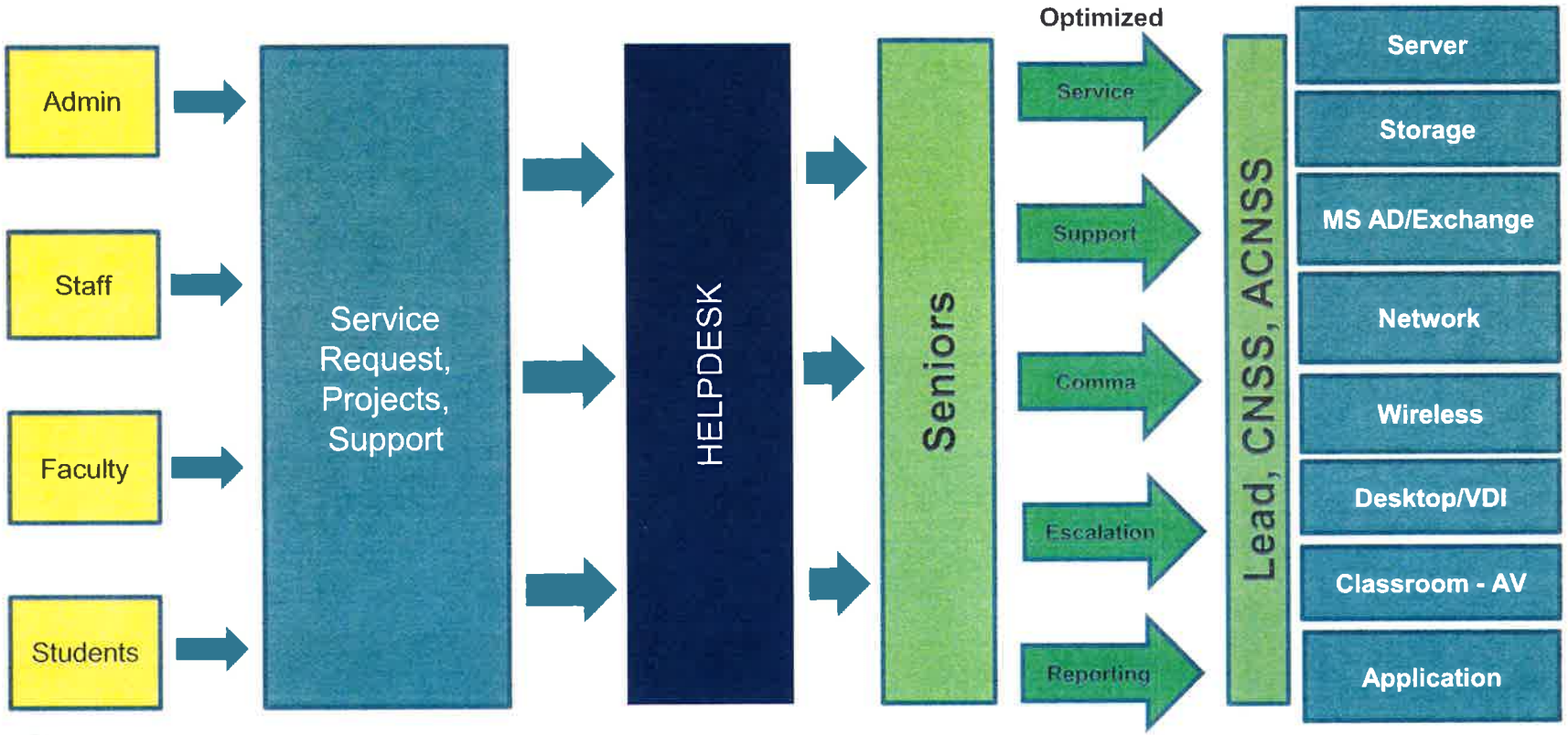
- IT Portfolio Management
- Enterprise Architecture
- Escalation
- Associate Training

Proposed IT System Design



- Customer input controlled through improved process and procedures
- Improved communication and end user interaction with IT systems
- Improve resource management and planning based on ongoing IT performance analysis
- Monitoring allowing better visibility into Infrastructure performance and availability
- Improved reporting for data analysis, trending, demand and capacity planning
- Improved customer satisfaction

Recommended IT Service and Support Workflow



IT Improvement Recommendations

- Start with a phased approach to improvements
- Determine what is realistic based on data, budget and resources
- Determine changes, design requirements and investment

Summary of Findings

Technical Assessment

Reporting Legend

- Issues are ranked **High**, Medium, and **Low** severity, please note that low severity items are still important, but may not be urgent
- Audit area refers to a specific segment within a focus area of assessment
- ID# refers to the specific technology, severity and issue found
  - Format example: NET01-H is Network Assessment Issue #1 High Severity

ID	Audit Area	Risk	Findings	Impact	Recommended Action
PHY01-H	Physical & Logical Network	High	Network design does not follow best practices.	Network performance issues and lack of scalability.	Create a network design that follows best practices. The design should be comprehensive from network layout to device configuration requirements and security considerations.
PHY02-H	Power	High	Most network closets do not have uninterrupted power supplies.	Power outage or brown outs can cause loss of phone functionality and delays in restoring network functionality after power returns.	All network devices should be supplied through UPS.
PHY03-H	Cooling	High	MPOE has temporary cooling. No locations have monitoring.	Insufficient cooling can cause damage to network equipment and cause unnecessary downtime.	Implement monitoring solution to get notification prior to failure. Provide sufficient cooling in primary locations.
PHY04-H	Cabling	High	Student Services building is connected with aerial fiber that is not properly terminated.	Cabling is compromised and causing unnecessary outages.	Install proper fiber cabling and terminate on a patch panel or fiber box.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
NET01-H	High Availability	High	The PA-4020's are in HA configuration however Link or Path Monitoring has not been setup for failover.	Hardware failures will result in extended downtime	Enable Link or Path monitoring for failover between the pair of PA-4020's.
NET02-H	Security Policies	High	Security Objects not applied to many of the PA-4020 security policies	Not attaching security objects means that IPS, AV, AS, and Vulnerability protections are not in place	Attach security objects to all of the security policies
NET03-H	SNMP Enabled on Perimeter	High	SNMP access is allowed vis outside interfaces	Potential for someone to obtain read/write strings on the outside	Create multiple Interface Management profiles, apply more strict profile on outside interface

ID	Audit Area	Risk	Findings	Impact	Recommended Action
WIFI01-H	Number of SSIDs (VSCs)	High	There is a total of 11 SSIDs for this network. 'Best Practices' recommends a maximum of 4-6.	Each SSID that is broadcast creates overhead traffic on the network. Increased overhead will slow the network down.	Group similar clients under a single SSID. Delete or disable any unused SSIDs.
WIFI02-H	WLAN client secure access	High	WPA/AES and pre-shared keys (PSK) are used on all SSIDs in this network.	PSKs are easily shared among students and staff allowing for possible unauthorized access. Unless changed often past users can still have access to the network.	Use RADIUS and Active Directory for authentication for all student, staff and faculty SSIDs.
WIFI03-H	Controller Failover Plan	High	There are 2-MSM 765 controllers with a license total of 200 APs. Pierce-1 has a total of 40 licenses with 40 active. Pierce-2 has a total of 160 licenses with 53 active.	If Pierce-2 were to fail there is no place for the 53-APs to move to. These controllers have the ability to be 'teamed' which provides for redundancy and failover.	Investigate the steps needed to configure these 2 controllers in a 'team' and do the configuration needed to setup the failover redundancy. Licenses can be 'pooled' amongst the team members and can move to another controller in case of a failure.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
VIR01-H	Compute – Security	High	Firewall settings & TSM timeout settings	These settings can lead to an increased security risk by opening ports that aren't explicitly required. No timeouts for Tech Support Mode can lead to unauthorized access.	Review firewall settings to validate all rules are needed. Enable TSM timeouts and configure a value that will not disrupt workflow.
VIR02-H	Network – High Availability	High	Lack of redundant network paths	This is a single point of failure within the environment and can cause an outage in the event of hardware failure.	Verify that there is redundancy in networking paths and components to avoid single points of failure.
VIR03-H	Storage – High Availability	High	Inconsistent storage path configuration, Virtual machines on local storage	Availability and manageability of storage is affected. VMs may not be recoverable in the event of a hardware failure.	Minimize differences in storage paths between hosts. Leverage shared storage for VMs for improved availability of resources.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
VIR04-H	VMware – Monitoring	High	No monitoring solution in place within current environment	Troubleshooting is more difficult and time consuming, reactive to issues, and no alerting	Assess monitoring solutions available for VMware based on requirements.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
SYS01-H	DHCP	High	Current DHCP is not stable or reliable	DHCP is a critical network service on which many other services rely	Replace with Windows Server 2012 R2 DHCP integrated with Active Directory.
SYS02-H	DHCP	High	Single DHCP Server on Windows Server 2003	This represents a single point of failure within the environment and the operating system is no longer supported so is at a greater security risk.	Replace solution with two Windows Server 2012 R2 servers per domain environment with DHCP Failover in Active/Active configuration.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
AD01-H	Active Directory	High	Current design does not adhere to Microsoft best practices, domain controllers on unsupported OS, large amount of cleanup effort needed	Windows Server 2003 is no longer supported, performance impact, single points of failure	Re-Design of Active Directory environment
AD02-H	Active Directory	High	High number of Windows XP and Server 2003 in environment	These operating systems are no longer in support and are at an increased risk of security exploits and vulnerabilities	Replace existing Windows XP machines with Windows 7, address problematic applications, Upgrade servers to Server 2008 or higher

ID	Audit Area	Risk	Findings	Impact	Recommended Action
STO01-H	Storage Area Network	High	Inaccessible Fiber Channel switch	Cannot make changes to switch configuration	Identify a method to access this fiber channel switch for administration and configuration
STO02-H	Storage Area Network	High	Inconsistent SAN topology	Potential design and implementation issues	Define and configure a uniform physical and logical SAN design and configuration to provide consistent presentation to all hosts.
STO03-H	Storage Array	High	HP P2000 G3 MSA End-of-Life (EOL) on 2/27/2015.	Lack of vendor support	Remove the P2000 array from production use. Potential use of the hardware for test/development environments

ID	Audit Area	Risk	Findings	Impact	Recommended Action
VDI01-H	VDI	High	No antivirus on VDI images	Viruses can inflict damage and are a significant security risk	Install & configure antivirus on VDI images.
VDI02-H	VDI	High	No SQL Server high availability	Limited availability of VDI environment in the event of a server or database failure	Configure SQL Mirroring with a witness to facilitate automated failover
VDI03-H	VDI	High	Infrequent image updates	Virtual desktops are at an increased risk of security vulnerabilities and exploits	Improve management of VDI solution – consider 3rd party software, hosting options, or managed services.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
EM01-H	Email	High	Current email environment is not stable	Availability of email is not consistent and email issues occur frequently	Evaluate Office 365 as an alternative for an on premise Exchange solution.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
DR01-H	Data Protection	High	Limited backups, No data validation, No alerts, Non-standard backup systems in place (external drives)	Loss of data & extended downtime in the event of an outage or system failure	Schedule recurring backups for all systems and configure alerts & incorporate backup validation procedures within Disaster Recovery Plan
DR02-H	Data Protection	High	Lack of defined backup and recovery requirements or policy	Nothing to audit existing systems against	Define a backup and recovery policy
DR03-H	Facilities	High	No monitoring or testing of UPS Battery Backups	Loss of data & extended downtime in the event of an outage or system failure	Perform regular testing of UPS battery backups and configure alerts
DR04-H	Disaster Recovery	High	No Disaster Recovery Plan in place	Critical system downtime in the event of a disaster	Create a Disaster Recovery plan to incorporate: people, physical facilities, technology, data, and policies and procedures.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
PHY05-M	Physical Network	Medium	Cabling is unorganized and abandoned cables are left in place.	Troubleshooting issues is difficult and replacing failed equipment is impossible.	Replace patch cables with appropriate lengths and install with cable management following best practices. Ensure structured cabling is deployed following best practices.
PHY06-M	Physical/Logical Network	Medium	Unmanaged switches are used for control systems.	Unmanaged devices cannot provide the level of performance or security required by the organization.	Run cables to network switches and utilize appropriate infrastructure for control systems.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
NET04-M	Subscriptions	Medium	The PA-4020 subscriptions for URL, Threat and Support will expire on September 30th, 2015.	Both PA-4020's will lose functionality for URL and Threat Protection in the next two months.	Purchase and apply the PAN-DB URL-Filtering, Threat Protection and Support renewal.
NET05-M	Subscriptions	Medium	The PA-4020's do not have subscriptions for WildFire	WildFire helps to provide signature updates for zero-day or unknown malware	Purchase and apply the WildFire subscription
NET06-M	Interface Management	Medium	The PA-4020's can be managed by their Ethernet interfaces internally and externally	Management of the firewalls can be accessed externally although it is restricted	Disable management on the Ethernet interfaces and only use the out-of-band management interface with the VPN client
NET07-M	Administrators	Medium	All Local accounts are SuperUsers	Admin logins are local to each firewall and do not use third party authorization	Utilize RADIUS or LDAP for user level admin authentication
NET08-M	VPN Tunnels	Medium	Legacy encryption protocols are allowed	Weak encryption ciphers decrease the security of data across the VPN tunnel	Remove legacy ciphers such as 3DES from the crypto settings on the PAN firewalls and the remote peer
NET09-M	Security Policies	Medium	Many rules have never been used on the firewalls	Unused rules can provide unnecessary access to systems	Review and remove unused rules

ID	Audit Area	Risk	Findings	Impact	Recommended Action
WIFI04-M	RF Channel Plan on MSM422 and MSM430 access points	Medium	Controller Pierce-1 has 40-MSM422 and 1-MSM430 APs associated to it.	These APs are dual radio configurable by software. Both radios are currently operating on the 2.4GHz frequency band using non-standard channel numbers. This does not follow 'Best Practice" guidelines and can be the result of excessive co-channel or adjacent channel interference resulting in poor WLAN performance and client connection issues.	Investigate why both radios are set to be on the same frequency (2.4GHz). These are dual-radio access points. The radios are software configurable to can be set for either frequency.
WIFI05-M	Controller Firmware Version	Medium	The current version of firmware on both controllers is 6.2.1.0.17104	Depending on the age of the controller it is generally recommended to keep current on firmware versions as bugs are found and corrected in these updates.	The latest version of firmware for these controllers is 6.5.0.1. The controllers will first need to be upgraded to 6.2.1.1 and then to 6.5.0.1.
WIFI06-M	RF Channel Plan	Medium	Will investigating all of the APs it was observed that the 5GHz radios are using UNII-1, UNII-2, UNII-2 extended and UNII-3 channels.	Some of the channels in the 5GHz channel rotation are DFS channels which have to co-exist with radar. 'Best Practices' suggest not using these channels for this reason. Also some clients cannot use these channels.	Remove these channels from the channel line-up.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
WIFI07-M	RF Power Plan	Medium	All of the radios on both frequencies are operating at full power.	Current 'Best Practices' recommends running radio power levels at a lower level to match client transmit level. This improves client connectivity and roaming. Also, if an AP were to fail there is no overhead from other APs to fill in the coverage gap created by the failure.	No coverage heat maps are available for this WLAN in order to observe the RF coverage in the campus buildings. It has been stated there have been passive surveys completed in the past but no one has access to them. In order to tune-up the WLAN it is recommended to conduct a complete survey to determine the levels of coverage and identify any gaps in coverage.
WIFI08-M	Data Rates	Medium	Lower data rates of 1, 2,and 5.5 are activated on 2.4GHz and 6 & 9 on 5GHz.	'Best Practices' suggests shutting off these 'legacy' data rates. Overhead traffic will choose the best possible data rate, which is generally also the lower data rate. This traffic, at low rates, will greatly affect the performance of the network. The legacy data rates must be left on if there are 802.11b clients accessing the network.	Disable data rates of 1, 2, 5.5 on the 2.4GHz radios and 6 and 9 on the 5GHz radios.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
VIR05-M	Network – Performance	Medium	Exceeded maximum threshold for NIC ports, Inconsistent portgroup config, inconsistent switch settings	Performance degradation. Inability to leverage features such as vMotion or DRS for hosts with inconsistent settings.	Configure network settings consistently across hosts in cluster.
VIR06-M	Network – High Availability	Medium	Portgroups pair together NIC ports on the same physical NIC	This is a single point of failure since physical failure of the NIC would cause an outage.	NICs should be teamed between separate physical NICs for improved redundancy.
VIR07-M	Storage – Performance	Medium	Limited use of Storage I/O Control (SIOC) & Lack of separation for storage network	Performance can be impacted by unfair distribution of resources & contention of resources.	Enable SIOC and separate storage network from regular traffic for Management network.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
VIR08-M	Datacenter – Security	Medium	Misconfigured authentication settings & vCenter permissions	Man-in-the-middle attacks are possible with the current authentication settings. vCenter permissions can allow unauthorized access to the environment.	Avoid using built-in Windows groups for vCenter security. Enable bidirectional CHAP authentication for iSCSI traffic so that CHAP authentication secrets are unique.
VIR09-M	Datacenter – Performance	Medium	Retention policies not configured, Inconsistent memory settings	Increased vCenter database growth without retention policies. Inability to leverage vMotion, DRS, HA, etc.	Enable retention policies. Ensure consistent configuration of memory between hosts.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
VIR10-M	Virtual Machines – Performance	Medium	Not using optimized network driver, Long term use of snapshots and VMware tools not up-to-date	Network performance may suffer with older drivers. Snapshots are meant to be temporary and can cause performance degradation over time. Management capabilities are more limited without VMware tools.	Leverage the VMXNet3 driver wherever possible to improve network performance. Limit the use of snapshots and remove unneeded snapshots. Ensure that VMware tools is installed on each virtual machine and are kept up-to-date.
VIR11-M	Virtual Machines – Security	Medium	Possible security vulnerabilities within current configuration	Increased attack surface due to unneeded features.	To improve security, limit sharing console connections and disable certain unexposed features.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
VIR12-M	VMware – Strategy	Medium	Lack of upgrade strategy and virtualization initiative incomplete	Limited planning can result in reactionary measures when products are no longer supported. Physical servers cost more to manage, take up more space, and are less efficient than virtual servers.	Define upgrade strategy and identify physical servers that are good candidates for virtualization and plan migration to virtual platform.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
SYS03-M	DNS	Medium	Single forwarder configured	DNS only has a single forwarder configured on all 3 DNS servers, however, failover to root servers is configured to limit risk.	DNS should be configured with a minimum of 2 forwarders for improved resiliency
SYS04-M	DHCP	Medium	Scavenging intervals are set too high	Scavenging intervals are currently set at 7 days for the no-refresh interval and 7 days for the refresh interval. This means that records could persist for 14 days before being deleted. Since DHCP lease times are set to 10 hours, this can have the undesired effect of maintaining stale records and manual deletion of records may be needed.	Adjust scavenging intervals to times closer to the DHCP lease time (i.e. 15 hours or 1 day). Pierce should thoroughly test these settings prior to implementation to ensure that undesired effects do not occur.
SYS05-M	DNS	Medium	Scavenging not enabled on DNS servers	Although scavenging is configured on DNS zones, the servers do not have it enabled so it is not currently in effect at all.	Enable scavenging on DNS servers

ID	Audit Area	Risk	Findings	Impact	Recommended Action
AD03-M	Active Directory	Medium	Ineffective password policies	Most password policies do not take effect due to accounts configured with 'Password never expires'. Passwords can be used indefinitely. No complexity requirements. Relaxed account lockout policies. These all lead to a more vulnerable and less secure environment.	Revise existing password policies and ensure that they are in line with security requirements and best practices.
AD04-M	Active Directory	Medium	Large number of inactive user and computer accounts exist within the environment	Users who are no longer authorized could still gain access to resources	Disable and remove unneeded user accounts. Define a process for the de-provisioning of user and computer accounts.
AD05-M	Active Directory / Asset Management	Medium	No centralized management of computers or servers. Inconsistent imaging processes.	Currently, there is no ability to centrally deploy updates to desktops and servers within the environment. Additionally, there is no hardware or software inventory management in place. Multiple imaging solutions are in place and lead to inconsistencies with builds.	Improve management and maintenance of devices by leveraging Microsoft System Center 2012 R2 for hardware/software asset management, patching of devices, and OS imaging and deployment.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
STO04-M	Storage Array	Medium	EMC Reconfiguration Requirements	Design and configuration does not follow best practices	Identify a new storage device to use as a temporary location for production data. Reconfigure EMC and use new storage array for dedicated VDI or server resources
STO05-M	Storage Area Network	Medium	Separate VDI onto dedicated storage	VDI has different I/O requirements than Server based workloads and performance can be affected.	Consider the purchase of a separate storage solution dedicated to VDI.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
VDI04-M	VDI	Medium	Image sprawl	VDI images are inconsistent and consume additional storage. Solution becomes more difficult to manage.	Consolidate & optimize VDI images.
VDI05-M	VDI	Medium	VDI configuration issues – high performance applications, disk space, permissions, and vCPU on desktops	Performance degradation of the VDI solution, inconsistent end user experience, lack of security	Remediate configuration issues.
VDI06-M	Thin Clients	Medium	No management of thin clients	Thin clients are susceptible to viruses, malware, and security vulnerabilities.	Improve management of thin clients by leveraging SCCM 2012 R2 or upgrading to HP Thin Pro

ID	Audit Area	Risk	Findings	Impact	Recommended Action
EM02-M	Email	Medium	Exchange 2003 Servers still exist within the environment	Operating system is no longer supported. Servers do not provide required services.	Decommission all Exchange 2003 Servers.
EM03-M	Email	Medium	Alerts are not configured for backup	Administrators are not alerted to issues that may require their attention	Enable and configure alerts within the HP Data Protector application.

ID	Audit Area	Risk	Findings	Impact	Recommended Action
DR05-M	Data Protection	Medium	No offsite storage of backups	Inability to restore data in the event that the network location for backups is unavailable or in the event of a disaster affecting the Los Angeles area	Define critical services within the Disaster Recovery Plan and evaluate options for offsite storage of backups
DR06-M	Facilities	Medium	Limited monitoring of datacenter	Not alerted to environment changes such as temperature, water, smoke, etc. Unauthorized datacenter access. Increased chance of theft of equipment.	Improve physical security of datacenter. Implement datacenter monitoring solution.
DR07-M	Disaster Recovery	Medium	No secondary datacenter	Critical systems will not be available in the event of a disaster affecting the Los Angeles area	Define critical services within the Disaster Recovery Plan and evaluate strategy for data center location(s).