CITY OF
WASILLA
• ALASKA •

	Presented
Date Action Taken:	3/24/2014
Other:	
Verified By:	

CITY COUNCIL INFORMATIONAL MEMORANDUM

IM No. 14-05: Information Technology Assessment Report to Council prepared by Moss Adams LLP, dated February 12, 2014.

Originator: Troy Tankersley, Finance Director
Date: 3/6/2014 Agenda of: 3/24/2014

Route to:	Department Head	Signature	Date
X	Finance Director		3/12/14
X	Deputy Administrator		3/12/14
X	City Clerk		3/12/14

Reviewed by Mayor Verne E. Rupright: ____________________

Attachments: "Final Report for City of Wasilla Technology Assessment", dated February 12, 2014, 28 pages.

Summary Statement: Through the following legislative documents:

RFQ 0520-0-2013/AD Independent Audit/Assessment of Information Technology, and

Ordinance No. 13-28 An ordinance of the Wasilla City Council amending the Fiscal Year 2014 budget by appropriating $41,592 from the Technology Replacement Fund, Fund Balance, as an appropriation to Moss Adams for the purpose of an IT review, security testg, and summary report to Council, and

Action Memorandum No. 13-32 Authorization to award a contract to Moss Adams in the amount of $41,592 for the Independent Audit/Assessment of the City of Wasilla's IT Infrastructure, and

Moss Adams LLP, Certified Public Accountants and Business Consultants have completed their independent review of the City's information technology infrastructure and have respectfully submitted the attached report for City's records.

FINAL REPORT FOR

CITY OF WASILLA

TECHNOLOGY ASSESSMENT

February 12, 2014

Prepared by:

Moss Adams LLP

999 Third Avenue
Suite 2800
Seattle, WA 98104
(206) 302-6500

MOSS-ADAMS LLP

Certified Public Accountants | Business Consultants

Acumen. Agility. Answers.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Moss Adams LLP ("Moss Adams") was engaged by the City of Wasilla ("the City") in October 2013 to conduct an information technology assessment that focuses on improving the IT operations that help to further the business objectives of the City. In addition, the team assisted the City with development of its request for proposal (RFP) for an outsourced IT support vendor. To this end, the Moss Adams team conducted fieldwork over four days in mid-October where several interviews, walkthroughs, and system observations took place. To ensure that a comprehensive perspective on IT operations was provided by the City, the Moss Adams team interviewed the City's sole IT Technician, the TekMate System Administrator, and various department representatives throughout the City.

A critical component of this study was gaining an initial understanding of the current state of technology at the City. While we found that each of the City's departments had specific application needs (e.g., work order functionality and document management), we found that the City's immediate need for improvement is in the foundational aspects of running optimized IT operations. To start, Moss Adams reviewed the various network components, server and workstation hardware, connection types, and the essential infrastructure-related software that was necessary for an optimal technology environment. We also reviewed essential functions around anti-malware protections, data backup and restoration strategy, software updating, security management, and physical/environmental controls. After obtaining sufficient understanding of the City's practices in these areas, Moss Adams gauged and assessed how the City was following best practices stemming from industry-accepted best practice frameworks such as IT Infrastructure Library (ITIL), ISO/IEC 27001/2, and PCI DSS, among others. In assessing the current IT situation at the City, we also drew from the team's collective experience from working on similar types of assessments at municipalities of similar size and complexity as Wasilla.

The following section, "IT Assessment," encompasses Moss Adams' understanding and assessment of the City's IT operations. The section is categorized into the following areas:

- Network Infrastructure
- Server Environment
- Applications
- Workstation and Mobile Devices
- Antivirus and Data Leakage Protection
- Backup, Restoration, and Disaster Recovery
- Security Management
- Incident Response
- Asset Management
- Physical and Environmental Controls

For each of these areas, we noted the following most-critical projects that the City should undertake to bring it in line with its peers:

1. Move Internet-facing systems to the DMZ.
2. Implement infrastructure updating/patching system.
3. Implement a more robust and secure wireless network.
4. Create and implement a server patch management policy.
5. Implement a virtualized solution for workstation and server infrastructure.
6. Implement Naviline security improvements.
7. Configure McAfee Antivirus to conduct regularly scheduled malware scans.
8. Replace Windows XP workstations with Windows 7 workstations (or upgrade systems)
9. Configure and deploy enforced antivirus updates.
10. Standardize on a sole backup management solution.
11. Create and institute a new hire/terminations checklist.
12. Develop a disaster recovery plan.

Most of these recommended projects do not cost additional funds, and only require enabling functionality within a system, instituting a formal process, or making a configuration change. However, minor as they seem to be, they are basic, essential practices for an operating and maintaining an IT Department.

In the next section, details around these recommended projects is provided, along with estimated costs and approximate man hours involvement in terms of high, medium, and low.

II. IT ASSESSMENT

A. IT DEPARTMENT MANAGEMENT

1. Current Situation

Wasilla's IT Department consists of the IT Technician, who is a full-time employee, and a contract System Administrator from TekMate, the City's outsourced IT support vendor. Both have been working at the City for several years (four and nine years respectively), with the System Administrator focused primarily on supporting the Police Department and the IT Technician supporting the other departments throughout the City. The IT Technician reports directly to the Mayor.

The IT Department appears to work almost exclusively in "break-fix" mode. That is, the IT Technician's time is mainly spent tending to end-user support issues and technical support requests. As a "one-man shop," the IT Technician leverages remote desktop tools and online resources to effectively assist end users with issues they are having with their workstations, connectivity, applications, and the like.

The annual budget for IT has been relatively flat from 2011 to 2013, averaging approximately $252,000 per year, or roughly 1.8% of the City's general fund. As a result, IT has been operating in maintenance mode with funds for special projects or major changes largely dependent on grant money.

2. Assessment

The City appears to be maintaining the status quo with its technology operations, and the activities of the IT Department reflect this objective. The IT Technician and System Administrator have only worked to maintain the City's network, systems, and end users in the current state given limited resources. In maintaining status quo, the City will be unable to further mature and advance its technology environment if it stays the course.

It is expected that the IT Technician is attuned to the needs of end users, and ultimately, the business needs of the City when it comes to technology; however, in the current "break-fix" state, the IT Technician and System Administrator have not provided the insight and perspective that the City needs in order to be proactive with technology projects that will benefit and enhance the City's service delivery to its citizens and other stakeholders. The IT Department requires forward thinking about technology and the business savvy to understand when technology can serve as a solution to issues the City faces in its day-to-day operations.

One suggestion is for the City to have an IT Director in place to provide the balance of technology understanding with the perspective of a business manager. In addition, the IT Director would be tasked with managing the IT Department and its staff, as well as providing motivation and a career path for them. Whether the IT Director role is assigned to an existing staff within the City or acquired from external hiring, the IT Director role can help to provide the technology leadership, proactive management, and foresight in its IT Department.

In addition to supporting technology to meet an organization's business objectives, an IT department's charter is to provide vision and thought leadership about the ways technology can help further an organization's mission and better serve its stakeholder community. Currently, the City does not have such a charter. In the current maintenance mode in which the IT Department is operating, there is very little chance that the network will be optimized, system performance will improve, data security will be enhanced, and newer technologies will be implemented in a timely manner. As a result, the IT Technician is consumed with technical support requests rather than working on new technology implementation/improvement projects and having time for forward thinking. In addition, the lack of regular technical training for the IT Technician can result in stagnation and lack of innovative thinking around the technology environment.

The City may need to look at hiring an in-house System Administrator as a FTE. The System Administrator should have experience working in larger, more complex IT environments that he/she has had a role in helping to grow. With the City in growth mode, IT needs to advance as well with the pace of growth. Having new IT staff onboard with more advanced skills than the IT Technician and contract System Administrator may provide the proactive planning, alignment with best practices, and advanced implementation skills that are needed and result in a more optimized network and systems that are poised for growth. Once an in-house System Administrator is in place, the City may consider terminating the ongoing contract with TekMate and utilize in-house IT staff exclusively. Having an in-house System Administrator would also help to address issues over data control and access authorization.

Like other municipalities similar to Wasilla, department budgets are "razor thin" and heavily scrutinized. However, cities that desire to maintain an up-to-date technology environment ensure that IT budgets keep pace with the current requirements for business. This is not to say that cities need to be on the "cutting edge" of technology, but they need to ensure that an adequate amount of the general fund is allocated to improving the state of technology use within the city. In surveys conducted by Moss Adams on similar engagements, we have noted that on average, a city spends 3.2% of the general fund on the IT budget. In Wasilla, that 1.4% increase easily translates into nearly $202,500 that could be used for continual technology improvements.

3. Potential Projects

One of the first solutions for addressing the IT Department's lack of direction is for the City to have a strategic technology plan. While an IT plan was developed in 2011 by the IT staff, it was never formally approved and adopted, and was more akin to a project list. A strategic technology plan is a formal document that serves as a roadmap for the way the City should spend its limited IT budget over the next three- to five-year time horizon. The plan would provide a vision for the IT Department to aspire toward, and it would establish a plausible charter. It would also help to position desired and necessary technology projects over the next several years for budgeting purposes. Whether developed by in-house staff or through the use of external consultants, the strategic technology plan would serve as the "go-to" guide for making technology decisions, and it would ensure that those decisions are aligned with the overall business strategy and objectives of the City. Once in place, the plan needs to be referred to regularly to ensure alignment and tracking of progression.

In addition to development of a strategic technology plan, a training plan for the IT Technician should be established. Providing regular training opportunities to IT staff can boost staff morale, serve as a performance incentive, trigger innovative thinking, and ultimately result in improved IT operations. Training can come in many forms such as conferences, instructor-led training at a technical education center, one-day summits, and web-based training resources. Because it has been several years since the IT Technician received training, the City should consider sending the IT Technician to a training conference such as Microsoft Tech Ed. At such a conference, the IT Technician can receive advanced training on Windows-based platforms and have the opportunity to learn about new technologies that could benefit the City. In addition, conferences provide the opportunity for the IT Technician to network and learn from peers and industry experts.

Acquisition of an in-house System Administrator would be a near-term project for the City to consider. The process would involve (1) development of the job description and requirements, (2) identifying the most plausible job search sites for posting the job advertisement, (3) posting the ad for a couple of weeks, (4) screening potential candidate resumes, (5) conducting a series of interviews (technical and non-technical), and (6) making a decision on the most viable candidate. The System Administrator should have experience in the following areas: network management, Windows Server administration, Active Directory administration, email system administration, SQL Server database knowledge, and data security.

Assignment or acquisition of an IT Director at the City is something that the City will need to consider in the next three to five years after the IT environment has been stabilized and improved to meet current needs. While leadership in IT is truly needed, there is much to do at the moment with instituting basic policies and procedures in place, along with needed technology improvements. As such, the City is not in immediate need of a "technology visionary" but more in need of an individual who can bring tangible technology improvements and ideas. This can be found in an experienced System Administrator.

4. Project Name

- Development of a strategic technology plan
  - Estimated cost: $0 (if developed in-house) to $25,000 (if external consultants are used)
  - Estimated man-hours: high
- Establish a training program for IT staff
  - Estimated cost: $5,000 annually
  - Estimated man-hours: low

- Acquire an in-house System Administrator
    - Estimated cost: $60,000 - $80,000 annually
    - Estimated man-hours: high
- Assign or acquire an IT Director
    - Estimated cost: $90,000 - $110,000 annually
    - Estimated man-hours: high

B. NETWORK INFRASTRUCTURE

1. Current Situation

Wasilla's network environment is comprised primarily of Foundry, Cisco, and HP equipment with a WatchGuard perimeter firewall. Matanuska Telephone Association (MTA) provides a 10Mbps down/2Mbps up DSL connection to the Internet. From the Police Department, 14 site-to-site MTA links provide network connectivity to other City facilities that extend services such as Voice over Internet Protocol (VoIP), network services, and Internet connectivity. The Police Department also provides network connectivity to City Hall via a 20MB full-duplex fiber link, which is also leased from MTA. Additionally, the Police Department maintains a private RF network used for providing connectivity to mobile data terminals located in the City's patrol vehicles.

2. Assessment

Because of the limited number of communication providers available in Wasilla, the City has few options for Internet Service Providers (ISP). The City has a single 10Mbps DSL link that provides Internet access to the PD, City Hall, and a few of the site-to-site MTA links. Many users complain about network connectivity issues, which likely stem from the limited connection speed. For example, users at the Library indicated they were having problems with their VoIP connectivity such as voice clarity issues and frequent dropped calls. Additionally, we noted that the network was not configured to utilize quality of service (QoS) functionality, which prioritizes certain types of traffic over regular network traffic. Balancing network traffic over the 20Mb fiber link between the Police Department and City Hall has been another challenge for IT because the server room is located in the Police Department facility while a majority of the network users reside in City Hall.

It was also noted that that a demilitarized zone (DMZ) was not being utilized off the WatchGuard firewall for Internet accessible systems. Since the City hosts several Internet-facing systems such as OWA, Sire Production, Terminal Services, and Virtual Private Network (VPN) access, Internet traffic is forwarded to the internal network rather than isolated in a separate network off the firewall. If an attacker compromised one of the Internet-facing systems, it could be used as an attack platform for the rest of the network. Additionally, a terminal server is housed within a Windows 2000 server that reached End-of-Life (EoL) on July 13, 2010. As a result, Microsoft no longer provides security updates to the Windows 2000 operating system, which means that critical security issues are not addressed quickly. Because the operating system has been outdated for over three years, it is often targeted by hackers since there are several relatively easy exploits that can compromise the system. Additionally, the server only requires users to authenticate with their Active Directory (AD) credentials rather than requiring multi-factor authentication. Multi-factor authentication requires users to provide extra information for authentication such as a knowledge factor, a possession factor, or an inherence factor. The City uses legacy small office home office (SOHO) wireless access points that are unable to properly encrypt traffic. Furthermore, during the onsite visit, MAC address security was being utilized, which can easily be compromised by an attacker monitoring wireless traffic. IT should leverage additional built-in security functionality in the access points, particularly WPA2, for an additional layer of defense. Finally, IT does not have procedures in place to ensure network infrastructure devices are updated with the latest firmware/software versions. These updates are critical because they address potential security and stability issues.

3. Potential Projects

Projects should be aligned and prioritized to ensure the confidentiality, integrity, and availability of network services. Therefore, priority should be given to gaps that pose a security risk to the City such as moving Internet-facing servers to the DMZ, removing the unsupported Windows 2000 terminal server from the network, and ensuring the infrastructure devices are properly updated.

Secondary focus should be placed on improving network stability and speed by implementing QoS, prioritizing VoIP traffic, and considering implementation of a network optimization appliance. Network optimization can help the City reduce latency, relieve network congestion, and speed up bandwidth-hungry applications. Riverbed and Akamai make appliances that can provide data compression, data reduction (by locally caching frequently accessed data), optimization of large data transfers, QoS, and packet coalescing (combines data packets rather than re-transmitting similar information). Since the City cannot increase the data rate between the Police Department and City Hall, this solution could improve network performance.

4. Project Name

- Move Internet-accessible systems off the WatchGuard firewall to the DMZ
    - Estimated cost: $0
    - Estimated man-hours: medium
- Remove the Windows 2000 Terminal Server from the network and utilize the WatchGuard VPN for all users
    - Estimated cost: $0
    - Estimated man-hours: low
- Implement multifactor authentication for the WatchGuard VPN
    - Additional multi-factor authentication can be implemented on the WatchGuard VPN such as SMS-based tokens and one-time passwords (OTP)
    - Estimated man-hours: medium

  - Estimated cost: $0–$3,000 (depending on the availability of server hardware for RADIUS)
- Implement infrastructure update/patching procedures
  - Estimated cost: $0/$2,500–$7,500 (based on vendor)
- Implement QoS on network devices to ensure the reliability of network services
  - Estimated cost: $0–$3,000 (if external vendor is used)
  - Estimated man-hours: high
- Implement a network optimization appliance between the Police Department and City Hall
  - Estimated cost: $15,000–$25,000
- Implement a wireless network that can authenticate users via RADIUS (802.1x) or, at a minimum, can encrypt traffic with WPA2.
  - Estimated cost (SOHO-class): $2,000–$5,000
  - Estimated cost (enterprise): $5,000–$15,000
  - Estimated man-hours: medium–high

C. SERVER ENVIRONMENT

1. Current Situation

The City's server environment is split between four locations: City Hall, City Library, the Sports Center, and the Police Department. The current layout includes nine servers at City Hall, one server at the City Library, two servers at the Sports Center, and 19 servers at the Police Department. The server environment is generally stable and no evidence of malware or infections is present. The City uses a single Windows AD domain for user account authentication, group policy, and organizational unit management. The AD environment is comprised of one domain and one forest, and it uses two domain controllers for redundant management.

2. Assessment

The City maintains 31 servers at four locations. These servers support various City functions such as Police Department dispatch, City Hall financial applications, and GIS applications for roads and airports.

Although the City's contract System Administrator maintains the servers monthly, there is no formalized system or application-level patching policies or procedures for keeping the servers up to date after deployment. For example, it was noted that Windows Server Update Services (WSUS) is available; however, it is not being used for patch management in the City's environment. Furthermore, server hardening is limited before deployment. The current process for pre-deployment hardening only includes enabling Windows firewall and installing anti-virus software. Failing to maintain and enforce a server patch and update management policy provides a potential pathway attackers could use to gain access to unpatched systems inside the City's network and compromise unprotected machines, including web servers. Patch management solutions such as WSUS or KBox would enable the City to download, analyze, test, and deploy new updates as they become available. This would ensure a patched and secure server environment.

The City's environment includes a number of HP Blade servers that will reach EoL in April 2014, but no plan is in place to address the expiration of vendor support and maintenance. Failure to implement a hardware lifecycle policy addressing EoL issues could allow hackers to compromise servers (and sensitive data) no longer receiving vendor patches or updates. Furthermore, unsupported hardware can also cause issues with replacement hardware and software. Implementing a lifecycle and vendor management policy would allow the City to plan for future hardware and software upgrades well in advance.

The City's AD currently contains approximately 130 users and contains mostly default group policies for user management. Group policy has been set at the domain level with group policy object settings for the network password policy and account lockout policy. While these are adequate configurations overall, they do not conform to recommended industry best practices. For example, the current policy allows users to keep passwords indefinitely, but they should be forced to change them every 90 days. It was also noted that users with elevated permissions do not require enhanced passwords. Domain Admins and other higher-level administrators should be required to use more complex passwords to keep administrative privileges more secure. These policies help reduce the chance that an attacker could gain access to a system and install backdoors, key loggers, or other malicious software.

The Active Directory security groups need a thorough review. The Domain Admins and Enterprise Admins groups contain user and service accounts that are no longer in use. A periodic verification of active users and services within Active Directory is advised to remove inactive and disabled accounts for security purposes. Otherwise, inactive users who have active accounts could gain unauthorized access to systems and sensitive City data.

3. Potential Projects

Due to the critical nature of managing patches to maintain a secure environment, we highly recommend implementing regularly scheduled workstation and server patching using Windows Server Update Services. With WSUS readily available in the environment, the main cost of implementation is man-hours for configuration and deployment. Implementing a patch management solution is an essential component of any technology environment.

Another potential project for the City would include the deployment of a virtualized environment. This environment could include either a hosted cloud solution or an in-house, on-premise solution. The advantage of a cloud solution is that the cost is associated with the number of licenses needed; however, the vendor controls the environment. An in-house solution would incur up-front costs, but the City would ultimately have complete control over the environment.

4. Project Name

- Implement in-house WSUS solution for patch management
    - Estimated cost: $2,500–$5,000
    - Estimated man-hours: low
- Create and implement a patch management policy
    - Estimated cost: $1,500–$2,500
    - Estimated man-hours: low
- Implement periodic AD user access reviews
    - Estimated cost: $1,000–$2,000
    - Estimated man-hours: low
- Implement a virtualized solution for workstation and server infrastructure
    - Estimated cost:
        - Hosted cloud virtualized solution: $456/year per user (50 seat minimum) NOTE: This solution is an infrastructure as a service (IaaS) option where the server-based applications would be hosted with a cloud service provider using virtualization technology.
        - In-house virtualized solution: $323/year per user (100 users)
- Hardware Estimates
    - Blade enclosure: ~$5,000
    - Infrastructure: ~ $2,000
    - SAN: ~ $30,000–$45,000
    - Blade server(s): ~ $18,000 (2 x $9,000)
    - 2 x 8 core Xeon processors:
        - Recommend 10 hosts per core in a VDI environment
        - Estimated 100 users per server with an extra for HA
- Software estimates
    - VMware Horizon View: $120 per user procurement cost with $64-per-year user maintenance cost
    - Horizon View Manager
    - Horizon View Composter
    - Persona Management
    - ThinApp
    - vSphere Desktop
    - vCenter Desktop

- Windows VDA: $28 per concurrent connection per year.
- **Cautions:** Due to the limited bandwidth between City Hall and the Police Department, the following considerations should be taken into account. (These are industry averages, to obtain more accurate bandwidth requirements, the City should consult a vendor specific implementation expert):Average bandwidth requirements for basic desktop use (web browsing, email, office applications, 2D applications) require between 0 – 200 Kbps.
- High bandwidth applications (steaming video, file transfers) require between 100 and 500 Kbps.
- Given the limited bandwidth, the city would likely be able to run approximately 100 -150 terminals at City Hall assuming an average of 100Kbps was required for each thin client. This would leave a link buffer of about 25% for overhead and other services.

D. APPLICATIONS

1. Current Situation

Naviline is the City's primary application for financial management, business licensing, sales tax, utility billing, and payroll. Naviline runs on the IBM iSeries AS/400 server platform. Its architecture consists of a console-based, "green screen" interface that accesses the server directly. There is no web front-end interface for user interaction.

New user requests are typically initiated by the Human Resources Department. Human Resources directs the Finance Director to set up a new user account within Naviline. The Finance Director serves as the application "owner" of the system. As a result, he is the only person who can authorize new users to the application. However, four individuals can set up new user accounts and terminate current user accounts. These individuals are the Finance Director, IT Technician, TekMate System Administrator, and Controller. Each Naviline user has his or her own unique user account. There are no shared accounts except for one used jointly by the IT Technician and TekMate System Administrator for troubleshooting purposes. This shared account is known as "Ted" and it has administrator-level privileges. When filling a new Finance position, the Finance Director copies the profile of an existing user account so the new user has similar access rights in Naviline, and at the same time modifies the access rights as needed to meet the requirements and restrictions based on the new user's position.

Naviline requires its own set of login credentials in addition to the AD credentials required to access the network. Currently, user passwords do not need to meet a minimum set of criteria in order to authenticate to the system. However, invalid attempts at accessing the system were limited to three before the user account is locked out and needs to be reset.

As the system owner, the Finance Director ensures that all active user accounts are valid by running an annual query to identify inactive user accounts. If invalid or terminated user accounts are found, the Finance Director disables the account immediately. No account deletions occur in case prior transactions are associated with a former employee.

No logging functionality is built into Naviline. As a result, user account changes are not recorded in a running log of transactions. Furthermore, active sessions are not automatically secured after a period of inactivity through an automatic trigger of the screen-lock function on the workstations or session timeouts through the Naviline system.

2. Assessment

As the City's primary critical business system, Naviline falls short with security functionality and meeting best practices for application security. Although the Naviline application runs on the robust AS/400 platform known for its durability, stability, and performance resiliency, the system does not enforce sound security practices such as strong password settings and transaction logging.

Additionally, the user setup process should be improved so that new user accounts are not copied from a previous user's account profile, as the access rights may seem excessive given the new user's role and level of responsibility. Ideally, a user account should be created from a "base user" template that has the minimal amount of access rights needed. From there, access rights should be added as needed and required for the job.

The password policy settings are non-existent and should be configured so that all users are required to enter a strong password to authenticate. Currently, Naviline's password settings do not enforce a minimum password length, maximum password aging, complexity in characters, and a minimum password reuse history. It was noted the lack of customization of the system's password settings is an inherent flaw in the software. Ideally, Naviline should be configured to utilize strong password settings that include a minimum of eight characters, 90 days maximum aging, complexity enabled, and the last 24 passwords remembered. However, the only password setting that can be changed is maximum aging. As such, security parameters are limited.

Login credentials, including passwords, should be known only to the individuals who primarily use the account. There should not be sharing of login credentials nor should employees know the passwords of others. For example, the shared "Ted" account used by the IT Technician and System Administrator should not be used by any individual. Given the administrator-level access that the Ted account holds, it can be utilized for nefarious or malicious purposes. Because the account is used by multiple individuals, it is suggested that the City disable the Ted account and assign administrator-level access rights to the IT staff's individual accounts. The reason behind this practice is that actions associated with every user account can be traceable and auditable to the specific user. If employees shares a user account or knows the passwords of others, an opportunity for fraud is created. It is recommended that the City change this practice to ensure that all users have user accounts that are unique to them.

The City should research the logging functionality within Naviline. IT should work with the vendor technicians to enable the system's logging functionality and ensure that transactions are recorded and traceable to specific individuals.

3. Potential Projects

The City should revise and formalize the user setup process to ensure that Naviline user accounts are created from a "base user" template and not from existing user profiles that may have more access rights than needed for the new user. In addition, the password settings for Naviline need to be bolstered to mimic best practices, including a minimum of eight characters, a maximum of 90 days aging, and complexity-enabled. Lastly, logging should be enabled on the system to provide a historical record of user actions that is traceable and can be used for forensic purposes. City IT staff and the Finance Director will need to work with Naviline technicians to resolve the issue.

Alternatively, it was noted that Naviline's One solution addresses the security deficiencies around transaction logging and password settings. The One solution leverages Windows Server technologies (e.g., Windows Server 2008/2012, SQL Server) rather than the IBM iSeries AS/400 platform. Migrating to Naviline's One solution was estimated to be $500,000 for conversion costs. As a result, the City should plan for and budget for eventual migration.

4. Project Name

- Formalization of Naviline user setup process
  - No cost; staff time
- Naviline Security Improvements (password settings, logging)
  - No cost; Maximum password aging should be set at 90 days. Technical support should be part of the service agreement the City has with Naviline
- Naviline One Migration
  - No initial cost; but the City should be setting aside budget for eventual migration. While $500,000 was provided as an estimate, $1,000,000 should be earmarked given that there will be additional costs with data migration, potential interface development, project management over implementation process, server hardware and related architecture, and end user training.

E. WORKSTATION AND MOBILE DEVICES

1. Current Situation

A large portion of the City's physical workstations are running on Windows XP, for which technical support ends in April 2014. Additionally, the hardware on the workstations is either reaching its end-of-life period or unable to fully meet the recommended application requirements.

Most of the City's desktop workstations have been standardized on Dell OptiPlex models with thin clients running on Hewlett Packard (HP) hardware. At the Police Department, HP has been the preferred vendor for blade PCs. The blade PCs were noted to be approaching their EoL.

The City Finance Department administers and maintains a policy and procedure for Fund 260 – Technology Replacement Fund (Policy Number: 260-2009-001) which details the process to be followed when replacing obsolete computing equipment and acquiring new IT assets. The Technology Replacement Fund defines an equipment's standard life as three to five years (economic useful life).

Hardening configuration standards have not been developed for the physical workstations and anti-virus software is not scheduled to run on a periodic basis.

2. Assessment

Interviews with department staff and inspections of several physical workstations showed that Windows XP Professional (XP) is the primary workstation operating system used in the City's environment. XP was chosen primarily because certain application software was not compatible with Windows 7. For example, in the Finance Department the IBM OS/400 release version V5R3 was not certified to run Windows 7, and the Museum Past Perfect archive software ran poorly on Windows 7 systems. IBM released a new operating system (OS) (version V6R1) compatible with Windows 7 that IT staff installed in August 2010, but most of the systems are still XP-based, and technical support for XP expires in April 2014.

Several of the workstations are running older processers (e.g., Intel Pentium 4) and CPU/RAM speeds do not meet the City's business demands. In most cases, the CPU/RAM speeds cannot support the software requirements needed for departments to efficiently perform their duties. For example, in the Planning Department, one system is running Windows 7 Professional with a 3.0 GHz processor (Intel i3 series), which is the minimum processing speed required to run the application AutoCAD Map3D 2012. Planning also uses software for "SketchUp," but the minimum RAM requirement is 2GB. While RAM memory chips are relatively inexpensive, replacement of RAM in older machines will serve merely as a "Band Aid" fix rather than addressing the collective performance issues which could extend to CPU utilization, onboard bus speeds, drive I/O speed, and the like. Many department staff also stated that their systems and applications run "slowly," which reduces the offered functionality of the software and the overall economic development within their department.

Replacement funds based on Fund 260 exist to refresh old workstations with new workstations, but the last replacement cycle took place in 2009/2010. Most workstations (including desktops and laptops) typically last between three and five years, which means a majority of the City's workstations are potentially reaching their EoL. Additionally, the City is using thin blade clients (HP Blade BC2800, enclosure G2) whose EoL is set for April 2014. The EoL for the thin blade servers (HP BC460, enclosure C7000) is also set for 2014. There is no current plan to address the expiration of the thin blade clients or servers.

Secure configuration and hardening documents do not exist for the City's workstations. Images are used for the thin blades but are not updated to reflect system or software changes. The lack of hardening results in systems that are less secure and more prone to network attacks (i.e., opened ports that are risky and could introduce malware into the network). For example, it was noted that the "CCleaner" tool is installed on some systems. Although the tool itself is not malicious, it is considered an unnecessary program that should be limited to the IT staff. While the IT Technician is designated as the system administrator, several users have local administrative rights to their systems, which allow them to download and install software. This includes the thin blade clients and the police dispatch systems, although the dispatch users are required to be local administrators in order to run the appropriate software.

McAfee is the City's primary anti-malware solution, and it is installed on the systems and servers. It is configured to update daily, but anti-malware scans are not scheduled to run on the workstations. One thin blade client was last scanned for malware in March 2012. If a virus is found, the IT staff's solution would be to reimage the client. Although this is a potential solution, it is inadequate because not all malware is easily detectable and it could spread to the rest of the City's network once a client is infected.

3. Potential Projects

The City will need to strictly adhere to the lifecycle defined in Fund 260 for user workstations. Four years is typical. However, the City could stretch that number by repurposing out-of-warranty workstations into lesser, non-essential use. As part of the workstation refresh project, the City should develop a standard, minimum set of hardware requirements for CPU speed, minimum amount of RAM, and minimum storage. Setting a minimum hardware standard will help to ensure that no user is relegated to a nearly obsolete workstation that does not have the adequate computing power for minimum expected performance. The City can align its workstation refresh and lifecycle approach with the purchases of Windows 7-compatible machines. If a bulk purchase of newer workstations is deemed cost prohibitive, the City will need to apply "Band-Aid" fixes such as upgrading the CPUs and RAM memory on the performance-deficient machines.

4. Project Name

- Replace the XP operating system with Windows 7
    - Estimated cost: $8,000–$12,000
- Upgrade the CPU hardware on systems where needed
    - Estimated cost: $5,000–$10,000
- Upgrade the RAM hardware on systems where needed
    - Estimated cost: $2,500–$5,000
- Develop plans to replace the thin blade clients and servers
    - Estimated cost: staff time
- The IT staff should develop and document secure configuration standards for the physical workstations, including laptops
    - Estimated cost: staff time
- Thin blade images should be updated on a periodic basis to reflect security and patch updates to critical software and the operating system
    - Estimated cost: staff time
- Local administrator rights should be removed from systems unless needed for business purposes (e.g., Police Department needs local admin rights to run the department's software)
    - Estimated cost: staff time
- McAfee should be configured to conduct periodic malware scans, both on the workstations and thin blade clients
    - Estimated cost: staff time

F. ANTI-VIRUS AND DATA LEAKAGE PROTECTION

1. Current Situation

The City of Wasilla currently supports workstations and servers across a number of locations city-wide. These locations include City Hall, City Library, the Sports Center, the Police Department and the City Museum. To protect the workstations across the network, the City currently uses McAfee Virus Scan. For email protection, Symantec MX is used to scan messages and attachments for malware.

2. Assessment

Currently, the City IT staff supports a large number of workstations including laptops, mobile dispatch machines, and desktops. While anti-virus is installed and virus definitions are updated before deployment, there are no regularly scheduled workstation updates. This is especially an issue for devices such as laptops that are not on the network for lengthy periods of time, so definition updates are missed. This may enable an attacker to gain access to a machine through a vulnerability that may have been eliminated if the anti-virus program had received its updates previously.

The City currently has a policy restricting the use of personal removable media. However, that policy is not being enforced. Users, especially those with laptops and mobile devices, are able to freely move potentially sensitive data between the City network and home or other remote locations using thumb drives or writeable CDs.

Finally, a methodology to properly destroy or sanitize City data from unused hard drives has not been developed. Currently, the media that needs to be destroyed is stored in the IT Technician's locked office, in a box at the Police Department, or within the contract System Administrator's working area. Media that is not destroyed can lead to hard drive theft, and data left on the hard drives can be accessed. Attackers could access sensitive data or passwords and further compromise the City's network or data in the future.

3. Potential Projects

It is recommended that the City implement a scheduled virus definition update to all workstations and servers, including laptops and mobile devices. A forced update would require all machines to have up-to-date virus definitions to keep their devices safe and secure before they can connect to the Internet.

Second, a project to implement a personal removable media policy in Active Directory is recommended. A group policy configured in AD would restrict the use of USB ports and other removable media by scanning the port to verify encryption. A policy like this would retain the integrity of personal information and sensitive data.

Last, the City should develop a documented procedure for destroying or sanitizing used hard drives. This type of policy will ensure that City data is not stolen or used for malicious purposes, and it keeps potentially sensitive data on those drives secure.

4. Project Name

- Configure and deploy enforced regularly scheduled anti-virus updates
  - Cost estimate: $1,500–$3,500
  - Estimated man-hours: low
- Create and implement an AD policy restricting removable media
  - Cost estimate: $2,000–$3,000
  - Estimated man-hours: low
- Create and implement a hard drive destruction policy and procedure
  - Cost estimate: $2,500–$5,500
  - Estimated man-hours/wipe software: low

G. BACKUP, RESTORATION, AND DISASTER RECOVERY

1. Current Situation

The City uses a multi-faceted approach to backing up critical data. Two backup systems are used for data at City Hall because of the operating system platforms for the key business applications. SunGard Naviline, the City's Finance and Accounting system, runs on an IBM iSeries AS/400 platform. Therefore, the application is backed up using the native backup management utilities that are part of the OS/400 operating system. The Naviline system backups use tapes as the media. The backup tapes are stored in a vault located at City Hall. The tapes are stored there until the Finance Director rotates and transfers them to a local bank safe deposit box.

The City uses its storage area network (SAN) in conjunction with Symantec's Netbackup for backup storage of all critical Windows-based department folders. Netbackup manages all of the backup functions for the City's Windows-based systems, and has been a solid performer. The computer-aided dispatch (CAD) system used at the Police Department leverages Acronis Backup and Recovery for managing its backup process. Full backups to the SAN occur every Monday at 7:00 p.m. The SAN is located in the second-floor server room at the Police Department. Backed-up data remains on the SAN and is readily available online if IT staff need to restore a file or folder. Neither Netbackup nor Acronis is configured to automatically send status emails at the conclusion of a backup job.

The City has an Information Technology Services (ITS) Disaster Recovery Plan document that was developed in 2006. The plan describes the actions that will be taken by IT staff during various disaster scenarios. The plan is fairly detailed with several key sections, including Classification of Computing Applications, Identification of Disaster Scenarios/Risk Analysis, Recovery Activity

Analysis, and Data Backup and Offsite Storage. While the plan appears to have fairly robust content, it has not been formalized and approved by City management or department heads.

2. Assessment

The use of disk-to-SAN as storage for backed-up data appears to be sound. Backing up data "over the wire" and to another storage system or server helps eliminate the need for tape libraries and drives, and also helps eliminate the need to track and store backup tapes. Tape drives and libraries are known to malfunction on occasion because of their mechanical nature, while backup storage tapes can be easily lost, misplaced, or stolen.

Symantec's Netbackup solution is a leader in backup management software. It is widely used across all industries and is supported by a "blue chip" company recognized as a leading high-tech software company. Acronis Backup and Recovery also appears to be a solid backup management solution. Although not as well-known as Symantec's Netbackup, the solution appears to function well for the CAD system. At some point, the City may want to consider moving the data backup functions to a cloud service provider. The benefits of this approach include a more robust backup infrastructure, enhanced disaster recovery capabilities, decreased administration of hardware and software, and less reliance on hardware and software viability.

In the meantime, the City should consider standardizing on a single backup management platform and select either Symantec or Acronis as its sole vendor for backup software. By standardizing, City IT staff is not burdened by the need to become the "expert" on two different backup management platforms. Having two different platforms could present a challenge when data restoration is necessary and IT staff is more familiar with one of the solutions than the other. In addition, it is recommended that IT staff enable the triggers for automatic status notification on both Symantec and Acronis to ensure that backup jobs are consistently completed with no issues. Otherwise, the City risks unawareness of whether the backups are actually occurring.

Although IT staff members know the process for restoring critical data from the backup media, routine restoration testing for either Naviline or the critical Windows-based systems does not occur. Consequently, it is unclear whether IT staff would be able to successfully recover data in the aftermath of a disastrous event. Restoration testing would also help ensure that the backup jobs are complete and that all files necessary to reconstruct a data set are accounted for and exist on the backup media. In addition, regularly scheduled restoration would help to determine whether IT staff is able to perform the restoration duties without issues, and determine the amount of time it takes to restore critical data.

The disaster recovery plan is extremely outdated and precedes the current in-house IT staff. Initially developed in 2006, the plan does not accurately reflect the changes and evolution of the technology environment at the City since then. As a result, the plan will not be effective at guiding IT staff through the recovery procedures to restore the City's critical business systems to an operational state following a disastrous event. It is recommended that the disaster recovery plan is updated to account for the changes in IT systems, network architecture, and operations that have occurred since 2006.

3. Potential Projects

The City should evaluate potential cloud solutions for data backup. Cloud backup solution options in the market today are plentiful and the benefit of storing backup data in the cloud is the automation, unlimited storage capacity, resiliency for disaster recovery purposes, and the fact that the City would not need to maintain a series of backup tapes that require continual rotation and eventual replacement.

In addition, the City should standardize on a single backup management solution to simplify management of the backup process.

The disaster recovery plan is in dire need of an update. Given that the current plan is more than six years old, most of its content is likely obsolete and not applicable.

4. Project Name

- Evaluate cloud backup solutions
  - Cost estimate: $0; staff time
  - Estimated man-hours: low
- Backup management software standardization
  - Cost estimate: $0; staff time (City has the licenses.)
  - Estimated man-hours: low
- Develop disaster recovery plan
  - Cost estimate: $25,000–$30,000 (if consultant engaged)
  - Estimated man-hours/wipe software: high

H. SECURITY MANAGEMENT

1. Current Situation

The City has engaged several vendors to support the IT environment including MTA, GCI, Tiberon, and SunGard, which are actively managed by the City. Sensitive information such as electronic protected health information (ePHI), HR records, and financial data is housed within the network. Access to this data is controlled by the City's various applications and network access controls inherent in AD. The City also maintains policies and procedures to protect the network, systems, and users from inappropriate use and security-related issues. Access to network systems is reviewed on a monthly basis by the IT Technician. However, user accounts for the Police Department users are currently not reviewed.

2. Assessment

Before network and application accounts are created for new users, owners must wait for authorization from HR. Currently, access is requested via an informal process of e-mail/phone call and it is difficult to verify that proper access has been approved by management. Similarly, system owners are not promptly notified when an employee changes jobs within the City and therefore should have his or her access modified or, in the event of a termination, revoked.

3. Potential Projects

Due to the potential security issues associated with inappropriate access, especially by users who were terminated and may still retain access to network systems and applications, a formal new-hire/access change/termination notification process should be implemented that specifically states which systems and applications a new-hire should be able to access. That same notification process should be used for job changes and quick notification of user access termination. In addition, it provides an opportunity to spot check and review active user accounts on systems. All access requests and changes should require approval from management before that access is provisioned on systems. We recommend the City leverage Microsoft SharePoint workflows or a ticketing system such as Track-IT! for this process, rather than a paper-based system.

4. Project Name

- Create a formal new hire/terminations checklist that is initiated by HR and required by IT and application owners for account creation
  - Cost estimate: $1,500–$5,000
  - Estimated man-hours: low
- Leverage Track-IT! for user provisioning workflow
  - Cost estimate: $0 for Track-IT! $5,000–$20,000 if leveraging SharePoint
  - Estimated man-hours: low to medium (SharePoint)

I. INCIDENT RESPONSE

1. Current Situation

The City does not have a formalized incident response policy or procedure in place that is specific to IT-related incidents such as a software virus outbreak or theft of a City-owned laptop. In the event of an IT-related emergency the contracting company, TekMate, is responsible for response and resolution. If a call comes in, the TekMate System Administrator is generally able to fix issues remotely using a VPN. However, for more critical issues or downtime, he must travel to the office to fix issues on-site.

2. Assessment

The ad hoc incident response plan currently in place includes contacting the IT Technician by phone or e-mail to remediate any issues. He currently lives approximately 20 minutes away from Wasilla, which makes response turnaround inefficient. The lack of a documented incident response procedure makes it difficult to respond to a potential network attack or denial of service. There is no segregation of responsibilities among first responders, which could lead to general confusion and work duplication.

3. Potential Projects

To ensure that potential incidents are responded to in a timely and efficient manner, we recommend that the City implement a documented incident response plan. This policy should cover responsibilities, back-up plans, chain of command, and a post-mortem plan. An incident response policy will help the City ensure the confidentiality, integrity, and availability of its systems in the event of an attack.

4. Project Name

- Create a formal incident response plan (initiated by the IT staff and approved by management)
    - Cost estimate: $1,500–$3,000
    - Estimated man-hours: low

J. ASSET MANAGEMENT

1. Current Situation

Although the City has an asset management module in Naviline, assets that are below $5,000 in total cost are not included. For tracking IT assets, the City has just started to use the inventory module of Track-IT!, the help desk management system. If there is a problem with a server or workstation, the IT Department maintains the warranty records and agreements for obtaining service and fixes from the vendors.

2. Assessment

The ad hoc nature of the current asset management procedure could lead to asset warranty expiration, retirement of assets, or procurement of new assets without cross-departmental knowledge. The lack of a formalized process for managing assets could lead to unnecessary expenses and missed equipment refresh dates.

3. Potential Projects

To ensure the City maintains timely and effective management of its IT assets, Moss Adams recommends implementing a formalized asset management policy and leveraging existing asset management systems like Naviline and Track-IT! to record and track IT assets. The policy should detail the asset lifecycle from approval, purchase, and procurement to retirement. An asset management plan will enable the City to determine where assets are in the lifecycle at any point in time. The City is already utilizing Track-IT! for tracking software installations and licensing and has recently been used for running hardware and software inventories of workstations. This software can also be leveraged to manage other IT assets such as printers, scanners, mobile devices, among other devices and systems.

Moss Adams also recommends procuring and implementing a complete asset management software package. This package includes bar codes for placement on assets and bar code readers, and the software portion to track them. The benefits from such a system include gaining control of the City's assets and their location, reducing costs to the City by eliminating unnecessary software licenses, improving productivity by tracking unproductive software installations, and ensuring users have the proper software for their departments.

4. Project Name

- Create a formal asset management policy
  - Cost estimate: $1,500–$3,000
  - Estimated man-hours: low
- Procure and implement a complete asset management package
  - Cost estimate: $3,500–$15,000
  - Estimated man-hours: moderate

K. PHYSICAL AND ENVIRONMENTAL CONTROLS

1. Current Situation

Computer and network equipment is located in several areas throughout City Hall, the Police Department, the Library, and several remote locations. Access to equipment at City Hall and the Police Department is permitted to employees who have the proper metal key, or a key fob configured for those areas. Vendors and visitors are required to be escorted when working on equipment within the server rooms. The Library's network equipment is located in an unlocked storage area in the basement and was difficult to access because of the amount of inventory in the room.

2. Assessment

Because IT management does not know who has access to the server rooms and communication closets at City Hall, it would be very difficult to investigate any theft of equipment or a physical data security breach of sensitive information. Metal keys are required to access the server room and communication closet that house the camera system DVR and several other servers that house the financial applications and file storage. At the Police Department, a key fob is required to access sensitive areas including those that contain network, communications, and computer equipment. However, it was noted that several City employees who did not need access to equipment retained access to these areas. In the Library, the network equipment rack was located in the back of a storage room that was unsecured from unauthorized access. We also noted that non-IT inventory was located around the equipment rack, which could cause damage to cabling or networking equipment.

The server room at the Police Department utilizes a Halon fire suppression system that "starves" fire of oxygen rather than spraying water, so it saves equipment from water damage. Installation of these systems requires the affected areas to be sealed off from the rest of the building to protect employees from hazardous gas. However, the server room was not sealed, which would cause a potential health hazard if the Halon system activates.

3. Potential Projects

To ensure the security of equipment and to properly protect data, we recommend that the City restrict access to the server rooms and communication closets to only those individuals who require access to complete their job-related duties. For locations such as the Library where space is very limited, a locked communications cabinet should be installed to protect equipment from the inventory in the room, and to help prevent potential theft. To ensure the effectiveness of the Halon system and the safety of Police Department employees, the server room should be immediately sealed off to ensure that the gas would be contained within the room.

4. Project Name

- Seal the Police Department server room off to ensure employee safety and the effectiveness of the Halon gas
    - Estimated cost: $25,000–$75,000
- Restrict access to server rooms and other locations where IT equipment exists
    - Estimated cost: (low) man-hours

MOSS-ADAMS LLP

Certified Public Accountants | Business Consultants

Acumen. Agility. Answers.