



**CITY OF WALLED LAKE
NOTICE OF SPECIAL MEETING
Wednesday, September 7, 2016
7:30 p.m.**

NOTICE IS HEREBY GIVEN that a special meeting of the City Council is scheduled for Wednesday, September 7, 2016 at 7:30 p.m. in the Walled Lake City Hall Council Chambers, located at 1499 E. West Maple Road, Walled Lake, MI.

AGENDA

CALL TO ORDER

PLEDGE TO FLAG

ROLL CALL

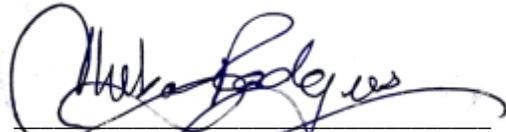
DETERMINATION OF A QUORUM

NEW BUSINESS

1. Resolution 2016-32 Ratifying the Agreement with the Michigan Association of Public Employees (MAPE) on behalf of the Public Works and Clerical Employees from July 1, 2016 – June 30, 2019
2. Public Safety Campus redesign construction plan pursuant to previously approved Council motion CM 08-03-16
3. Approve budgeted Information Technology platform upgrade (New City Server)

ADJOURNMENT

Dated this 2nd day of September 2016


Chelsea Rodgers, Deputy City Clerk

STATE OF MICHIGAN)
COUNTY OF OAKLAND) SS.
CITY OF WALLED LAKE)

AFFIDAVIT OF POSTING

Chelsea Rodgers, being first duly sworn, deposes and says: That she is the duly appointed and qualified Deputy City Clerk of the City of Walled Lake and that on this 2nd day of September 2016 she caused the above Notice to be posted at City Hall, Police Department, and Library and the City Website.


Chelsea Rodgers, Deputy City Clerk



**CITY OF WALLED LAKE
SPECIAL COUNCIL MEETING
Wednesday, September 7, 2016
7:30 p.m.**

PLEDGE TO FLAG & INVOCATION

ROLL CALL & DETERMINATION OF
A QUORUM

NEW BUSINESS

1. Proposed Resolution 2016-32 Ratifying the Agreement with the Michigan Association of Public Employees (MAPE) on behalf of the Public Works Employees from July 1, 2016 – June 30, 2019 Pg. 3
2. Proposed Resolution 2016-33 Public Safety Campus Redesign Pg. 5
3. Proposed Resolution 2016-34 Budgeted Information Technology platform upgrade (New City Server) Pg. 7

ADJOURNMENT

STATE OF MICHIGAN
COUNTY OF OAKLAND
CITY OF WALLED LAKE

A RESOLUTION RATIFYING THE COLLECTIVE BARGAINING
AGREEMENT WITH THE WALLED LAKE MUNICIPAL
EMPLOYEES ASSOCIATION FOR THE CITY OF WALLED
LAKE PUBLIC WORKS EMPLOYEES AND AUTHORIZING THE
CITY MANAGER TO EXECUTE THE AGREEMENT

Proposed RESOLUTION 2016-32

At a special meeting of the City Council of the City of Walled Lake, Oakland County, Michigan, held in the Council Chambers at 1499 E. West Maple, Walled Lake, Michigan 48390, on the 7th day of September, 2016, at 7:30 p.m.

WHEREAS, there being only one member of the Clerical unit the City's bargaining team has placed the Clerical unit as part of the of Public Works union unit; and

WHEREAS, the City Manager representing the Governing Body of the City of Walled Lake, County of Oakland, State of Michigan, has negotiated with the Walled Lake Municipal Employee Association (MAPE), hereinafter referred to as the Union; and

WHEREAS, The City's bargaining team, acting under the authority of the City Manager, as Chief Negotiator, has negotiated a tentative agreement with the Union, for the year's beginning July 1, 2016 and ending June 30, 2019; and

WHEREAS, the City's bargaining team recommends adoption of the provisions of the agreement; believing that said provisions in the agreement are consistent with the budget and financial direction established by the Council; and

WHEREAS, the terms of the tentative agreement have been ratified by the membership of the Union; and

WHEREAS, the City Council, as the Governing Body of the City of Walled Lake, has reviewed the tentative agreement and is desirous of ratifying said agreement;

NOW, THEREFORE, BE IT RESOLVED, by the Council of the City of Walled Lake, County of Oakland, State of Michigan that:

Section 1. The Council confirms the merger of the Clerical and Public Works Employees as one union unit with MAPE.

Section 2. The Council formally expresses its approval, and accepts and ratifies the collective bargaining agreement with MAPE for the benefit of the Walled Lake Public Works Employees.

STATE OF MICHIGAN
COUNTY OF OAKLAND
CITY OF WALLED LAKE

A RESOLUTION TO APPROVE THE RECONSTRUCTION OF THE PUBLIC SAFETY AND CITY CAMPUS PARKING LOT AND DIRECT SAID PROJECT TO INCLUDE STORMWATER INFRASTRUCTURE UPGRADES, ENHANCED STABILITY OF THE FIRE DEPARTMENT DRIVING AREA, IMPROVEMENT OF THE POLICE DEPARTMENT TRAFFIC FLOW AND SAFER PEDESTRIAN CROSSING

Proposed RESOLUTION 2016-33

At a special meeting of the City Council of the City of Walled Lake, Oakland County, Michigan, held in the Council Chambers at 1499 E. West Maple, Walled Lake, Michigan 48390, on the 7th day of September 2016, at 7:30 p.m.

WHEREAS, the deteriorating public safety and city campus parking lot situation has been addressed by Council in its annual strategy sessions and repair of the same has been budgeted as part of the 10 year capital improvement program since fiscal year 2015; and

WHEREAS, in summer 2016 a sinkhole opened in a portion of the pipe that runs under the Fire Department driveway and emergency repair of the one segment of the pipe was performed by the Oakland County Water Resources Commission leaving the remaining pipe to be upgraded at a later date; and

WHEREAS, in consultation with the Water Resources Commission and the Michigan Department of Environmental Quality the City Engineer has designed a green infrastructure solution for the failing storm water drains beneath the parking lot with an estimated savings of \$43,000; and

WHEREAS, the crumbling parking area near the Fire Department caused one trip and fall accident for a paid on call fire officer; and

WHEREAS, police vehicles must currently back out of their parking area before responding to a call for service; and

WHEREAS, the City Engineer determined the emergency nature of the campus parking lot problems required a more immediate solution than anticipated; and

WHEREAS the City Engineer aggressively pursued the contractor during the recently completed Maple Road construction and requested they perform on-site inspections and prepare a bid with pricing mirroring the bid award price for the Maple Road construction; and

WHEREAS, Section 12.1 of the City Charter states “Council may authorize the making of public improvements or the performance of any other city work by any city agency without competitive bidding”; and

WHEREAS, the construction bid from Cadillac Asphalt LLC for the parking and storm water improvements is \$691,202.20 plus any performance bond expenses;

NOW, THEREFORE, BE IT RESOLVED, by the Council of the City of Walled Lake, County of Oakland, State of Michigan that:

Section 1. Council affirms the City Engineer’s position as to the emergency nature of the deteriorating campus parking lot.

Section 2. Council awards the construction contract for \$691,202.20 plus any required performance bond cost incurred by the vendor to Cadillac Asphalt LLC subject to final review and approval of the City Attorney and City Administration.

Section 3. Council directs the City Manager to execute and sign Contract 15-027 a copy of which is on file with the Clerk.

Motion to approve Resolution offered by _____ and seconded by _____.

AYES: ()
NAYS: ()
ABSENT: ()
ABSTENTIONS: ()

RESOLUTION DECLARED ADOPTED.

STATE OF MICHIGAN)
)SS
COUNTY OF OAKLAND)

JENNIFER A. STUART
City Clerk

LINDA S. ACKLEY
Mayor

STATE OF MICHIGAN
COUNTY OF OAKLAND
CITY OF WALLED LAKE

A RESOLUTION TO APPROVE THE PURCHASE OF A
PUBLIC SAFETY AND CITY HALL SERVER

Proposed RESOLUTION 2016-34

At a special meeting of the City Council of the City of Walled Lake, Oakland County, Michigan, held in the Council Chambers at 1499 E. West Maple, Walled Lake, Michigan 48390, on the 7th day of September 2016, at 7:30 p.m.

WHEREAS, the City in 2015 solicited an IT Assessment Report which outlined the following risks:

- The City's IT environment is unstable
- The main server is inadequate for the tasks it's asked to perform
- The email architecture is unnecessarily complex
- There is a high risk of data loss
- There is a risk of extended server outage
- The layers of security can be enhanced

WHEREAS, replacement of the city server has been budgeted as part of the 10 year capital improvement program; and

WHEREAS, the Police Chief has reviewed and approved the server specifications as meeting the public safety requirements; and

WHEREAS, the estimated cost of the server and installation are \$22,460 which is less than Council's budgeted \$30,000 for this item;

NOW, THEREFORE, BE IT RESOLVED, by the Council of the City of Walled Lake, County of Oakland, State of Michigan that the purchase of a Dell server and installation for a price not to exceed \$25,000.00 is approved.

Motion to approve Resolution offered by _____ and seconded by _____.

- AYES: ()
- NAYS: ()
- ABSENT: ()
- ABSTENTIONS: ()

RESOLUTION DECLARED ADOPTED.

STATE OF MICHIGAN)
)SS
COUNTY OF OAKLAND)

JENNIFER A. STUART
City Clerk

LINDA S. ACKLEY
Mayor

**New File Server Budget for City of Walled Lake
25-Aug-16**



These are budget numbers. Product estimates are based on today's government pricing from vendors. Labor estimates are based on historical averages, and will be refined after you approve the budget. Product estimates will be final when we get actionable quotes from vendors.

<u>Item</u>	<u>Unit Cost</u>	<u>Qty</u>	<u>Ext. Cost</u>	<u>Comments</u>
Server Hardware and system Software				
Server	\$2,410	1	\$2,410	Rack-mount Dell PowerEdge R330 with 3-yr next-biz-day warranty
Optional warranty upgrade	\$850	1	\$850	Marginal cost of upgrading warranty to 4-hr mission critical on-site service.
UPS	\$710	1	\$710	APC Smart-UPS 1500VA, sufficient to cover everything in the svr cabinet
Svr Operating System (OS)	\$650	1	\$650	Windows Server 2012 R2 Standard, volume license
OS user licenses	\$27.55	55	\$1,515	Purchased in 5-packs. Not needed for non-domain users, count TBD
Server Cabinet	\$750	1	\$750	
Total, Server hardware and system software			\$6,885	
On-Premise backups:				
Synology Backup NAS	\$1,650	1	\$1,650	Rack-mount back-up storage device w/RAID
Veritas Backup Exec	725	1	\$725	Backup software to run on the server, for on-premise backups
Total, on-premise backup hardware/software			\$2,375	
				\$360/year support renewal after year 1
Off-site backup options:				
Portable drivges for off-site backups	\$700	1	\$ 700	this option provides off-site storage for *all* data but requires human intervention once/week.
Cloud backups, <i>BS&A only</i>	\$160/month			Cloud backups are set-it-and-forget-it, but monthly storage costs can be high, especially for large data sets like yours.
Cloud backups for <i>200GB critical data</i>	\$325/month			Would require you to identify 'critical data'
Labor Budget			\$12,500	This is an estimate based on recent prior work, adjusted for your specific requirements. When we do the formal project plan, we'll have a closer estimate.
Estimated total cost			\$22,460	Suggest we get \$25K pre-approved to provide some room to maneuver, or wait until project plan is complete to get approval for labor.

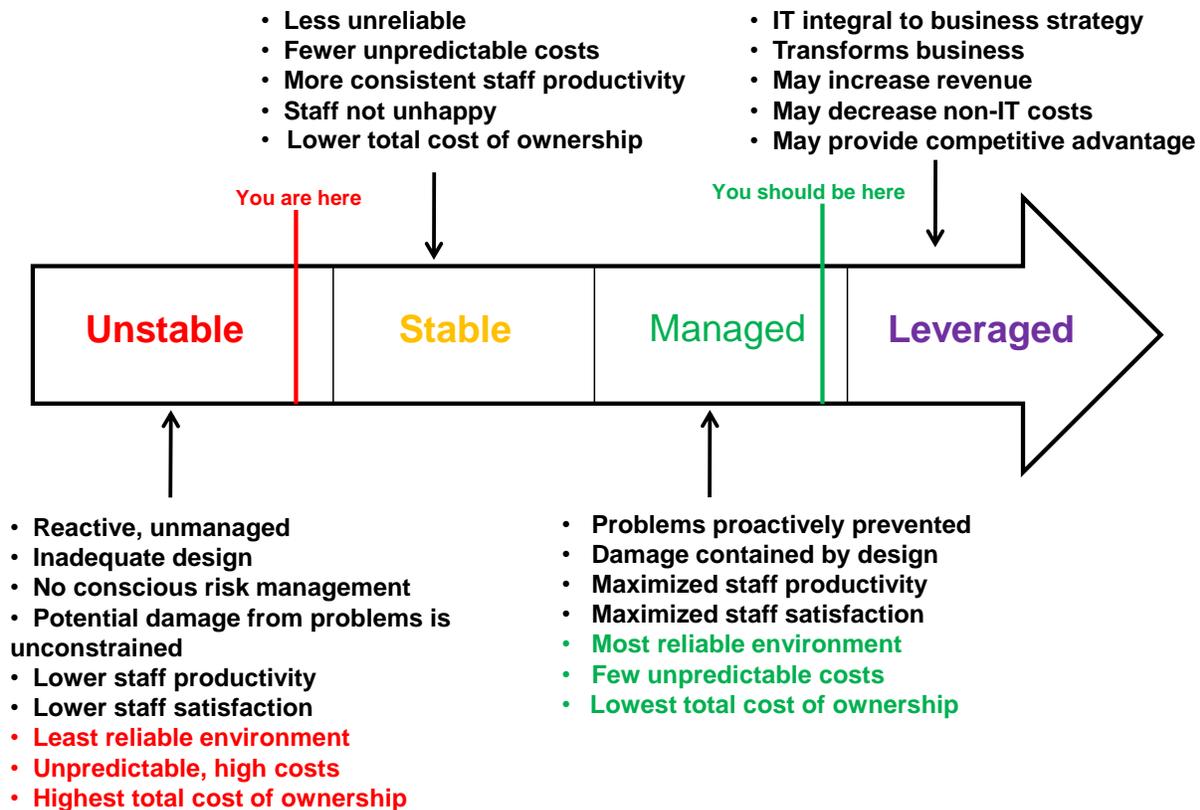
Final IT Assessment Report City of Walled Lake May 1, 2015

Summary: In February, Nimble Systems visited your site and began an assessment of your server and network. We found some serious issues that we felt required immediate attention and issued a preliminary assessment report, which is attached as Appendix E. Since issuing that report, we have done some remedial work to address some of the issues we found; this work is described below, as is a discussion of additional issues we found as we completed our assessment.

This is our final report. We've kept the main body of the report focused on the business impact of the issues we found, with only such technical detail as is required to understand that impact. Appendix A contains additional technical nitty-gritty for readers who want it.

Overall, we find that your IT architecture lacks significant basic features. Your email architecture is unnecessarily complex. Your server is under-specified for the tasks it's asked to perform. Your exposure to IT-related risks is unnecessarily high, performance is sometimes poor, and problems languish unresolved. User productivity often suffers, and it appears that at least some users have lost confidence in the City's IT.

Here's a rubric we use to characterize IT environments; you are in the "unstable" region. There are significant benefits to moving into the 'managed' space, as illustrated here:



Our discussion of issues is organized along the lines of security, reliability, recoverability, and business value. Here are the highlights:

- Security. We talk about security with reference to 8 'layers' that work together to provide good protection. We found 3 of the layers missing (backups, software patches, and anti-malware protection), and two could not be immediately assessed because you lacked the required access credentials (anti-virus, firewall). We've provided temporary fixes for the BSA backups and software patches, are installing a new firewall, and we are working with Cynergy PC Solutions ('Cynergy') on gaining access to your anti-virus software. They have gotten backups going for your files. Backups remain inadequate, but you are no longer totally exposed.
- Reliability. You are exposed to higher-than-normal risk of server downtime and data loss due to certain aspects of the server's hardware configuration and the fact that it is not being systematically monitored and maintained. We found significant issues with how your email is configured that compromise its reliability and create other issues for users; we have rectified some of them, but the long-term answer in our opinion is to move to Microsoft Exchange Online.
- Recoverability. It would be very difficult for you to recover from a server hardware failure because the server is five years old, out of warranty, and the maker's inventory of spare parts for your model is very thin; in fact, you may not be able to recover at all. You have the potential for irrecoverable data loss due to inadequate RAID configuration and lack of comprehensive backups.
- Business value. Your server is inadequately configured for the tasks it is supposed to perform. Your email set-up is unnecessarily complex, is cumbersome to maintain (and has not been maintained), has not been delivering all email, and causes inconsistencies in Outlook content between your own server and the Oakland County server through which your email is routed. Your IT assets are not serving the business of the City and the productivity of your staff as well as they could and should.

The report concludes with our recommendations, the most important of which are:

- Put a new, robust backup system in place.
- Cease routing your email through Oakland County now, and migrate your email to Microsoft's Exchange Online as soon as possible.
- Replace your existing server with one properly configured and powered to run BSA and to provide file and administrative ('domain') services.
- Install anti-malware protection and develop appropriate security policies
- Institute pro-active management of your IT environment, especially your server, backups, and anti-virus/anti-malware protection.
- Assess your inventory of PCs and user software.
- Plan on upgrading all installs of Office 2007 or earlier editions soon.

Security. This section discusses issues that affect your vulnerability to unauthorized network access and malware. In discussing security, we find it useful to segment defenses in 8 categories or "layers". There is no technology that can guarantee your complete safety; the best defense comprises strong implementations of all 8 layers: physical, LAN configuration, email filtering, anti-virus and anti-malware protection, up-to-date software, robust backups, and finally, staff who are educated and vigilant.

We did not assess your facility's physical security, software on your PCs, nor staff awareness/education. We did assess the other layers and found the following:

- We were unable to evaluate the adequacy of your firewall, because no one has the log-on credentials required to examine how it's configured. The device is a custom-built PC of indeterminate age. Since we can't tell what it's doing and can't maintain it, we've recommended its replacement, which was approved and is in progress.

- The status of your anti-virus protection is unclear. Until December 2014, there was no anti-virus at all installed on your server, and your workstations were using free-ware products whose performance was not (and could not easily be) monitored to make sure it was performing as intended.

In December 2014, Cynergy installed a quality, enterprise anti-virus solution (Symantec Enterprise Protection). The software provides a central management console that is installed on the server, which should allow inspection of anti-virus software on each 'end point' where it is deployed, along with a host of other variables that determine whether or not this software is providing the protection it should. Neither you, nor we, nor Cynergy has the credentials to access this console; Chris is working on that. Chris also installed anti-virus protection on your server, which had none. A routine, periodic inspection of this software should be part of a periodic maintenance plan. (We requested an update from Cynergy several days prior to issuing this report but have had no response.)

Installation of this software has caused some performance issues, which is just one more indication that the server is under-powered for the tasks it's supposed to perform: a production server should be able to run this kind of software in while performing its other tasks, without degraded performance.

- You may not have adequate malware protection. While Symantec Enterprise Protection can help you fend off many kinds of attacks, today's best practice is to run an antimalware tool along with your antivirus. That anti-malware tool (one specifically designed to help protect you against malware you pick up while on the Internet) should operate in the same manner as your antivirus, that is, it is always active in the background. We recommend Malwarebytes Professional, preferably as a managed (monitored and maintained) solution to strengthen your protection against malware infections of all kinds. Anti-malware software isn't guaranteed to protect you against all issues but used in conjunction with your antivirus, it provides an additional layer of protection.

You should be aware that there is a class of malware called "crypto-virus" that can infect your machines quite easily, even from legitimate websites. This malware irreversibly encrypts data on the infected machine and on any mapped drives, such as you might use for your server data. The only ways to recover the data are to pay a hefty ransom (in Bitcoin), or to recover from backups, and your backups are currently weak. We have helped two clients recover from this malware. We sent information about it, including some that can be disseminated to users, to the Police Chief.

In response to Internet-borne threats, some of our clients have adopted a policy that their network and computers may only be used for Internet access directly related to a user's job function. Staff who want to conduct personal business on the Internet use their own smart phones or tablets and their carrier's network. You might consider instituting such a policy.

- We found your server's operating system to be very far behind on updates—150 behind. (We did not assess whether or not BSA is up to date.) Since most updates are released to close security vulnerabilities, this means you were more vulnerable than you would be if someone performed regular routine maintenance on your server. Further, a large number of outstanding updates can have a negative impact on server performance. We also found issues with how server updates were configured, problems with the SBS Monitoring database, and SharePoint. Taken as a whole, these findings clearly show that your server has not been receiving competent routine maintenance. (See Appendix A for the technical nitty-gritty.)

We have installed the missing updates, but do not favor setting servers to automatically update their operating systems. We recommend you contract for routine server maintenance including regular installation of relevant software patches to the operating system, backup software, and anti-virus software.

Reliability. This section discusses issues that can or do affect the continuous, proper operation of your server and its software. We found the following issues:

- Your server has inadequate protection against hard drive failures (which are not uncommon). While we believe that the server has RAID hardware (multiple hard drives configured in a manner so that if a single drive fails, the server will continue to operate), we were not able to undertake a physical examination of the server when we were onsite and there is no utility software installed on your server that allows us to look at drive health without physical inspection. However, it appears that the RAID functionality may be provided by the built-in feature of the motherboard, known as “host RAID” or “fake RAID”. While this feature does provide RAID, it has a number of shortcomings that make it unsuitable for servers, especially for an SBS server. In our experience (and that of others) there are conditions that can arise against which this type of RAID will not protect. In the event that your motherboard needed to be replaced, unless you can find an identical manufacturer/model, there is a high probability that the existing RAID drives will not work, resulting in a complete loss of data.
- No one (and no software) is monitoring the health of your server hardware, so there is no opportunity to detect brewing issues early, when they can be resolved in a planned manner. While monitoring can’t catch every issue, we make it a practice to monitor dozens of indicators of server health in real time, programmatically. That is, our monitoring happens automatically and constantly, without the need for physical or manual intervention. We contacted the manufacturer of your server to see what programmatic monitoring tools are available for your server and they recommended Intel utilities designed to work with the chip-set on your motherboard. Installing these will require some downtime and we prefer to be onsite when installing this type of utility. We recommend it be installed and the initial results assessed. If possible, the utility should be used to facilitate ongoing, real-time, programmatic monitoring.
- Users report that being “kicked out” of BSA has been an ongoing issue. We have not yet had the opportunity to identify a root cause. That’s best done by getting on the server as soon as possible after that’s happened. We’d be happy to do that; just contact us when a user loses access.

Further, we looked into onto why the mayor and two other users weren’t getting email. We found the following issues with how your email is configured, which made it highly unreliable in a number of ways. This unreliability is the consequence of the way your email is routed through Oakland County servers, and the fact the ‘connector’ that fetches your mail from that server was not properly configured and has not been maintained.

Here’s a summary of the business issues. (For those who are interested, the technical nitty-gritty is in Appendix A).

- Not all users were properly configured to receive mail from the County server.
- There were unnecessarily-low email size limits set, which meant that emails with attachments that were larger than the limit were never delivered to users on your server.
- Some messages (many likely spam) were arriving at your server with a special error message; when more than 5 such errors were encountered for a given user, the connector stopped trying to receive that user’s email, causing incomplete email delivery for that user.
- Some users were receiving error messages when they tried to access their Walled Lake email boxes.
- People who use webmail on the Oakland County server almost certainly create inconsistencies between what’s in their Oakland County email box and what’s in their Walled Lake email box.

We strongly recommend the long-term solution of Microsoft Exchange Online (discussed further below). This technology is now firmly in the mainstream and provides a substantial cost savings over running your own Exchange server. There is widespread consensus in the IT world that only the largest organizations should consider keeping email on premise.

That said, your migration to Exchange Online will be much simpler and smoother if we first remove the Oakland County server from the picture and begin processing all of your email on your existing server. This recommendation is predicated on the assumption that the status of the server RAID configuration is good and that it can be easily monitored. Removing the Oakland server will also permanently eliminate many of the reliability issues with your current set-up.

Here's a good way to think about it: We call Exchange the "everything is always the same everywhere, all of the time" solution for managing email, contacts, calendars, and tasks (the 4 Outlook 'objects'). Exchange is able to provide this benefit because all of these objects are stored in a single database that users can access in a variety of ways, at any time, from any device that's Internet capable, from anywhere the device has connectivity. No matter how, when, or where you access Exchange, your transactions (sending, receiving, creating/deleting contacts and calendar entries, etc.) are posted to this single database. So when you next access it—however, whenever, wherever—it reflects your prior activity.

The City is not getting this key benefit of Exchange because there isn't one central database—there are *two*: the one on your server and the one on the Oakland County server. So let's eliminate one and start giving your users the value Exchange is supposed to provide.

Here are the steps necessary to eliminate Oakland County from the mix:

- Install filtering to block incoming and outgoing viruses and spam, to replace the filtering that Oakland County is currently providing.
- Adjust your backups so that you are backing up your Exchange database (called the 'store') using appropriate backup technology.
- Assist users in making sure that all email content that is only on the Oakland County server is moved to the City server.
- Pick a cut-over date (usually a Friday) and switch the email flow away from the County sever and point it to yours.
- Provide post-cutover support for users who want to access email from other devices or locations.

This will not only eliminate many existing email headaches, but also leave you in a great position for a later, smooth migration to Exchange Online.

Recoverability. Even with the tightest management of the best-designed IT environments, problems occur. Recoverability addresses your ability to contain the damage and recover from it.

- It could be difficult for you to recover from some kinds of server hardware failure. Your server is not under warranty. We have contacted the manufacturer of the server to verify that they will not extend the warranty. In addition, they said they have only a very small inventory of spare parts for your machine model. While failed disk drives can be readily sourced and replaced, a motherboard failure would be a costly and time-consuming repair. For this reason, we highly recommend that servers always have an active warranty.
- Your risk of permanent data loss is higher than it should be. Your backups are not as complete and robust as they need to be. We found that Cynergy had installed and configured backup software to backup data files. These backups are being done to a network-attached storage (NAS) device located in another building. Colleen had been making BSA backups to an external hard drive.

The backup software Cynergy installed is not capable of making an Exchange or SQL Server backups (necessary for solid backups of BSA). It does not have any "rotation" scheme or "versioning" that would permit restorations of older versions of files in the event that the most current backup is not adequate. It appears that the status of the backups must be manually monitored. There have not as yet been any routine test restores to ensure that the backup data

are good. So while these backups are better than none, they fall far short of accepted best practice.

- As there are no backups being made for the Walled Lake Exchange server, certain catastrophic failures could result in the loss of all email on it. It is not clear what backups are being done for you by Oakland County and whether they can recover individual email messages. Even if they could, other Outlook data (contacts, calendar entries, tasks) could be irrevocably lost.
 - BSA recommends and supports 'SQL Server-aware' backups. As a short-term measure, we installed and configured such backups for you using our own software; these are being stored on the external drive that Colleen was using. We are maintaining 3 weeks of backup data. We are monitoring these backups programmatically on a daily basis. (So far, they've been 100% successful.) These backups meet our standard in all ways with the exception of the configuration of the backup drive itself (see below).
 - Our backups and Cynergy's backups are both stored on devices that do not have disk redundancy (RAID). This means that a failure of the backup device drive could result in the loss of the backups contained on that drive. We recommend that backups be stored (a) on a device with RAID, (b) on multiple devices (without RAID) that are rotated, or (c) in cloud storage.
- Since we did not examine individual user computers, we don't know if any important data are stored on any of them, but if there is data there, it isn't being backed up and is at risk of loss.

We strongly recommend that you inventory the data that matter and institute a new backup architecture that properly protects all important information assets.

- You have not ensured that you have the information you need from your prior IT service providers to maintain and recover from some kinds of problems. While it's not necessary to have it in your possession, you should know what information is required and when/if you discharge a provider, you should ask that this information be turned over to you.

It appears that your prior provider(s) lacked the skills to understand and resolve some of your issues.

Business Value. Business value refers to how well and how cost-effectively your IT architecture meets the needs of your organization.

- Your server is under-configured for the tasks it is performing. Microsoft Exchange (email server) requires a good CPU, a large amount of RAM (memory), and fast hard drives for best performance. In addition, you are running BSA, which requires SQL Server and that also requires a good CPU, a decent amount of RAM, and reasonably fast hard drives for best performance. When you combine these requirements into the same server, you need at least 2 CPUs for good performance.

Your server is a low-end server from a non-mainstream vendor with a single CPU. Your server does have sufficient RAM, however, we suspect that the hard drives are not enterprise grade devices in terms of speed and reliability.

- Using Oakland County servers to receive and forward your mail adds unnecessary complexity and potential failure points and associated service, productivity and other soft costs. The technology used to set this up is out of date and requires maintenance that is not being done. It is not a good email solution.
- We see evidence that users are frustrated by frequent, recurring issues and lack of responsive resolution, which has a negative impact on their productivity, job satisfaction, and trust in the City's IT architecture.
- We're not sure how you ended up with a server that wasn't up to the job, but it suggests misplaced trust in a provider who lacked the skills needed to deliver good results for the City.

Key Recommendations

While we see a host of small improvements you'd probably value, here we concentrate on the big picture: what are the most important things you can do to improve security, reliability, recoverability, and business value? Here they are, in order of priority, taking into account the practicalities and dependences. A discussion of costs can be found in Appendices C and D.

1. Implement robust monitoring of the existing server as soon as possible. If possible, install RAID monitoring software. Institute a program of monitoring and preventive maintenance (managed services). This should include programmatic monitoring of hardware and key services, periodic installation of operating system and other updates, maintenance of hard drives (defragmentation, temp file clean up) and periodic inspection of event logs, anti-virus software, and the health of your Exchange Store. This will immediately reduce your risk of surprise server outages and other issues.
2. Gather a full data inventory and institute robust backups. Make sure that all business-critical data are being stored on the server and are being backed up in a robust manner, including Exchange and SQL Server. Use a backup device with RAID or multiple non-RAID devices or cloud storage to store the backups. Monitor backup performance daily and intervene when things get off track. Perform periodic test restores.
3. Consolidate all of your email onto your existing server and stop using oakgov.com. This will provide immediate benefit in reducing complexity and eliminate problems that arise from the use of the Pop3 Connector (the thing that fetches your email from oakgov.com), and from having email in two places.

Another benefit: as you'll see below, we are recommending that you migrate your email to the cloud as a precursor to replacing your server. Trying to migrate from both the existing Exchange server and oakgov.com may present issues and additional costs that are eliminated by removing the oakgov.com server from the mix, leaving you positioned for a smooth transition to Exchange Online.

4. Migrate your existing Exchange server to Microsoft Exchange Online. This step must be completed before replacing your server. You are currently running SBS 2008. It and its successor, SBS 2011, are no longer offered by Microsoft. The primary advantage of SBS was that it provided file server, application server (e.g. for BSA), and email server licenses and operating software at a very attractive price point for organizations under 75 users. To replace all of this functionality today would require a new file server *and a separate server and licenses* for Exchange 2013.

Implementing Exchange 2013 is a major undertaking that would add significant upfront and on-going costs and complexity, resulting in a significantly higher total cost of ownership than Exchange Online—about 32% higher of the five-year expected life of an Exchange server. Exchange Online is now considered mainstream technology, and the accepted conventional wisdom is that only the largest organizations should consider keeping Exchange on premise.

See Appendix B for more information about Exchange Online, including citations of other local governments who use this service, comments about its security, etc. See Appendix D for a comparison of the costs of Exchange Online compared to a new on-premise Exchange server.

5. Replace your server as soon as practical. The age of the server, the lack of a warranty and the deficiencies of the RAID hardware are the key drivers for this recommendation. A new server will also resolve performance issues. We recommend that you buy a well-known, brand-name server. (We prefer Dell.) Recommended specs are in Appendix C.
6. Assess your workstations, laptops, tablets, and other mobile devices. Based on what we saw of your server and network, someone should review your inventory of user devices and software to assess what risks may be lurking there.

We see that Colleen is using Office 2007, which we assume means others may also be on this version. You should plan to upgrade all installs of Office 2007 or earlier versions soon. In the interim, you should make sure that all Office 2007 installs have been updated to Service Pack 3. All support for Office 2007 ends in 2017. Although Office 2007 with Service Pack 3 will work with Office 365 and Exchange 2013, Microsoft won't fix any issues in this environment, as mainstream support for Office 2007 has already ended. So you should plan on upgrading in the foreseeable future.

Appendix A. Technical Details of Key Assessment Findings

Email/Exchange

Your email is routed through Oakland County's Exchange server at oakgov.com. Email is retrieved from oakgov.com to the Walled Lake Exchange server using your server's SBS Exchange POP3 Connector which had the following issues:

- This connector requires a current and correct list of email users. This list requires upkeep, which was not being done. A number of Walled Lake users were not set up at all. A number of users in the list were no longer on staff. We are working to correct the list.
- The connector also requires the correct oakgov.com password for each user, and these were incorrect in some cases. Passwords were changed some time ago to a common password for all users, but it seems that some users were able to change these passwords and did so without informing the system administrator so that the connector could be updated. (Having the same oakgov.com password for all users does pose some potential security concerns.) We are working to insure that each user's password is correct.
- The connector was receiving "message too large" errors, meaning that some emails with large attachments weren't being delivered. We increased the allowable message size from 10 MB to 60 MB.
- The connector was receiving "invalid message header" errors. Once 5 of these errors were encountered on a given email address, further processing was aborted for that user and hence not all of their emails were retrieved. We set the connector to abort only after 500 errors. We also made a fix to reduce these errors, however, it may not be possible to eliminate all of them. (Any email messages with this error cannot be retrieved into a user's Walled Lake inbox. The only way to tell whether these messages have business value is for a user to compare their Walled Lake email with their oakgov.com email to identify the messages that are not being retrieved, and then to examine the un-retrieved messages on the oakgov.com server.)
- A few users were getting errors in accessing their Walled Lake email mailboxes. We reconfigured their connections to correct this condition.

Once we corrected these issues, many short-term and long-term issues were resolved immediately.

Colleen Coogan asked why it can take up to 15 minutes to receive some emails. Here's the answer: the connector is set to its default of receiving email from the Oakland County sever every 15 minutes. Once initiated, the connector takes some amount of time to retrieve messages; that time will vary depending on the number of new messages to be retrieved. The connector cannot be triggered to start a new round of retrieval until the prior round is completed. For these reasons, the 15 minute interval is required to ensure that all email is received from one round before the next begins. Note that some email might be received in less than 15 minutes: if, for example, oakgov.com receives an email five minutes before the connector is next triggered, then the user will receive that email in about five minutes.

Here's another way that user of this connector may cause users to perceive it as unreliable: The connector only receives emails from the oakgov.com Inbox. Emails in any other oakgov.com folder are only available via the oakgov.com webmail. This behavior is by design and an inherent limitation to doing POP3 connections. For users who use the oakgov.com webmail, this can create additional issues:

- Since emails in Sent Items aren't retrieved by the connector, any emails sent using oakgov.com webmail are only available on oakgov.com webmail and will not appear in the user's Walled Lake Sent Items folder.
- When using oakgov.com webmail, any emails moved from the Inbox to other oakgov.com folders may not be received if the connector did not run before the emails were moved. If moved in a webmail session after the Walled Lake server received them, they won't be moved in the user's Walled Lake folders; this can result in inconsistent folder contents between what's in the users' oakgov.com inbox and their Walled Lake in-box.

- Any emails deleted during a webmail session from any oakgov.com folder, including the Inbox, will not have those deletions reflected in the users' Walled Lake email mailbox. The POP3 protocol does not have a way to detect and propagate those deletions. This is another source of potential inconsistency.

Issues found that indicate inadequate server maintenance

Your server was very far behind on operating system updates. Since many updates are released to close security vulnerabilities, this means your server was not as secure as it should be. Further, a large number of outstanding updates can begin to have a negative impact on server performance.

The reason that your server got so far behind is that, by default, SBS is configured to use the Windows Server Update Services (WSUS). WSUS requires ongoing upkeep, which was not being done. We disabled WSUS. In the process of disabling WSUS, the server began to immediately download and install 150 updates (approximately 6 months of updates).

The server is presently configured so that it does not automatically download or install updates automatically, per the generally-accepted practice for servers. After the server rebooted from the updates, the Exchange System Attendant, Exchange Information Store, and SBS POP3 Connector services did not automatically restart as they are supposed to. This happens on some Exchange servers, so it's important to check when the server is rebooted. If these issues are persistent, steps can be taken to fix them.

The SBS Monitoring database was throwing errors because it had reached its maximum capacity. We installed a clean database and is running normally now.

SharePoint is throwing errors. Unless you are using SharePoint, fixing these can be deferred a subsequent server maintenance window.

You should plan on regular server maintenance to install updates and to check for issues updates can sometimes cause, such as services that don't restart as they should. The regular maintenance should also include inspections of backups, anti-virus software, disk health/space/fragmentation, and event logs.

Issues with your anti-virus protection

Your antivirus status is not clear. In order for anti-virus software to provide the protection it's supposed to, certain things have to happen:

- The virus definitions on each computer need to be updated daily to provide protection from newly-discovered malware.
- Preventative scans should run periodically.
- Someone should monitor detection to be sure they have been handled correctly and require no further attention. Sometimes the software will find a potential problem but not be able to fully resolve it, requiring additional manual intervention.

You are using Symantec Endpoint Protection (SEP) Small Business Edition (SBE), which Cynergy installed. The software has a central management console, Symantec Endpoint Protection Manager (SEPM) installed on the server in which it is possible to view the current status of all machines with SEP installed, provided that all of the clients are "managed". Neither we nor Cynergy has the SEP credentials, but Chris is working on getting them. Without these credentials, we can't tell if the software is working correctly without examining every 'end-point' (computer on which it is deployed). We can't tell if you are properly licensed, if the software is up to date, if all end points are protected, etc.

Cynergy noticed that there was no antivirus installed on the server and installed SEP.

A routine, periodic inspection of this software should be part of a periodic maintenance plan.

Appendix B. Information about Office 365

This appendix describes the Office 365 plans you should consider, and provides basic information about Office 365 and Exchange Online.

We are recommending that in conjunction with replacing your server, you migrate your email to Microsoft Exchange Online. This is Microsoft's hosted (cloud) version of Exchange. It is part of the Office 365 suite. There are many other vendors who offer hosted Microsoft Exchange, but in our opinion, Microsoft's service represents the best value. Many of our clients use either Exchange Online or the full Office 365 suite. It is now accepted conventional wisdom in the IT industry that only very large organizations should consider continuing to operate their own Exchange servers.

We have also recommended that you plan on upgrading outdated versions of Microsoft Office (2007 or earlier); one way to do that would be to purchase an Office 365 plan that includes software to install on user devices.

Is Exchange Online/Office 365 a mainstream, accepted platform?

Yes. Various estimates put the number of users of hosted Exchange services at 20-22 million users worldwide, or about 20% of all Exchange mailboxes. Growth rates are high: the logical time to migrate to this platform is when an organization's on-premise Exchange server reaches end of life (as yours has).

More than one million workers in government agencies and units in all 50 states are already Office 365 users. Among them are:

- San Francisco city and county government
- Los Angeles county
- City of Chicago
- Kansas City
- City of San Jose
- State of New York
- Santa Clara County, California
- Sound Transit, Washington State
- State of Minnesota
- US Department of Veterans Affairs
- US EPA

Is Office 365 secure?

Yes. Microsoft uses a defense-in-depth strategy assures that security controls are present at various layers of the service and ensures that should any one area fail, there are compensating controls to maintain security at all times. Your data are housed in dual, geographically diverse Microsoft Network Operations Centers (NOCs) protected by sophisticated physical security (including network firewall hardware) that is far more robust than you could afford to deploy yourself. Logical layer tools include anti-virus and anti-malware controls, and more. Office 365 services follow industry cryptographic standards such as SSL/TLS (Secure Sockets Layer / Transport Layer Security), AES etc. to protect confidentiality and integrity of data. Microsoft engages in regular risk management reviews, and it develops and maintains a security control framework that meets the latest standards. Internal reviews and external audits by trusted organizations are incorporated into the Office 365 service life cycle.

There are also account and user-level security features help you adhere to compliance requirements, control access to services and content by your users, configure anti-malware / anti-spam controls, and encrypt data.

Here is a link to Microsoft's "Office 365 trust center" that reviews security at a high level:
<https://products.office.com/en-us/business/office-365-trust-center-cloud-computing-security>

At the bottom of that web page is a link to a whitepaper entitled "Security and Compliance Office 365" that provides copious technical detail.

Is Office 365 reliable?

Yes. Microsoft provides a contractual guarantee of 99.99% uptime. Your data are maintained in more than one NOC, with automatic replication; if one NOC has issues, you are automatically 'failed over' to another. Widespread service outages are rare and typically short-lived.

What plans might be appropriate for the City?

The full Office 365 suite includes hosted Exchange, shared and private (per user) cloud storage, online meetings, instant messaging, video conferencing, a corporate social network, full on-line versions of Microsoft Office tools, and can include licenses for Microsoft Office on up to 5 devices per user.

Microsoft offers various government plans that have some of all of these features. Here are the ones that might be appropriate for the city; you can start with Exchange Online and add functionality later by upgrading your plan:

- If the only thing you want from the Office 365 suite is hosted Exchange, you'll want Exchange Online Plan 1. Government pricing is \$3.50/user/month.
- If you are interested in email and the communications suite (the online meetings et al) and cloud storage, you'd want the Enterprise E1 plan, which also includes access to full online versions of the Office tools you know and love (Word, Excel, etc.). It's \$6/user/mo.
- If you want the full Monty including the right to install the latest version of Office on up to 5 devices per user, it's \$17/user/month. We have not done an analysis of the cost to procure Office this way vs. simply purchasing licenses for single or dual installs; the advantage of purchasing it as an Office 365 subscription is that you automatically get upgrades as part of the subscription, so you'll never have to upgrade Office again.

In our analysis of the cost of getting a new on-premise Exchange server vs moving to the cloud, we used the E1 plan pricing.

How hard is it to migrate my email to Exchange Online?

Pretty easy, once we have you disconnected from the Oakland server and have a definitive list of users, email addresses and passwords. (These same steps are also necessary to install a new on-premise Exchange server.) There are a few other readiness steps: verifying your Internet connection speed, verifying that all users are on Office 2007 SP3 or later, installing our remote support agent and the migration software agent, and lastly, setting user expectations.

After we complete the readiness steps and procure your Office 365 licenses, the rest of the process is highly automated. It begins with a "pre-migration" that is completely transparent to users, in which we copy all email that's older than 30 days. Once that step is completed, we choose a mutually agreeable cutover date (typically a Friday), and schedule the final cut-over. The automated tool copies the rest of users' mailbox contents and configures their Outlook for the new service. We arrive onsite the next business day when your office opens, to provide support and to help users who want to sync cell phones or other mobile devices.

Appendix C. Cost of Select Recommendations

We can't estimate the cost of each and every recommendation in our report, but we can for the most important ones.

Please note that all estimates that include purchased components are based on pricing for our standard suppliers at the time we made the estimate. These prices are subject to change. For projects such as new servers, we prepare proposals with detailed cost estimates that are based on hard quotes for which the vendor will maintain pricing for some period, typically 30 days, and would prepare such a proposal for the City if you want us to replace your server.

Please be aware that Nimble Systems does not mark up equipment and software we help you procure. We are a member of Dell's Consultant Network, and as such we are guaranteed to get any Dell business product at the lowest cost Dell offers to anyone, and we pass those prices straight through to you. We are skilled at procurement; we know who the lost-cost vendors of quality products are, and we get special pricing from some of them.

The only time we mark up purchases of equipment or software is if we fund the actual purchase and then invoice you, in which case we add on a commercially-reasonable handling fee. (We arrange for you to pay the vendor directly for most purchases. The things we end up funding are typically low-cost items where there's a reason to procure locally at retail.)

Here are some cost estimates:

1. Implement robust monitoring of the existing server as soon as possible. The cost of the recommended bundle of managed services for your existing server is \$500/month.
2. Gather a full data inventory and institute robust backups. We can't estimate the cost of inventorying your data; that depends on what role you want us to play. The estimated cost of an on-premise backup solution that meets our standard is \$1,900 installed.
3. Migrate your existing Exchange server to Microsoft Exchange Online. Estimated cost is \$3,700-\$4,500, not including readiness activities.
4. Replace your server as soon as practical. Because we are recommending that you move your email to Microsoft's Exchange Online service, you do not need a new Exchange server, only a new file server (which will also be your 'primary domain controller').

We recommend that you buy a well-known, brand-name server. (We prefer Dell.) \$13,500-16,000, including the backup solution estimated above. The hardware/software cost portion of this estimate is based on a server with these key specifications:

- a. 4-core, 2.40 GHz processor, such as the Intel E5-2407
 - b. 16GB RAM
 - c. Chassis should provide room for 8 hard drives, preferably hot-plug
 - d. RAID 5 hardware controller
 - e. Qty 3, 300GB 10K RPM SAS hard drives
 - f. DVD ROM drive
 - g. Windows Server 2012 Standard and licenses for each user
 - h. 3-year warranty that provides for 7x24x4-hour response time, preferably with direct access to US-based support.
 - i. APC Smart-UPS 1500 LCD battery backup
 - j. Symantec Backup Exec software
 - k. A backup appliance for on-site backups comprising a NAS with an initial capacity of 6TB in a RAID-5 configuration.
5. Assess your workstations, laptops, tablets, and other mobile devices. We can assess your user computer hardware and software inventory and produce a report for about \$1,500.

See Appendix D for comparison of the cost of an on-premise Exchange server vs Exchange Online (cloud email).

Appendix D. Comparison of On-Premise vs Hosted Exchange for Email

You expressed special interest in a comparison between these alternatives:

- Replace your existing SBS server with a file server and move your email to the cloud.
- Replace your existing server and keep Exchange on premise (which requires *two* servers, one for files and one for Exchange).

With the demise of Microsoft's Small Business Server as a package that includes Exchange, keeping Exchange on-premise and assuring good performance means you'd end up with two servers where you now have one. One server would provide file services, domain (user and device administration) services and host BSA, anti-virus, and backups. The second server would house Exchange and a backup 'agent' that would allow your file server backups to include Exchange data. Keeping Exchange on-premise also means paying for an email filtering service. (Exchange Online includes filtering.) In either case, we assume that you cease routing your mail through Oakland County's server.

A proper differential analysis compares the cost of migrating Exchange from your server to Microsoft Exchange Online and the on-going support costs for that service, to the cost of putting in a new on-premise Exchange server and maintaining it over its useful life. For the purposes of this analysis, we've used a 5-year useful life for the on-premise server. There is no 'useful life' for Exchange Online. Once you're on it, you're on it; Microsoft provides all updates and upgrades as part of their service.

We've used the higher end of our estimates for all services costs. Purchased components are based on quotes we solicited from our standard vendors; your actual cost for the on-premise server could change if server and software license pricing changes. For Exchange Online, the only purchased item is licensing for the migration software we use (we don't expect that price to change).

Here are the costs for those two alternatives so that you can compare the total cost of ownership of both solutions.

Comparison of 5-year Total Cost of Ownership, Exchange Online (EOL) for 25 users vs. On-Premise Exchange 2013 Standard Server (On-Prem)		
	EOL	On-Prem
<u>Installation</u>		
Purchased components	\$ 750	\$ 7,075
Installation/migration services	<u>\$ 4,500</u>	<u>\$ 8,490</u>
Total installed cost	\$ 5,250	\$ 15,565
<u>Monthly on-going (recurring) costs</u>		
Exchange Online Licenses, 25 users	\$ 88	n/a
Managed Services	<u>\$ 375</u>	<u>\$ 500</u> Includes email filtering for on-prem
Total montly on-going costs	\$ 463	\$ 500
Monthly costs for 60 months	\$ 27,750	\$ 30,000
Server warranty renewal, yrs 4 and 5	n/a	\$ 1,500 Estimated based on prior experience
Backup Exec Agent renewal, annual, 4 years	n/a	\$ 1,200 Estimated based on prior experience
Total 5-year cost of Ownership	\$ 33,000	\$ 48,265
Savings from using Exchange Online	\$ 15,265	32%
Year 6 costs	\$ 5,550	Another new server!

Appendix E. Preliminary Assessment Report

Items Requiring Immediate Attention

City of Walled Lake

February 6, 2015

About this report. We visited your site yesterday and began our examination of your server and network. We have not completed our assessment. However, we've already found some problems that in our opinion are serious enough that they should be immediately addressed. So we are issuing this preliminary report right away to highlight those issues and our recommended amelioration.

Summary: We can already say with confidence that this server is inadequate to the tasks you need it to perform and will be recommending that you replace it. We will address this in more detail in our full report once we have completed the assessment. That said, we found several things that we believe you should address right now, even though we hope you'll replace this server quite soon:

- Risk of data loss. You are backing up neither email nor BS&A data. This is especially troubling given that the health of your server drives can't be determined or monitored, your server does not have robust recovery features in the event of a disk failure (see below), and the drives are being exercised very heavily.
- Possible network security risk. We found that you *may* have security risks at your network perimeter. You are using an off-brand security appliance to which no one has the log-on credentials, making this essentially a "black box". You don't know and we can't tell what it's doing. Further, we see some evidence that this device may be impeding network performance.
- Risk of extended server outage. Finally, we find that you are at risk of an extended server outage on two counts: first, this server is no longer under warranty; it could take days to get parts (if they are even available—it's an off-brand server). Second, this server's RAID configuration is weaker than generally accepted as good practice for a server (more below), and as configured cannot be examined to see if it's healthy, nor can it be monitored to provide early warning of impending failure. Since hard drives are one of the components most prone to failure and yours are exercised heavily, these findings are troubling.

Risk of data loss. Your backups are currently configured to run using software that came with the NAS appliance on which the backups are stored. This software is consumer grade. While it is capable of backing up ordinary files (like Word, Excel, etc.) and appears to be doing so, it cannot backup (and therefore is not backing up) the following:

- Exchange email store
- BS&A data
- Other application data, such as the Pontem Cemetery Manager data

Further if the NAS itself lacks RAID (we haven't examined it yet, but since the device came with consumer grade software this seems likely), you will lose your backups altogether if the hard drive in that device fails. It also appears that no one has done any test restores to verify that data can in fact be restored, and no one is monitoring the backups (such as they are) to be sure they complete properly each day.

Recommendation: Immediately institute temporary cloud backups, at least for the BS&A and Exchange data. We won't know what the best permanent backup solution is for the City until you choose a replacement architecture. However, we could initiate cloud backups today and begin monitoring them daily. There is no required contract or associated long-term commitment; we can turn them off whenever that becomes appropriate. There is no upfront capital investment required.

The monthly cost is \$100 to cover the daily monitoring plus \$0.75/GB of storage. If you back up just the BS&A and Exchange data, your monthly storage cost for the first month would be something around \$150, so the total cost would be about \$250. After the first month, storage would likely drop to under \$100; with monitoring your on-going total cost would be in the range of \$200/month. Set-up would cost about \$200.

These are estimates only. It's hard for us to be more precise right now because we have no experience with the volume of new data you generate each day, which adds to the backup size. The reason for the drop between month 1 and later months has to do with technical details of how our cloud solution performs the first backup for Exchange. (In a nutshell, it keeps a pretty large log file for about the first four weeks, after which the log file is deleted and your cloud storage drops accordingly.)

We do want to make you aware that it could take days to complete the first backup due to the amount of data to upload and the fact that your network performance is poor. However, there is no other solution that can be put in place immediately, without upfront capital investment and without a contractual commitment.

Possible network security risk. You appear to be securing your network perimeter with some kind of software running on an off-brand computer. This solution was apparently put in place by a prior IT service provider. No one knows the log-on credentials to this device, so it is impossible to know what functions it is performing and how, nor to monitor or maintain it. We performed some speed tests and found that you are getting good speeds from Comcast, but access to the Internet is still slow. We suspect that this device might be part of the cause, but of course we can't confirm that because we can't access the device. Even if this device isn't the cause of your network slowness, it's inadvisable to entrust your network perimeter security to a setup that no one understands, no one can access, and no one can support. There are simply too many threats for this uncertainty to be acceptable.

Recommendation: Replace this device immediately with an enterprise-grade, name-brand appliance. We would recommend immediate replacement with a WatchGuard XTM-25 hardware firewall appliance. We particularly like this appliance because it's a great value, very easy to set up, supports secure VPN remote access (should you ever require it) and it provides enterprise-grade protection. It's what we use to protect our own network. The appliance itself is about \$450 including shipping. Installation costs (done as an hourly service) should not exceed \$500, assuming you don't need us to configure any VPN access. It's a great long-term solution for protecting your network.

Risk of extended server outage. Your server does have RAID, which is good. RAID stands for "redundant array of independent disks". The purpose of RAID is to reduce your risk of data loss associated with hard drive failures of various kinds, such failures being among the most common server hardware problems. It accomplishes this via data redundancy: it uses multiple drives and creates a "mirror" of your data and operating environment, so that if a single drive fails the server can continue to operate and no data are lost. When you replace the failed drive, the mirror rebuilds.

There are several ways this mirroring can be accomplished. In order of reliability (from least to most reliable) those are: via software, via 'host RAID' (a facility built into the computer's motherboard), and via 'hardware' or 'true' RAID (a separate card devoted to managing the RAID). Your server has host RAID; the generally accepted standard for a server is hardware RAID.

This 'host RAID' leaves you vulnerable to some kinds of (low-probability) issues that hardware RAID addresses, including some kinds of errors from which you cannot recover. Of even greater concern is the

fact that it's not possible to assess the current health of your drives, nor to monitor that health in real-time, without the addition of specialized utilities that your server lacks. This is of particular concern in your environment for these reasons:

- You have no backup of BS&A or email data. An unrecoverable drive failure could mean complete loss of these data.
- BS&A and Exchange are both drive-intensive applications. Your server's hard drives are exercised heavily and this makes them comparatively more prone to failure.
- Your server is no longer under warranty. It could take several days to procure and install a replacement drive, during which time you would be down.

Recommendation: Install an appropriate utility, verify drive health, and continue to monitor it. Your server is an off brand, so we can't be sure we'll be able to find an appropriate utility. But it does use standard Intel chips, so we have high hopes that we can find a utility that will let us examine the current state of your RAID array, and which will generate event log entries that allow us to monitor drive status in real time. If we can locate a utility quickly and it installs without issue, that work should fit within the scope of this audit. We can provide on-going monitoring for \$100/month. (There is no required contract and no minimum commitment; the monitoring can be turned off at any time with 30 days' notice.)

Assuming you agree that replacing this server will be a high priority that can be accomplished quickly, we don't feel that you have to spend the money to renew the warranty. But if that replacement could take many months (e.g. due to procurement policies), then we should get a quote for the renewal and you should consider that as well.

Summary. Here is a summary of the cost of implementing the immediate risk mitigations outlined in this report:

Item	Installation Cost	Ongoing Monthly Fee*
Cloud backups	\$200	\$200-250
WatchGuard Security Appliance	\$950	n/a
Server health monitoring	Included in assessment	\$100
Totals	\$1,150	\$300-350

* There are no contracts or term commitments required. You can turn any of these services off with 30-days' notice when you have permanent replacements in place and no longer need them.

As we continue our assessment, we'll keep you apprised if we discover any other issues we believe require immediate attention. We can begin any of the recommended mitigation steps outlined above as soon as you approve them. Our final report will outline at least two alternatives for replacing your server with one that is up to the tasks you want it to perform. The first solution will assume you continue to keep all current server functions on premise. The second solution will include a hosted (cloud) Exchange email solution and an on-premise BS&A/file server.