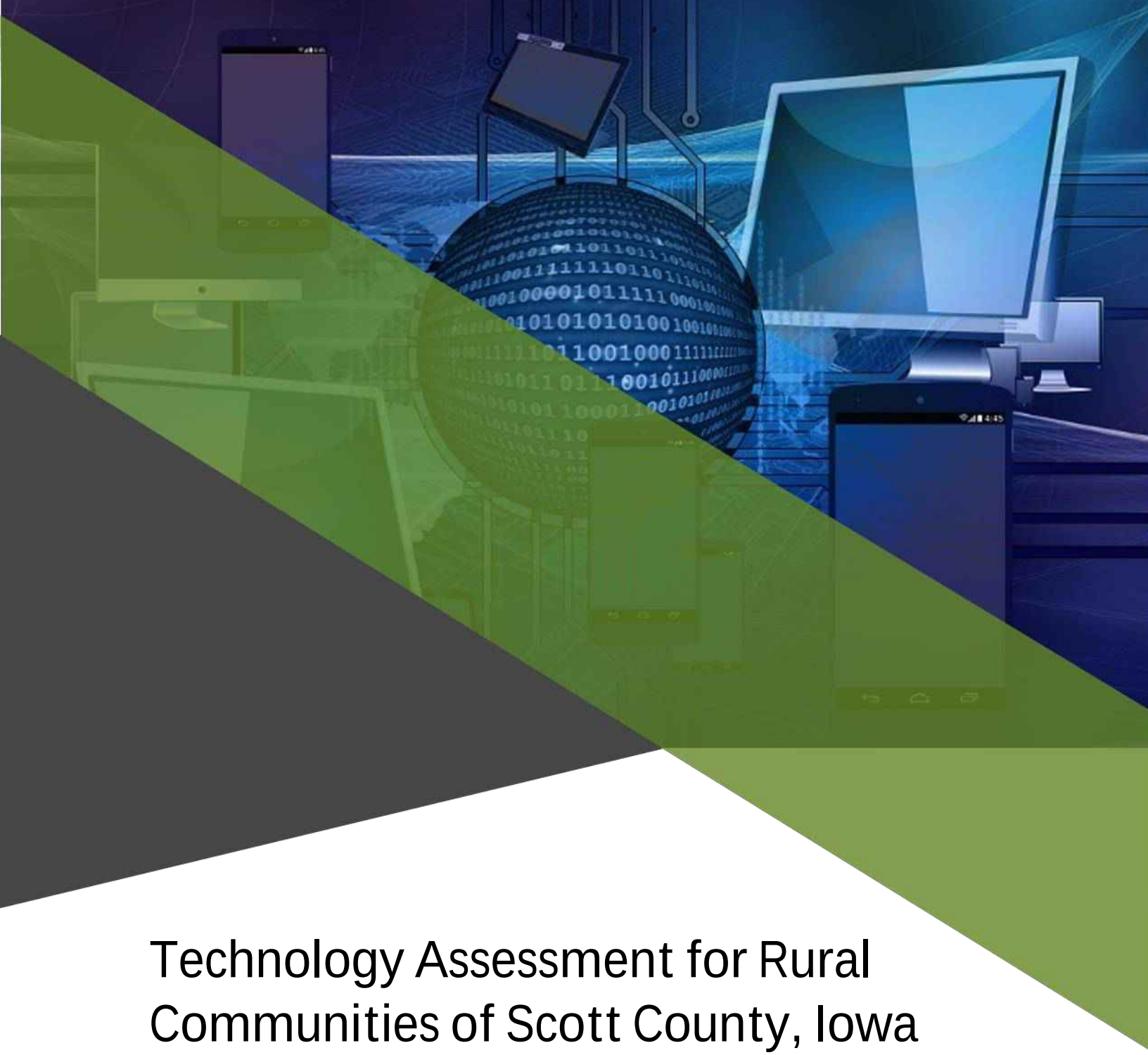


Technology Assessment for Rural Communities of Scott County, Iowa

PHASE II – ASSESSMENT AND PLANNING

March 23, 2018

Presented by
Chandra Oakland, PMP
IT Project Manager
coakland@rkdixon.com
563-359-5900

rkdixon
COPIERS • PRINTERS • IT SERVICES

TABLE OF CONTENTS

INTRODUCTION

RK Dixon was contracted by Bi-State Regional Commission to perform a technology assessment for select rural communities (Figure 1) of Scott County, Iowa. This report details phase two, assessment and planning, of the three part process (Figure 2).

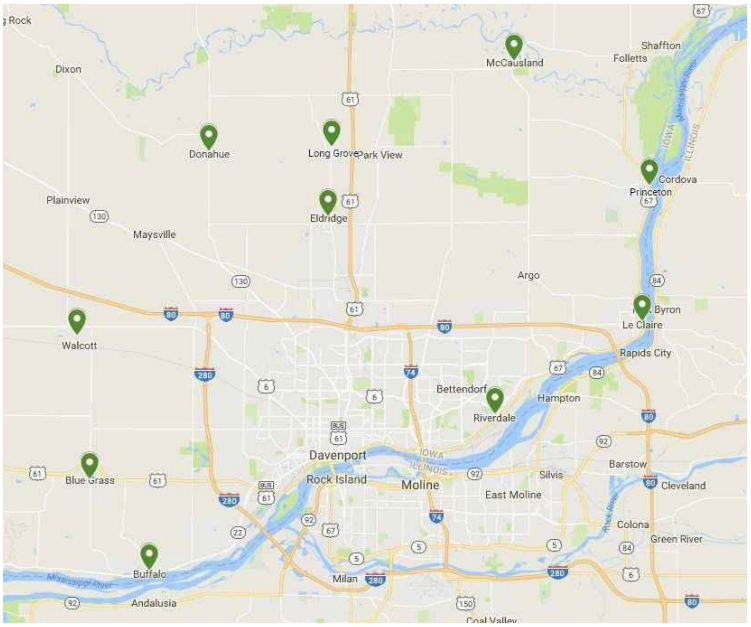


Figure 1

The purpose of phase two, assess and develop to-be design, utilizes information gathered in phase one to develop a SWOT analysis for each community, and to prepare a set of feasible recommendations to affectively support and maintain IT assets and services for each community individually and as a whole.

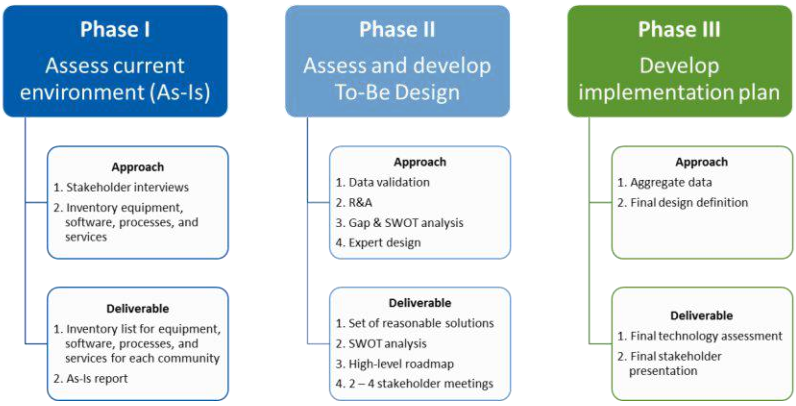


Figure 2

SWOT ANALYSIS

Based on information gathered through interviews and infrastructure assessments in phase one, we have identified key strengths, weaknesses, opportunities and threats for each community.

Blue Grass

	Helpful	*Harmful*
Internal	**Strengths** • Professional-grade firewall	**Weaknesses** • Aging hardware • Missing critical patches and/or updates • End-points missing anti-virus • No offsite backup identified
External	**Opportunities** • Information Security assessment • Risk mitigation and disaster recovery	**Threats** • End-points vulnerable to malicious attacks • End-points vulnerable to failing hardware • Data loss

Buffalo

	Helpful	*Harmful*
Internal	**Strengths** • Costs are low • Off-site backup	**Weaknesses** • Aging hardware • Missing critical patches and/or updates • Consumer-grade hardware • End-points missing anti-virus • No defined IT training, policies or security procedures • No formal central support • New World application support challenges
External	**Opportunities** • Information Security assessment and training • Hardware and procurement upgrades • IT support services	**Threats** • End-points vulnerable to malicious attacks • End-points vulnerable to failing hardware

Donahue

	Helpful	*Harmful*
Internal	**Strengths** • Small population creates limited infrastructure needs • Anti-virus in place	**Weaknesses** • Consumer-grade hardware • No defined IT training, policies or security procedures • No off-site backup identified
External	**Opportunities** • Information Security assessment and training • Risk mitigation and disaster recovery • Hardware and procurement upgrades • IT support services	**Threats** • End-points vulnerable to malicious attacks • Data loss

Eldridge

	Helpful	*Harmful*
Internal	**Strengths** • Anti-virus in place • Central support (Computer Evolution)	**Weaknesses** • Aging hardware • Missing critical patches and/or updates • Consumer-grade hardware • No defined IT training, policies or security procedures • No formal support agreement • New World application support challenges
External	**Opportunities** • Information Security assessment and training • Hardware and procurement upgrades • IT support services formal agreement	**Threats** • End-points vulnerable to malicious attacks • End-points vulnerable to failing hardware

LeClaire

	Helpful	*Harmful*
Internal	**Strengths** • Central formal support (Platinum) • Professional-grade hardware • Anti-virus in place • IT training, policies and security documentation from Platinum	**Weaknesses** • Missing critical patches and/or updates • New World application support challenges
External	**Opportunities** • IT support services renewal	**Threats** • End-points somewhat vulnerable to malicious attacks

Long Grove

	Helpful	*Harmful*
Internal	**Strengths** • Central formal support during current Mayoral term (Integrated Solutions) • Identify Theft Protection policy • Ant-virus in place • Off-site backup	**Weaknesses** • Missing critical patches and/or updates • Consumer-grade hardware • No defined IT training
External	**Opportunities** • IT support services renewal • Hardware and procurement upgrades • Information Security assessment and training	**Threats** • Loss of IT support services after Mayoral term • End-points somewhat vulnerable to malicious attacks

McCausland

	Helpful	*Harmful*
Internal	**Strengths** • Off-site backup • Central support (Geeks Online)	**Weaknesses** • Consumer-grade hardware • No defined IT training, policies or security procedures • No formal support agreement • Public computer on internal network • End-points missing anti-virus • No formal support agreement
External	**Opportunities** • Information Security assessment and training • Hardware and procurement upgrades • IT support services formal agreement	**Threats** • End-points vulnerable to malicious attacks • Data vulnerable to unauthorized access

Princeton

	Helpful	*Harmful*
Internal	**Strengths** • Central support (Shared IT)	**Weaknesses** • Aging hardware • Consumer-grade hardware • End-points missing anti-virus • No defined IT training, policies or security procedures • No formal support agreement • New World application support challenges • No offsite backup identified
External	**Opportunities** • Information Security assessment and training • Hardware and procurement upgrades • IT support services formal agreement • Risk mitigation and disaster recovery	**Threats** • End-points vulnerable to malicious attacks • End-points vulnerable to failing hardware • Data loss

Riverdale

	Helpful	*Harmful*
Internal	**Strengths** • Identify Theft Protection policy • Central formal support (Integrated Solutions)	**Weaknesses** • Aging hardware • Consumer-grade hardware • End-points missing anti-virus • No defined IT training • No backup monitoring
External	**Opportunities** • IT support services renewal • Hardware and procurement upgrades • Risk mitigation and disaster recovery • Information Security assessment and training	**Threats** • End-points vulnerable to malicious attacks • End-points vulnerable to failing hardware • Data loss

Walcott

	Helpful	*Harmful*
Internal	**Strengths** • Password policy	**Weaknesses** • Aging hardware • Consumer-grade hardware • End-points missing anti-virus • No defined IT training • No formal support agreement • New World application support challenges • No offsite backup identified
External	**Opportunities** • Information Security assessment and training • Risk mitigation and disaster recovery • Hardware and procurement upgrades • IT support services	**Threats** • End-points vulnerable to malicious attacks • End-points vulnerable to failing hardware • Data loss

RECOMMENDATIONS

Findings from the technical assessment and stakeholder interviews identified opportunities for improvement in several critical information technology operational areas. Initial planning recommendations are outlined below.

Baseline Infrastructure

Security and non-public disclosure of residents' private information should be a primary focus of public government. Protecting information falls into several categories that include preventing access from non-authorized individuals and hackers, backing up of data both onsite and offsite, and separation of public and internal wired and wireless networks. As a first step, we recommend baselining the infrastructure at each community.

At a high-level, the following would be required at each location:

- A professional-grade firewall and server
- Wired and wireless upgrades, and configurations to isolate public from private information
- Additional, or modified, backup infrastructure
- Antivirus solution
- Continuous infrastructure maintenance, patching, and updating

The challenge then becomes asset procurement and on-going infrastructure support. There a several options for this; however, the feasibility of each varies.

Procurement

As-is, the communities are procuring their hardware independently, from various vendors at various costs. With the exception of LeClaire, all communities are using some form of consumer-grade hardware or operating system. While this method is technically possible and undoubtedly lowers the initial capital expenditure, it could be seriously undermined in the long term by the operating and downtime costs incurred from using less robust technology.[1]

Another procurement challenge is how long to use an asset and when to reasonably replace it. With the exception of LeClaire and Eldridge, all communities reported replacing hardware only 'as needed'. While this method aims at utilizing the hardware for the maximum amount of time, the community runs the risk of increasingly slow response times and even extended downtime for an unexpected asset loss. Additionally, unless the hardware is kept up-to-date, the security risks increase as the equipment ages and ultimately becomes more vulnerable to malicious attacks.

The communities may choose to continue procuring assets independently; however there may be opportunities of scale available should the communities purchase together. Either way, it is recommended that an acceptable vendor list and minimum requirements be established.

[1] McLaughlin, Gavin. (2014, December 01). The hidden risks in consumer-grade storage components. Retrieved from https://www.techradar.com/news/computing-components/storage/the-hidden-risks-in-consumer-grade-storage-components-1275041.

Acceptable Vendors

Establishing a list of acceptable vendors ensures that all communities, independently or jointly, are receiving the acceptable grade equipment at a fair price.

Option 1 The State of Iowa has negotiated set pricing for business-class devices with several select vendors for use by local government employees. A current list of contracts is updated daily and can be found at https://das.iowa.gov/procurement.

Option 2 Purchased through local private vendors equipped in procuring and selling business-class devices.

Option 3 Secure a strategic partnership with Scott County (detailed further in under Support).

Minimum Requirements

Minimum PC specifications to consider

- Processor
- Memory
- Storage
- Graphics
- Optical drive
- Operating system
- Expansion options
- Age
- Anti-virus

Other professional-grade infrastructure requirements to consider

- Server
- Switch
- Firewall
- Router
- Back-up appliance

Procurement Planning

When considering age as a minimum requirement, it becomes increasingly important to plan for asset depreciation and replacement. IT infrastructure assets should be integrated into any existing procurement plan for community expenditures. Rather than replacing as needed, the current age of IT infrastructure equipment should be assessed during fiscal year budgeting and replacement costs should be integrated into budget planning. This could be managed

- Internally by each community
- By a single procurement planner responsible for all communities
- Using strategic vendor relationships who manage the support and procurement process

Larger expenditures, such as servers, are commonly managed through hardware-as-a-service (HaaS) agreements. Similar to leasing, the ownership of the equipment would remain with the managed service provider and not the community. This type of agreement is beneficial because it

- Decreases initial capital costs and allows for consistent expense planning over the life of the agreement
- Releases responsibility of repair through managed monitoring and maintenance
- Alleviates internal replacement planning process and ensures opportune hardware upgrades

Support

When considering the term support, we are referring to

- Remote helpdesk support
    - Infrastructure remediation
    - Desktop/end user support
    - Line of Business (LoB) application and system support
    - Domain user management
- On-site support for
    - All remote helpdesk items
- Standard environment and infrastructure policies
- Infrastructure monitoring and maintenance
    - Backup monitoring
    - Server, network and internet circuit monitoring
    - Server drive space and service monitoring
    - End-point patching and updates
    - Anti-virus/anti-spam services
    - Network performance reporting
- Professional-grade hardware and software procurement capabilities and incentives

As-is, all communities are securing IT support independently of each other: either internally or through various vendor relationships. With the exception of LeClaire and Riverdale, no other communities have secured a formal IT support agreement. The drawback to separate operations is each community is independently responsible for securing their own support at full costs. Depending on access to reliable information, finding credible and secure support may be a challenge.

Shared Support

Rather than securing support independently, another approach would be to contract with a vendor for IT support of the individual community infrastructures at a shared cost. The benefits of this approach includes

- A reduced need for IT knowledgeable personnel within each community
- Streamlining the support process and increasing efficiencies
- The ability to leverage buying power for all IT assets across all communities
- The ability to distribute support costs across all communities

Vendor selection becomes the critical path for this option. Vendors need to be competent in end-user support, infrastructure, backup, recovery, and security with a focus on government requirements. They would need to be a capable liaison for the various line-of-business applications utilized by each community (i.e. New World). Additionally, they would need to prove their capability to geographically support all of the communities and be able to distribute costs at a prorated rate based on community size.

Option 1 Secure a shared IT support agreement with a private vendor. There are serval options for this path, including vendors who are already working with some of the communities. In Appendix A you will find high-level information for three private managed service support vendors who would be qualified to support the communities.

Option 2 Secure a strategic partnership with Scott County. As-is, the communities are receiving support from Scott County for New World applications only. Unfortunately, this support relationship is not backed by a formally outlined agreement. As summarized in the Phase I – AS-IS report, this undocumented relationship has ultimately created tension between the communities and Scott County.

When asked about the current relationship, Scott County IT Director Matt Hirst stated he, "expects [the communities] are very frustrated". The county is doing the best we can to support them; however the short-sighted leadership that was involved in the development of the SEC consolidation has helped to create where we are." Without additional funding, the county does not have additional support to efficiently distribute to the communities brought on during the consolidation.

While the current relationship is not ideal, with the right collaboration and agreement there is a genuine and unique opportunity to develop a strategically beneficial partnership between the communities and Scott County. When considering vendor selection, Scott County meets all of the capabilities to support the communities while offering some unique differentiators that may not be recognized through a private vendor.

Their exclusive government-only operations make them an ideal partner for the communities. The word 'partner' is intentionally used here and meant to signify that this would not be a typical vendor-customer relationship. While there would be a formal agreement with associated costs, it is significant to highlight that Scott County is a not-for-profit organization. This may help alleviate and reduce the joint costs incurred by the communities for this support.

Scott County also offers significant economies of scale. As it stands, they support over 900 network accounts and recently purchased and deployed over 500 computers for upgrades.

Appendix B details further high-level support information for Scott County.

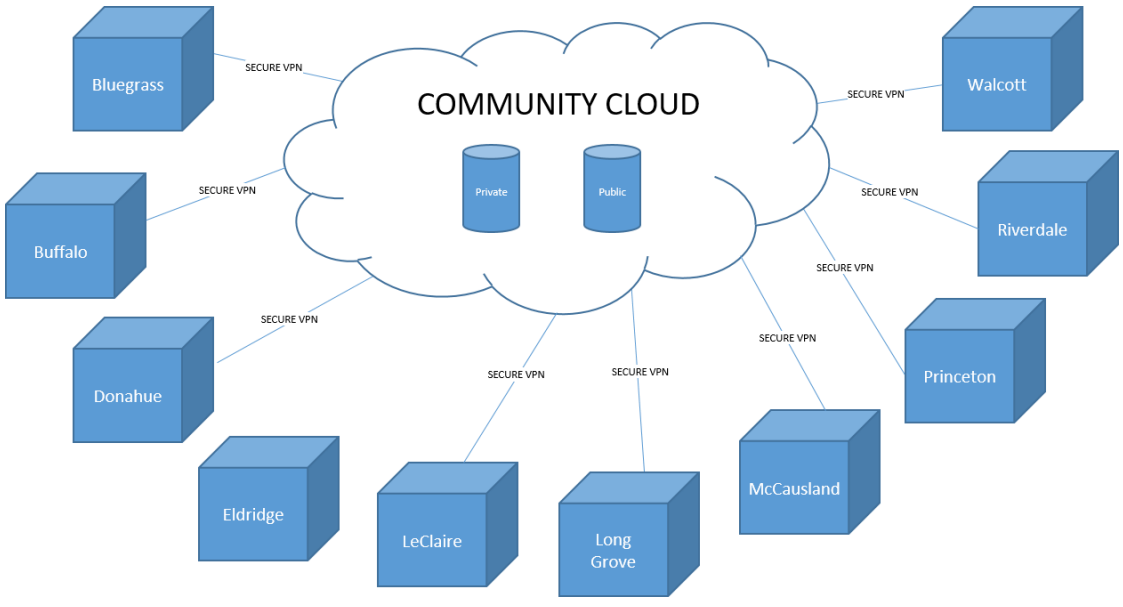
Consolidate Infrastructure

There is an option to combine all of the communities' infrastructures into one single parent\child remote infrastructure relationship. In this model, all of the infrastructure would be either, private, or public, or cloud based. The communities would share a common cloud infrastructure, thus sharing costs, while maintaining separation of governmental agencies.

The following excerpt from StateTech.com summarizes how the cloud has helped the state of Indiana:

> The state of Indiana's private community cloud significantly cut IT expenses and has encouraged the IT department to deepen its commitment to the cloud. "For new proposals, we consider the cloud first, then we determine if there are any unique reasons why the cloud wouldn't make sense," says Jim Rose, the state's chief technology officer.
>
> The private cloud uses VMware virtualization technology and runs about 75 percent of the state's servers. Agencies no longer invest in their own hardware and software for web -servers and other IT resources, but instead pay a set monthly service fee based on use. That has helped to shutter several data centers, and save the state about $14 million annually, Rose says. Those savings are important, but they're not the only benefit. Having a mature cloud strategy in place is essential for future IT success, Rose says.[2]

Like Indiana, this approach may be the least cost option long-term for all communities to efficiently utilize and maintain an updated infrastructure environment. As with shared support, the correct vendor selection is critical in leveraging all of the benefits of a shared infrastructure.



[2] Joch, Alan. (2017, April 10). Local governments take cloud to the next level. Retrieved from https://statetechmagazine.com/article/2017/04/local-governments-take-cloud-next-level.

Beyond the Baseline

Based on information gathered in phase one, there are additional beneficial opportunities available for the communities to leverage beyond standardizing, updating and securing their infrastructure.

FISA™ Security Assessment

Results from the technical assessment and information gathered during stakeholder interviews suggest several communities would benefit from a baseline security technical assessment. The Fiducial Information Security Assessment is the most objective and comprehensive measurement of information security risk available in the market. It was designed by engineers at FRSecure, who average more than 15 years of information security experience, with these specific objectives in mind:

- The assessment is based on risk. The most effective way to manage information security is based on risk, not on specific controls that may or may not fit for your organization.
- The assessment is easy to understand. *Easy to understand* and *effective* are not mutually exclusive. In fact, they usually go hand in hand. The most effective information security programs are typically simple and effective. Complexity is often the enemy to good security.
- The assessment is comprehensive. Information security is not an IT issue; it is a business issue.
- The assessment is objective. FISA™ scoring is as objective as is possible given what we know about threats, vulnerabilities, exploits and risk in general. Each assessed control is given a risk metric based on professional opinions, best practices, and real-life data.
- The assessment is clear and free from technical jargon. Terms like "NextGen", "Internet of Things" (IoT), "Advanced Persistent Threats" (APT), etc. are all avoided as much as possible.
- The assessment leverages and references current security frameworks and standards such as ISO/IEC 27001:2013 and the NIST Cybersecurity Framework (CSF). This is very good news for organizations that have built their information security programs per one or more of these frameworks and helps to lend to the credibility of the assessment.

For smaller organizations, there is FISA-SB™. Small to medium sized organizations in particular are vulnerable. According to governmental agencies, there are 28.8 million small businesses in the United States. The latest Symantec Internet Security Treat Report (ISTR) indicates that 1 in 40 small businesses are at risk of cyber-attack. A FISA-SB™ allows small organizations to know and understand how they are vulnerable and how they compare with peers within similar industries. The FISA-SB™ is constantly calibrated to the latest security threats used by attackers with controls designed to medicate those threats and protect data from unauthorized access, disclosure, distribution and destruction.

KnowBe4 Security Awareness Training

Along with a security assessment, it is important to train users on proper IT security awareness. No communities identified having standard IT training. KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform with over 16,000 customers.

KnowBe4 security awareness training provides baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack. After identifying your baseline, train your users with the world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. See the results with enterprise-strength reporting, showing stats and graphs for both training and phishing.

Disaster Recovery Planning (DRP)

Half of the communities assessed did not have sufficient offsite backup and/or monitoring to effectively recover from a total loss. Today, a total loss doesn't only happen when natural disasters strike; it can happen in seconds as a ransomware virus encrypts every end-point on the network.

In a 2018 report from The Center for Digital Government, it details just how important disaster recovery is:

> In 2016, a ransomware virus took control of the desktop computer of a city of Sarasota, FL, employee. The virus encrypted three servers and 160,000 files, rendering them inaccessible, as cyber criminals demanded up to $33 million in Bitcoin as ransom.
>
> Unfortunately, Sarasota's experience isn't unique. The U.S. Department of Justice estimates more than 4,000 ransomware attacks have occurred every day since the beginning of 2016, and government is a prime target. According to a recent Bitsight report, government agencies had the second-highest rate of ransomware and the second-lowest security rating among six industries examined. Given such risks, a robust disaster recovery and data protection plan is critical for any state or local government organization.

The report concisely summarizes four critical best practices for local governments to employ to successfully execute disaster recovery planning:

1. Implement an automated backup solution
2. Take a 3-2-1 approach to data storage and recovery
    a. 3 copies of data
    b. 2 of those copies on different media, such as disk and tape
    c. 1 copy of data backed up off site
3. Ensure strong data recovery capabilities are in place
    a. Rapid recovery
    b. Verified recoverability
4. Confirm complete data visibility
    a. Collect the right data
    b. Monitor multiple environments
    c. Provide real-time issues discovery

Fortunately, for Sarasota, they were prepared and equipped for response:

> Sarasota avoided paying millions to cyber criminals because it employed effective disaster recovery practices. By following the 3-2-1 rule for data storage, Sarasota ensured backups were consistent and successful and was prepared with a rapid data recovery solution. Its plan provided end-to-end visibility to monitor and effectively respond quickly to a crisis. "If we hadn't been able to recover our files, we would have

had massive data loss affecting all facets of the city and ultimately, it would have impacted our citizens," says Rodriguez.[3]

NEXT STEPS

This report is being presented in conjunction with two to four stakeholder meetings. The stakeholder meetings will

- Include key stakeholders from participating communities, representatives from Bi-State Regional Commission, and representatives from RK Dixon
- Summarize information gathered during the AS-IS technical assessment and stakeholder interviews
- Review initial planning recommendations and various feasible options
- Allow community stakeholders to ask questions and participate in the decision-making process that will shape and define the long-term strategic technology plan for rural communities of Scott County

Once the stakeholder meetings have commenced, the final phase of the assessment will be to develop an implementation plan for select technical strategic solutions.

[3] 4 Best Practices for State and Local Government Disaster Recovery Planning. © 2018 Center for Digital Government Content Studio. Retrieved from http://www.govtech.com/library/papers/4-BEST-PRACTICES-FOR-STATE-AND-LOCAL-GOVERNMENT-DISASTER-RECOVERY-PLANNING-98247.html.

APPENDIX A – PRIVATE MSPS

On a high level, Platinum offers four services that would relevant to the project you have outlined.

1) IT Complete Support
2) Hardware- Software acquisition I management, including Office 365.
3) Proactive Network Management I Monitoring
4) On-Site I Off-Site backup programs.

All of the above mention programs are charged on a per server/per pc basis.

IT Complete provides an interactive helpdesk manned five days per week from 7:00AM to 5:30PM. All calls are answered by a live local voice. 80% of the service calls are handled remotely by this staff. For issues requiring an on-site technician, they are dispatched by the helpdesk at no additional charge. Services run from end-user break I fix to full server management. Also included is a partnership with the ERP software provider to provide a local set of hands, ears and eyes for trouble shooting and software updates. As mentioned above, all fees are based on the number of computes supported and does not increase after a certain number of hours are expended each month.

Hardware I Software acquisition. Our annual sales with vendors like Dell and Microsoft gives us excellent pricing, which we pass on to our clients without a not mark up.

Proactive Network Management I Monitoring. We monitor networks 24x7, 7 days per week with a 15 minute notification of any event. Many of the problems detected by the monitoring service is fixed on the flat fee based IT Complete. This service also allows patch management on network software as well as pushes for desktop software ERP programs. Anti-Virus, Anti-Spyware, Web content Filtering and remote pc access through Log-Me-In is part of this service.

On-Site I Off-Site Backup. A hardware appliance is placed at each location with a server. The backup covers data as well as OS and application software. On a regularly scheduled basis, a snap shot is taken and stored on the local backup device. This allows client data to be restored from the date the device was initially installed. On a nightly basis, the backup for the day is transferred to an off-site location in case something happens to the local office. In addition to backup, the local device can act as a local VMware server to provide network services in case of server hardware I software failure. This can also be achieved from the remote location in case the local office is destroyed. The local device can be right sized to accommodate the needs of the various communities.

CompuSuite, Managed IT Services by RK Dixon, offers a comprehensive IT service plan that is driven by metrics and focused on providing your organization with world-class support. We have dedicated service delivery areas, each specializing in a certain facet of your IT support:

Support Services

Support Services is responsible for handling the reactive work that occurs when you encounter an incident relating to your company's IT needs. We aim to provide world class customer service by getting to know how your company operates. We are staffed in a centralized location which allows you to submit a service ticket directly to our team via e-mail, customer portal or phone call. Our team is built around skilled engineers that have a wide range of experience and technical abilities allowing us to efficiently resolve your issues. Our goal is to ensure there is minimal impact to your business so that you are free to do what you do best while we do ours.

Centralized Services

Centralized Services ensures we have visibility and control of your IT infrastructure. Critical IT infrastructure such as servers, routers, switches and access points are monitored for hardware and software failures. We ensure your IT infrastructure is secure with the use and monitoring of vital anti-virus software, deploying critical software patches and state-of-the-art backup solutions. We'll provide your company with a periodic technical report providing visibility to important IT metrics, empowering you to make crucial business decisions. Centralized Services can also help your company stay on the leading edge by utilizing advanced cloud solutions.

Network Administration

Your Network Administrator plays a critical IT role by providing proactive services such as accurately documenting and inventorying your environment and performing recurring on-site preventative maintenance. The Network Administrator will collaborate with Centralized Services to ensure all IT infrastructure is being monitored. Recurring on-site visits allow the Network Administrator to verify server and network health, maintain backup solutions and perform an IT risk assessment. The IT risk assessment identifies key areas of your infrastructure that may need to be addressed to ensure the greatest level of performance, reliability and security. By keeping your IT environment in proper technical alignment, your Network Administrator will develop an advanced understanding of how your business operates, allowing us to provide you with world-class service.

vCIO

We provide our customers with a dedicated vCIO (Virtual Chief Information Officer) with technical skills and sound business acumen to ensure continual delivery of high-value technology consulting while reducing IT related business risks. Vendor management, technology planning and budgeting helps ensure the best possible technology recommendations for your IT investment.

CompuSuite, Managed IT Services by RK Dixon	Service Plan		
Service Delivery Areas	Ultimate	Essentials	Basic
Support Services			
On-site Support (M-F 7am to 5pm)	✓		
Remote Support (M-F 7am to 5pm)	✓	✓	
Help Desk (M-F 7am to 5pm)	✓	✓	
Remediation of Infrastructure & Monitoring Alerts	✓	✓	
Desktop / End User Support	✓	✓	
Line of Business Application/System Support[1]	✓	✓	
Domain User Management - Adds, Changes, Deletions	✓	✓	
Billable After-Hours Support (Weekends and Holidays)	✓	✓	
Centralized Services			
Monitoring Backups & UPS protection[2]	✓	✓	✓
Monitoring Server, Network Devices & Internet Circuits[2]	✓	✓	✓
Monitoring Server Drive Space & Critical Services[2]	✓	✓	✓
Monitoring Network Device CPU Load/Throughput[2]	✓	✓	✓
Operating System Security Patching	✓	✓	✓
Anti-Spam/Virus Services - Licensing, Monitoring & Remediation	✓	✓	✓
Network Performance Reporting	✓	✓	✓
Network Administration			
Develop & Maintain Technical Documentation	✓	✓	✓
Scheduled On-site Preventative Maintenance	✓	✓	✓
Assess Technical Alignment Against Our Best Practice Standards	✓	✓	✓
Identify Technical Risk	✓	✓	✓
Verify Centralized Services Monitoring	✓	✓	✓
Ensure Network Usability	✓	✓	✓
Review of Service Delivery	✓	✓	✓
vCIO			
Align Technology Strategy with Business	✓	✓	✓
Advise & Prioritize Technology Goals	✓	✓	✓
Budget Planning & Lifecycle Management	✓	✓	✓
Technology Scorecard	✓	✓	✓
Identify Business Risk Associated with Technology	✓	✓	✓
Scheduled On-site Review	✓	✓	✓

SHARD IT COMPANY OVERVIEW

Shared IT was started in 2000 by Kevin Stutting and has been growing steadily over the years. Shared IT has empowered many Quad City businesses to focus on their core business while leveraging our team to manage their technology needs.

Shared IT has been given the responsibility to manage and support local city entities in our area that included Princeton and Eldridge Iowa. This has given great insight on the environment and technology to provide best practices for a city-based network.

Our carefully crafted staff consist of professional technology experts that combine a hobbyist enthusiasm. We pride ourselves on constantly growing in various technologies and meeting the unique needs of each our clients. Our hands on day-to-day experience combined with continuous training keep us on top of the leading technologies that we implement for our sites.

Our mission is to meet the unique needs of our clients. No two clients are the same. We recognize this and embrace the uniqueness of the client and empower the client to meet their goals using technology.

Shared IT sets themselves apart by focusing on the relationship with the client. We have remote support capabilities when needed, but pride ourselves on the service we provide onsite - interacting side-by-side with users. We provide great customer service that creates a comfortable environment for your staff and executive team.

INFORMATION REQUESTED

RK Dixon requests information detailing an IT service plan that would support the below communities, individually or as a group, including general cost estimates

- BLUE GRASS
- BUFFALO
- DONAHUE
- ELDRIDGE
- LECLAIRE
- LONG GROVE
- MCCAUSLAND
- PRINCETON
- RIVERDALE
- WALCOTT

SHARED IT SUPPORT REQUEST DETAILS

SUPPORT REQUEST BRIEF REVIEW:

Items below are requested items that are included with Shared IT's Managed IT Services:

SUPPORT ITEM	PROVIDED	SUPPORT ITEM	PROVIDED
INFRASTRUCTURE REMEDIATION	YES	SERVER, NETWORK AND ISP CIRCUIT MONITORING	YES
ON-SITE AND REMOTE SUPPORT	YES	SERVER HEALTH AND DRIVE SPACE	YES
DESKTOP/END USER SUPPORT	YES	END-POINT WINDOWS & THIRD-PARTY PATCHING/UPDATES	YES
LINE OF BUSINESS APPLICATION/SYSTEM SUPPORT	YES	ANTI-VIRUS/ANTI-SPAM MANAGEMENT	YES
DOMAIN USER MANAGEMENT	YES	NETWORK PERFORMANCE MONITORING & REPORTING	YES
BACKUP MONITORING (BUSINESS GRADE)	YES		

SPECIAL REQUIREMENTS:
Each site will require a supportable network review, documentation creation & network discovery during the first few months of Managed IT services.

All of the sites/entities listed can be managed as a whole by Shared IT with a sub-scope charter that defines each entities hours, projects and specific technology needs.

Adding and removing sites/entities can be accomplished and must follow defined guidelines.

SUPPORT REQUEST DETAILS:

INFRASTRUCTURE REMEDIATION
Each city's IT infrastructure will be evaluated, and a plan will be mutually developed to address any issues that require remediation.

ON-SITE AND REMOTE SUPPORT / DESKTOP & END USERS SUPPORT
Each operation or issue may require/warrant on-site or remote support. Shared IT technicians can either come onsite or use remote access tools for each scenario to best support, assist or manage client tasks.

LINE OF BUSINESS APPLICATION/SYSTEM SUPPORT

Where desired, Shared IT will gain the skill set to provide end-user support to line of business applications in use.

DOMAIN USER MANAGEMENT
Shared IT technicians will use best practice and client standards to manage user accounts, groups and security access.

BACKUP MONITORING (BUSINESS GRADE)
Shared IT highly recommends the use of business grade backup solutions based on the 3,2,1 standards**. These tools allow for easy management and monitoring by our technical staff.

** 3,2,1 STANDARDS
3 COPIES OF THE DATA, 2 MEDIUMS, 1 OFF-SITE

SERVER HEALTH, SERVER DRIVE SPACE, NETWORK AND ISP CIRCUIT MONITORING
Shared IT uses layered business grade utilities to monitor and proactively support Server, network and circuits. Regularly scheduled routine checks, thresholds and alerting are used to monitor each site.

END-POINT WINDOWS & THIRD-PARTY PATCHING/UPDATES
Each site is different and requires different approaches to patch/update management. Shared IT will use tools that fit each site to maintain a healthy patched network environment.

ANTI-VIRUS/ANTI-SPAM MANAGEMENT
Our technicians support a wide range of Anti-Virus products. We can recommend various products depending on the client. We regularly manage virus definition updates, regular scans and unique system policies (exclusions, application friendly policies)

NETWORK PERFORMANCE MONITORING & REPORTING
Network monitoring is important by recognizing that a site is running well. Shared IT applies business level best practices, routines and utilities to monitor network traffic. We are notified when anomalies impact a network.

CAPABILITIES AND EXPERIENCE

SHARED IT TEAM CORE CAPABILITIES, EXPERIENCE AND FIT

CORE CAPABILITIES	• TEAM ORIENTED SUPPORT & PROBLEM SOLVING • UNIQUE / CREATIVE SUPPORTABLE SOLUTIONS • DOMAIN ADMINISTRATION • END-USER SUPPORT (SOFT SKILL DRIVEN) • VIRTUAL ENVIRONMENT ADMINISTRATION (VMWARE, HYPER-V) • SERVER ADMINISTRATION MONITORING • NETWORK ADMINISTRATION MONITORING • MULTI-VENDOR/SOFTWARE SUPPORT (WE DON'T REQUIRE YOU TO PURCHASE A CERTAIN TECHNOLOGY BASED ON OUR SUPPORT. WE RECOMMEND BUSINESS GRADE TECHNOLOGY) • CUSTOM APPLICATION CREATION • HIGH-LEVEL STORAGE MANAGEMENT • END-USER VPN & REMOTE ACCESS • SECURITY AND NETWORK BEST PRACTICE
HIGH-LEVEL EXPERIENCE	• MULTI-SITE NETWORKS • VMWARE / HYPER-V VIRTUAL ENVIRONMENTS • COMPLEX WINDOWS DOMAIN ADMINISTRATION • COMPLEX DATA & SERVICE MIGRATIONS • COMPLEX & REDUNDANT NETWORK CONFIGURATIONS • HIGH-LEVEL STORAGE MANAGEMENT • DEEP NETWORK ANALYSIS

PRICING MODELS

SHARED IT PRICING MODELS

SHARED IT MANAGED IT (HOURS PER MONTH)	• UP TO 12 HOURS PER MONTH – $XXX / HOURS EXCEEDING 12 PER MONTH WILL BE BILLED AT $X/HOUR
ADDITIONAL DISCOUNT BUCKET OF HOURS *(PURCHASED WITH MANAGED IT SUPPORT ABOVE FOR UPCOMING PROJECTS AND OVERAGES)*	• 10 BUCKET HOURS @ 20% DISCOUNT RATE *THIS CAN BE USED FOR OVERAGES AND IT PROJECTS*

SHARED IT SUPPORT BUCKET	• 12 BUCKET HOURS TO USE OVER 12-MONTHS AS NEEDED / 1-TIME OR MONTHLY INVOICING

MANAGED IT AGREEMENT & SCOPE EXAMPLE

PROJECT CHARTER DOCUMENT

PROJECT NAME: SCOTTY COUNTY RURAL AREAS MANAGED IT SERVICES
DATE: 4/12/2018
PAYMENT: MONTHLY INVOICING
STAKE HOLDER: N/A

EXECUTIVE SUMMARY

Each city entity is committed to serving their community and residents; this will require Shared IT to focus on their unique technology needs. The cities can be managed as a whole by Shared IT with a sub-scope charter that defines each entities hours, projects and specific technology needs.

Shared IT works in the best interest of the client and will work alongside each city entity on technology best practice, network changes and cost analysis. Shared IT technicians will create and maintain on-going documentation and topology diagrams.

Managed IT Services provide proactive monitoring of server health, backups, anti-virus, windows/third-party patches, network traffic, ISP circuits and network devices. Shared IT will work on-site and remote support for day to day IT operations, end-user support and assisting with technology solutions. End users are encouraged to open support tickets for day-to-day issues. Projects are defined through project charters with a scope, deliverables, cost and a tentative deadline.

- BLUE GRASS
- BUFFALO
- DONAHUE
- ELDRIDGE
- LECLAIRE
- LONG GROVE
- MCCAUSLAND
- PRINCETON
- RIVERDALE
- WALCOTT

MANAGED IT SCOPE

- Services will be provided when possible during regular business hours 8am-5pm CST.
- The project charter defines professional services only, no hardware or software is included in the scope of this charter.
- Additions to the site and project-based services will require a separate project charter.

- Supportable network and discovery will need to be done in the first 3 months of Managed IT services.
- When project hours exceed the bucket of hours, the client will be invoiced at an hourly rate in ½ hour increments.

SUB SCOPE DEFINITIONS (EXAMPLE)

BLUE GRASS MANAGED IT EXAMPLE	• UP TO 10 HOURS A MONTH / 12-MONTH AGREEMENT • SUPPORTABLE NETWORK REVIEW, DOCUMENTATION CREATION & NETWORK DISCOVERY / FIRST 3 MONTHS
LECLAIRE MANAGED IT EXAMPLE	• UP TO 20 HOURS A MONTH / MONTHLY INVOICING / 12-MONTH AGREEMENT • SUPPORTABLE NETWORK REVIEW, DOCUMENTATION CREATION & NETWORK DISCOVERY / FIRST 3 MONTHS
DONAHUE / SUPPORT BUCKET OF HOURS EXAMPLE	• 12 BUCKET HOURS TO USE OVER 12-MONTHS / 1-TIME OR MONTHLY INVOICING

APPENDIX B – SCOTT COUNTY

Scott County has identified the mission of the Information Technology Department as:

To provide dependable and efficient data and voice services for County employees by:

- Informing, educating and empowering employees with technical knowledge
- Researching, installing, and maintaining innovative computer and telephone solutions
- Implementing and supporting user friendly software systems

Scott County Information Technology is a customer service organization with three primary functions:

- Applications – Support commercial off-the-shelf software as well as develop custom applications meeting business requirements.
- Networking - Develop and administer the voice and data network infrastructure to support the business environment.
- GIS/Web - Develop methods of information and application deployment centralized in nature.

Scott County Information Technology is a technical resource and liaison for their customers:

- Facilitates outsourcing of hardware service and support where feasible.
- Advocates/Consults on technology issues with hardware/software vendors, external consultants, and service providers.
- Provides technology guidance and support from acquisition to decommission.
- Tracks and accounts for technology hardware and software maintenance and licensing.

When considering Scott County as a partner for community IT support, Scott County recognizes both organizations are funded by property tax and shared services allows for the best cost for the taxpayer.

Example agreement services include:

A) Scott County Information Technology will monitor, administer, and maintain a network including the following:
    a. Servers
    b. Storage
    c. Network equipment
    d. Printers and multifunction devices
    e. PCs and/or thin clients
    f. Internet services
    g. Telephone services
    h. Other services

B) Monitoring, administration, and maintenance will include the following:
    a. Security and access control
    b. Updates and patches
    c. Anti-virus software
    d. Spam filtering
    e. Data backup and recovery
    f. Technology trouble shooting
    g. Liaison with ISP, telephone, hardware and software vendors for problem resolution

C) Additionally, Scott County Information Technology will also provide the following services to documented partners:
    a. Procuring approved hardware
    b. Installing approved hardware
    c. Procuring approved software
    d. Installing approved software