Dover School District – SAU #11

IT ASSESSMENT REPORT

August 18, 2015

Prepared by:
Neoscope Technology Solutions
30 International Drive, Portsmouth, NH 03801
603-505-4902
www.neoscopeit.com

Contents

About Neoscope

Founded in Derry, NH in 2006, Neoscope is an expert provider specializing in information technology solutions for schools, businesses, municipalities, and non-profits, growing over 33% year-over-year for the past nine years. Our customers range in size from 30 to 10,000 employees. We work with businesses in all verticals and municipalities including multinational companies with complex compliancy requirements. Our staff strives to fulfill the diverse needs of organizations by leveraging technology to increase efficiencies. Our professional scope ranges from infrastructure systems assessment, design and engineering to custom managed and help desk support as well as staff augmentation. Our vendor partnerships with industry titans allow us to design and implement scalable and affordable solutions; we analyze the specific requirements of your organization and design a tailored solution to fit your needs and budget.

Through our strategic partnerships with vendors as well as other service organizations we're able to serve our client's geographically disperse offices throughout the continental United States and provide the best possible service. Our operations are based in Portsmouth NH as is our helpdesk.

Our local community focused approach is paramount to our goal of keeping and growing jobs in NH so that we can keep our local communities thriving. We hire interns for IT, sales and marketing positions directly from the local colleges, to give them learning opportunities in a fast pace industry leading MSP Company.

Why Neoscope?

- ✓ Quality of service guaranteed by a service level agreement (SLA)
- ✓ Turn 80% of variable labor costs into predictable monthly fees
- ✓ 30% to 50% less expensive than traditional IT support
- ✓ Access to a national team of computing professionals 24x7x365
- ✓ Rapid response, critical issues resolved as alerts are generated, client survey rating 4.8 of 5.0
- ✓ Regular monthly report review meetings with your account manager
- ✓ Field engineers and consultants available for on-demand projects
- ✓ Extensive range of products and services to support your business

Industry Awards and Credentials

2013 and 2014

The annual MSPmentor 250 report identifies the world's top managed services provider (MSP) experts, entrepreneurs, and executives.

2013 and 2015

CRN's annual Next-Gen 250 identifies solution providers that are on the cutting edge of technology and business model shifts, driven by their focus on IT markets.

Neoscope strives to bring the most qualified personnel and experience to this opportunity with the Dover School District and Town of Dover. A few of our certifications include Microsoft's MCP, MCSA, MCSE, MCTS and MSBS along with Cisco's CCNA & CCNP, VMWare VCP, VoIP Allworx and CompTIA A+. Our staff includes account managers, project managers, project coordinators, technicians, engineers, network administrators, and help desk staff, dedicated to your success. This level of experience and certification enables Neoscope to provide you with the confidence that your needs will be met by the most qualified team members.

Neoscope Solutions:

IT Assessments	Managed Services	IT Consulting and Implementation Services	Procurement and Buybacks
✓ Network ✓ Security ✓ Virtualization ✓ Backup and Disaster Recovery ✓ Cloud Readiness ✓ Technology Roadmap and Planning	✓ Monitoring and Management ✓ Backup and Disaster Recovery ✓ Help Desk Services ✓ IT Staff Augmentation ✓ Neoscope Shield Security ✓ Cloud Integration ✓ Mobile Device Management	✓ vCTO ✓ vCSO ✓ Technology Roadmap ✓ Design and Planning ✓ New Installation ✓ E-rate ✓ Migration Services ✓ Hardware Refresh	✓ Hardware and Software Procurement ✓ Equipment Buybacks and Trade-ins

Case and Discovery Scope

Dover School District has engaged Neoscope Technology Solutions to perform an assessment of its information technology assets and strategic plan. Information technology is a sizeable investment, maximizing its effectiveness in a time of growing demand, constrained resources and rapid technological change requires consistent and proactive management. Neoscope will advise what improvements should be made to ensure that the right human and technology resources are in place to bring the organization forward. Neoscope did not evaluate the use of technology in the classroom, focusing only on the stability and capability of the infrastructure to support current demands.

The IT Assessment included the following discovery tasks:

- Interviews with IT and other administrative staff
- Site visits to each facility
- Data collection and monitoring of all critical systems
- Topical analysis by our CTO, CSO and several specialized engineers

As part of the discovery tasks, we evaluated the following individual systems:

Active Directory	Assess the Active Directory health and identify potential issues with design and operation.
Systems and Operations Policies	Assess the implementation of system and operations policies and their effects on the environment manageability, user experience, and security.
Messaging Platform	Review of the messaging organization structure.
Backup and Maintenance	Review a number of key indicators to determine efficacy of current maintenance and backup procedures.
Server Environment	Review the configuration, health and security of the Server Operating System environment.
Network Devices	Review of Networking Devices, their topology, and configuration.
Virtual Environment	Review of the specifications of the virtual environment and its viability.
Storage Environment	Assess health and resource utilization of storage devices.
Physical Environment	On-site inspection of IT infrastructure including data rooms and assessment of continuity practices
Anti-Virus Landscape	Identifies coverage of servers and endpoints to ensure this security risk is at a minimum
Workstation Probe	Review connected workstation endpoints to determine potential user experience concerns, security vulnerabilities, and unnecessary management overhead.

Executive Summary

Based on industry-wide best practices and Neoscope' s extensive experience with School Systems and large organizations, we find the state of Dover School Districts information systems to be substantially deficient in a number of areas, with critical concerns in the areas of governance, staffing and systems serviceability. These deficiencies are in no way indicative of a dereliction of duties, but frequently encountered oversights or knowledge gaps that occur because of a small or overly taxed internal IT staff.

In this section, we will provide a high-level overview of these issues as well as cursory recommendations. Keeping in mind the larger mission to provide for the betterment of the students and the future of the organization, Neoscope has categorized the issues into three main areas:

Technical Issues and IT Infrastructure

Neoscope found substantial deficiencies in key components of the IT infrastructure introduced by misconfiguration and/or inadequate maintenance. A number of these items are urgent and need to be addressed immediately. While there are many, these are the largest and most critical to the organization:

- Active Directory, which is the core authentication system to the network, is effectively in a state of disrepair and should be rebuilt separate from the City.
- The data backup strategy is incomplete and leaves the organization at great risk. Backup objectives must be defined and an appropriate solution implemented and validated.
- The single email server is a critical single-point-of-failure and redundancy features are recommended for implementation.
- The virtual environment, while seemingly of adequate capacity, needs to be reconfigured in order to meet the demands that are being placed upon it.

The technical findings section of this document provides a deeper understanding of these, and other individual issues, discovered during this assessment. We will recommend remediation efforts on a system-by-system basis.

Human Capital and Vendor Management

Neoscope interviewed a number of IT and administrative staff to glean how well they are suited to their roles and if those roles are, correct for the organization. The staff shared many of the same concerns as our team and validated a number of impressions. Recurring themes taken from these conversations include:

- Staff are often incapable, be it due to politics or technical ability, of making changes necessary to maintain the environment. Separating from the City and assigning application and data owners will empower IT staff.
- The technical limitations in their ability are further hampered by IT not being their primary job function. Supplementing their efforts with specialists well-versed in the complex systems will allow for a more proactive IT team.
- IT leadership is not consistent across the organization, leaving many without clarity as it relates to their responsibilities and department initiatives. Designation of a leader for this team is recommended to act both as a resource for staff but to also help design and enforce policies and procedures.

IT Governance, Policies and Planning

Throughout the assessment process and staff interviews, it became evident that there was a significant void in IT governance, including policies, procedures or strategic technology planning for the District. Simple systems management tasks are not being undertaken due to a lack of direction and standards asked of the department.

- Neoscope found there to be no organized system of documentation. This introduces risk of knowledge loss through employee attrition, as well as creating inefficiencies among staff and vendors.
- Basic security policies have not been enacted, that are inherent to the systems themselves and require no additional resources.
- Professional tools to centrally manage, monitor and report on the environment were not in place prior to Neoscope being engaged. This contributed to major inefficiencies in managing the environment.
- There was no awareness of a strategic technology plan for the District, preventing the department from acting with purpose.
- There is currently no change management process in place, leading to undocumented changes being made in the environment that have unforeseen consequences.

Neoscope is recommending a full course of operational audits, policy design initiatives, and designation of an IT leadership role to provide both accountability to staff and aid in the policy design and enforcement process, as well as commissioning of a Master IT Plan.

IT Governance, Policies and Planning

The District has not had consistent proactive management as evidenced by an absence of many of the industry standard policies and procedures necessary to ensuring operational continuity. The same is true concerning the lack of a strategic short, mid, and long-range technology plan for the District.

Without standards defined by policy, the default mode of operation for IT staff and technology has been reactive, and as a result, grossly inefficient for both IT staff and end-users.

Best-practices and routine maintenance do not occur organically, and therefore must be tasks for which certain resources are held accountable. A number of the technical issues outlined in this document are a direct result of a lack of policy and accountability.

The IT department exists to support the larger organization, so without clear direction as to its purpose these policies cannot be defined in whole. An audit of internal workflows, interviews with internal stakeholders and review of compliance standards needs to be undertaken to identify the specific needs to be considered during policy design.

Separate from these business-centric policies are the more generic IT best practices, these are often starting points for more specific business policies and should be implemented as soon as possible in order to turn the department in the right direction.

These generic IT practice policies would typically include:

- Password and Account Policy
- Acceptable Use
- Confidentially Notices
- Documentation Standards
- Change Tracking
- Backup Policy
- Monitoring Policy
- Service Level Agreements
- Application and Data Owner Policy
- Anti-virus and patch policies
- Maintenance schedules

These policies, where they exist, warrant review as language in these were found to lack strength. Additionally, IT should be leveraged for electronic delivery and acceptance of these policies to guarantee completeness, compliance, and to simplify management.

The accountability aspect to these policies necessitates leadership in this field, not only to assist in design but to continually validate their practice. This is also crucial to making staff as effective as they can be by giving them the appropriate resources they need to be successful in their roles.

At current, the bifurcation of management between the District and the City presents its own set of challenges. It may not be practical, or even possible, to define policies in the interest of the organization when they are in contention with those in place at the City level. For these reasons, and those mentioned in other sections, we also recommended delineating IT systems and management from those of the City.

There was no awareness of a strategic technology plan for the District, preventing the department from acting with purpose and direction. Neoscope recommends the above concerns come into the scope of a Master IT Plan.

Human Capital and Vendor Management

We found through the discovery and interview process that a number of people, of which IT support is not their primary or even their professional role, are those currently supporting the environment. This is resulting in a number of priority conflicts and skill gaps beyond what is already expected given the limited number of staff relative to the size and scope of the environment.

Some of the pain points identified by these staff are they feel they are not empowered to make the changes they see fit as a result of the integration with the City, and that the lack of resources forces them into situations where their time is monopolized by reacting to issues instead of being proactive. Additionally, they would like to see management and monitoring tools implemented across the entire network to make doing their jobs possible, but often lack either the technical or political ability to implement these.

Beth Dunton and Louise Paradis are splitting the role that Joe used to hold, and while doing an admirable job in attempting to manage this, it is evident that technical leadership is required. Sites are being managed individually rather than the network being treated as a single large environment, and thus creating further bifurcation in the environment.

Our interviews were limited to Kevin Bourre, Cheryl Black, Kristen Rup, and Beth Dunton because of the summer break and was focused on the technical aspects of the IT environment at the schools. We would still like to interview the Building Tech Coordinators, Mark Raiche and Kathy Britt who were unavailable at the time of this writing.

Beth is a very capable project manager, but with her other responsibilities it is difficult for her to handle the scope of projects needed to run and maintain the IT infrastructure at The District.

Kristen is focused on managing applications and databases that effect all of the schools, she is capable in this capacity, but we would recommend some application specific training from the vendor of these applications.

Kevin is responsible for managing the CTC environment at the high school and he assists Louise with managing the high school environment. Kevin is very capable, but is over loaded with the day-to-day

reactive support to be able to fully maintain or expand the environment. We recommend Kevin receive some additional training in-line with Microsoft certifications.

Cheryl is responsible for managing the middle school environment, she is a capable technical resource but expressed that there are political implications affecting what she is able to work on. Due to most of the technology in the school system running through the middle school, there is equipment in the environment Cheryl knows little about managing. We recommend some specific technical training on the hardware and software in the middle school environment with a focus on Microsoft certifications.

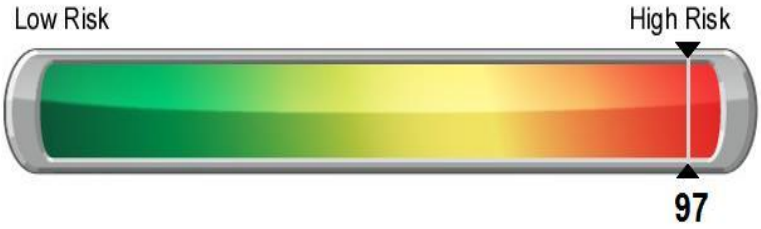
While we were unable to interview the IT paras, the impressions we got from the other IT staff are that these individuals require additional training in order to fulfill the role of front-line support for the end users of the District. We would recommend that these staff members have, at minimum, at least 1 year field experience and/or entry-level, industry-standard certifications such as CompTia A+, and Microsoft Desktop certifications.

It was challenging to gather information, not due to anyone's unwillingness to help, but due to the disjointed environment structure. Proper credentials that would allow us to scan the environment were needed and simultaneously we were not allowed to survey the City of Dover systems that were interconnected. Additionally, while troubleshooting a networking outage at Dover Middle School (DMS), we had to reach out to the City for support as they controlled affected hardware. This exemplifies what these staff experience on a daily basis. We find many of their concerns echo our findings.

Technical Issues and IT Infrastructure

Based on industry-wide best practices for network health, performance, and security we find the state of Dover School Districts information systems to be substantially deficient in a number of areas, with critical concerns in the areas of maintenance, security, redundancy and overall supportability. These deficiencies are in no way indicative of a dereliction of duties, but of frequently encountered oversights or knowledge gaps that occur because of a small or overly taxed internal IT staff.

To standardize the scale of the risks to the environment currently present as a result of the following issues, one of our analysis tools quantifies these by number and nature to calculate a "Risk Score".



Several critical issues were identified. Identified issues should be investigated further and addressed in accordance with our recommendations or Master IT Plan.

Active Directory – We discovered numerous errors surrounding core AD functionality, and Domain Controllers. These issues are likely leading to substantial performance issues with both back office applications and user systems, dependent applications and administrative functions not working predictably, and inconsistent user experiences.

The directory appears to have been originally of robust design, but many ongoing administrative tasks have been either overseen or neglected resulting in the environment evolving into misconfiguration and effectively a state of disrepair.

The logical unification of the school and municipal directories presents its own set of challenges given the management landscape and is a likely contributor to the aforementioned issues.

Substantial risks exist to any future projects involving changes or additions to the infrastructure that are dependent on Active Directory, including directory integrated mail solutions, given the current state of this environment.

Messaging – The Exchange mail organization lacks implementation of a number of the redundancy features built into the product. This leaves the entire organization email system vulnerable to the down time of a single server. This particular messaging solution is heavily integrated with Active Directory, and as a result shares many of the same issues aforementioned. Staff interviews have revealed that account management requests go through the City and leaves much to be desired in terms of responsiveness and cooperation. A separate platform, Google's education services, is being utilized for teacher to student communications because of constraints put on them by the City of Dover's IT department.

Currently the only way to access the Exchange environment is by using an old system admin's account (Croberge), Dover School District does not currently have any other way to manage the Exchange environment. This creates not only an administration issue should the password ever be changed, but also a major security issue as many people share this account to perform administration.

Networking – The switches and routing environment is functional and serves its purpose; however, there are substantial configuration improvements possible to better align the environment with best security and management practices. Connected systems also seem to be exhibiting signs of larger configuration issues affecting connectivity. The City of Dover manages the routers and the firewalls for the schools which is causing issues with resolving network outages and fine tuning the network to meet the organization's needs. Currently there is no one on staff for the School District that is knowledgeable with network environment to aide with troubleshooting with the City and resolve the issues in a timely manner.

Infrastructure – Both the virtual environment and storage infrastructure are great assets and will continue to serve the organization well into the future. However, relatively minor reconfigurations and remediation of acute issues would help to better leverage these assets. It is clear that substantial investments have been made in the past towards power redundancy, but these assets sit derelict and not implemented thus leaving the infrastructure prone to downtime and susceptible electrical damage. The state of backups is fragmented and largely dysfunctional. The backup methodology warrants addressing immediately, particularly where this infrastructure does not currently use a replication partner.

Acute Issues

Anti-virus not installed

Issue: Anti-virus software was not detected on a large number of computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
Recommendation: To prevent both security and productivity issues, we strongly recommend assuring anti-virus is deployed with some level of automation to all possible endpoints.

User passwords set to never expire

Issue: User accounts with passwords set to never expire present a risk of use by authorized users. They are more easily compromised than passwords that are routinely changed.
Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

Security patches missing on computers

Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software.
Recommendation: Refine the existing path management solution to address environmental challenges so that patching on computers and servers is current across the landscape.

Un-populated Organization Units

Issue: Empty Organizational Units (OU) were found in Active Directory. They may not be needed and should be removed to prevent misconfiguration.
Recommendation: Remove or populate empty Organizational Units.

Inactive Computers

Issue: 1060 computers were found as having not checked in during the past 30 days.
Recommendation: Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, or powered on. It is possible to, via script, automate removal of these inactive objects. Removing obsolete objects is a best practice of systems administration.

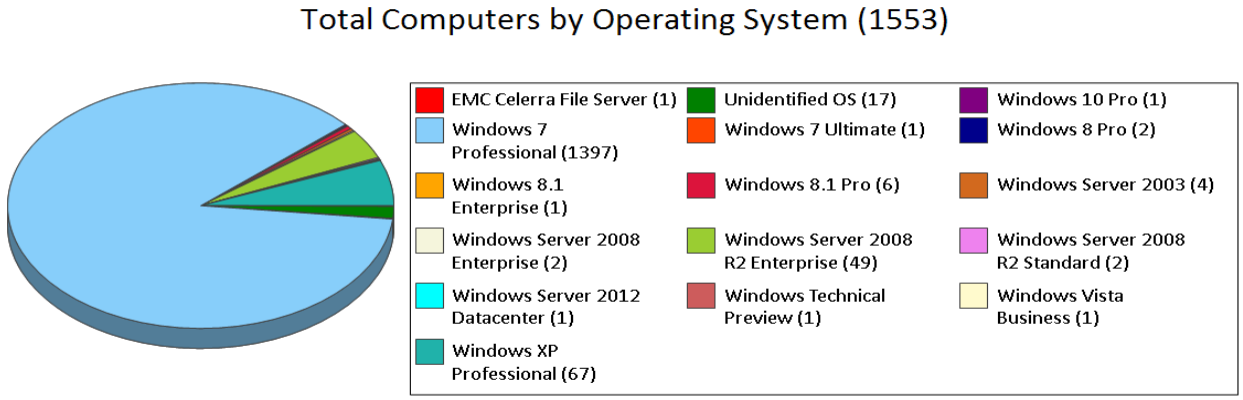
Empty Distribution Lists

Issue: Two lists do not contain any members or groups. Empty groups may be merely legacy lists which can be removed or lists which should be populated. Empty distribution lists will not deliver messages to individual mailboxes and may be lost or missed. This is often a sign of misconfiguration.
Recommendation: We suggest examining each empty list and either removing the list or populating properly.

Unsupported and Extended Support Operating Systems

Issue: 71 computers were found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk. 1452 computers were found using an operating system that is in extended support. Extended support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.

Recommendation: Upgrade or replace computers with operating systems that are, or about to be, no longer supported.



Terminal Server Resources

Issue: Our alerting brought some performance issues to our attention regarding a terminal server that was discovered to have over 40 dependent thinclients on 6GB of RAM.

Recommendation: An assessment of these particular systems should be performed to determine if it needs to be reconfigured or reengineered with purpose in mind.

User password set to never expire

Issue: User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.

Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

Unrestrained Web Access

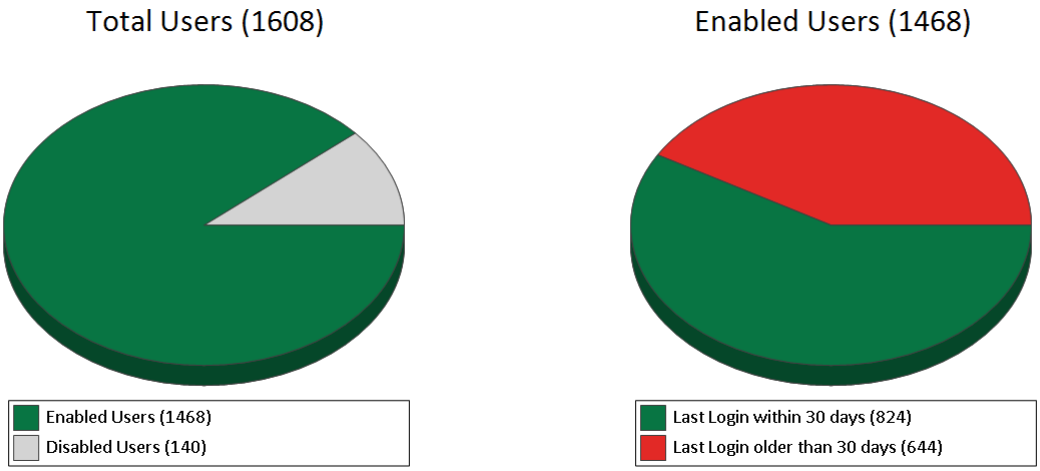
Issue: One of our analysis tools determined it was able to reach undesirable web content unimpeded. Web filtering not only serves to keep employees innocent, but are an important component of malware protection and data leakage prevention.

Recommendation: Implement web filtering as an added layer of protection, this may even be possible with existing hardware that is in place.

Users have not logged in in 30+ days

Issue: Users that have not logged in in 30 days could be from a former employee or vendor and should be disabled or removed.

Recommendation: Disable or remove user accounts for users that have not logged in in 30 days. It is possible to, via script, automate removal of these inactive objects. This is again an indicator of that closer attention needs to be paid to routine administration.



Domain Controllers in Poor Health

Issue: Multiple domain controllers are still configured to replicate to domain controllers that are no longer existing, thus creating errors in replication. There are also numerous issues where controllers are citing communication issues with online systems.

Recommendation: The extent of the issues present in the directory, combine with the management challenges, forces us to recommend a migration to a clean forest.

Network Documentation

Issue: A comprehensive network documentation package was not readily available. While information was provided on an as-needed basis, there is substantial risk of knowledge loss in the event of employee attrition.

Recommendation: A comprehensive documentation package should be assembled and regularly audited and updated.

Equipment Warranties

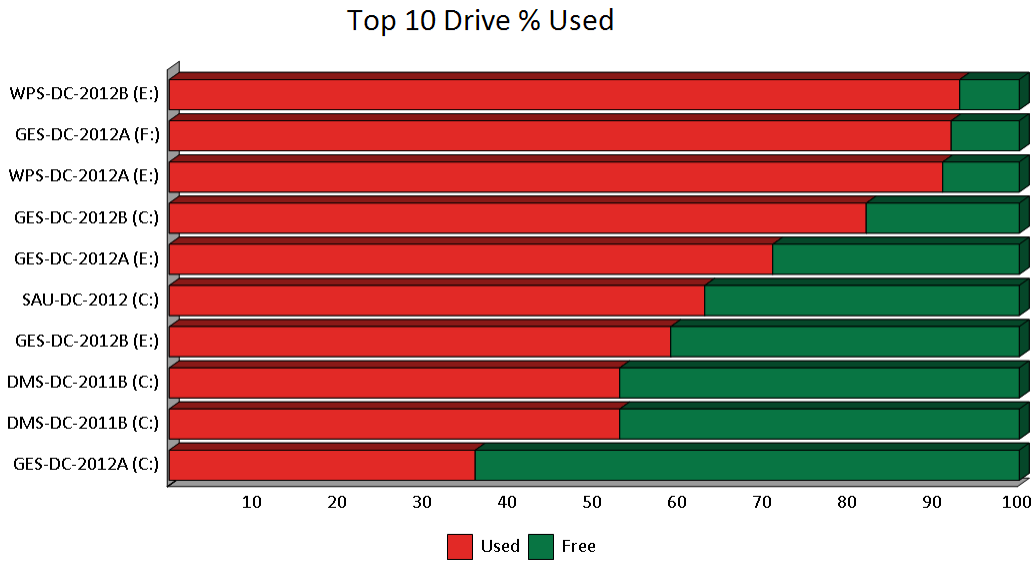
Issue: A number of physical devices, including production servers, were found to be out of warranty.

Recommendation: Production systems out of warranty create risk to the environment of prolonged downtime resolution if the vendor is called upon, if available. Warrantied systems ensure the system is both supportable and that the fastest resolution possible by the vendor is guaranteed per their respective service level agreements.

Server Drive Space at Critical Capacity

Issue: Multiple drives are issuing warnings that they are at or near their maximum capacity. This may result in service outages and possible data corruption if the data residing on the store becomes unable to grow.

Recommendation: Re-provision the data stores and underlying storage to accommodate the needs of the hosted applications.



Internet Speed Discrepancy

Issue: Tests show a greater than normal disparity between internet upload and download speeds. This is generally an indicator of a misconfiguration between the ISP and local networking equipment.

Recommendation: A deeper review of networking is necessary to detail recommendations, but outside the scope of this assessment due to the management of WAN devices being done by the City.

Lack of Monitoring

Issue: Our alerting notified of other acute issues, some of which were able to be addressed by specialists in those respective technologies while others have helped bring attention more systemic issues in this environment.

Recommendation: The nature and number of alerts to date are indicative of the need for proactive alerting to aid in identifying issues before they effect the user population or important data.

Moving Forward

While the number of issues itemized may seem voluminous on paper, it is somewhat expected given the size and complexity of the organization versus the number of IT resources. There are a number of areas where findings were positive, as many of the physical components are already in place for a robust and secure network.

It is advised these next steps be taken to remediate the deficiencies itemized in this report.

- A data retention and backup specialist should leveraged immediately to implement a stop-gap measure as it relates to the server backups given that many are a single-point-of-failure away from data loss.
- Implement a short-term IT plan that brings into scope the critical issues outlined in this document.
- Designate an acting technology officer who can guide the organization through implementing the remaining recommendations.

Active Directory	Rebuild the Active Directory system, separate from The City of Dover
Systems and Operations Policies	Address the lack implementation of system and operations policies and train staff on Standard operating procedures as they relate to the IT infrastructure
Messaging Platform	Review of the messaging organization structure, to prepare for move to office 365
Backup and Recovery	Implement a consistent, manageable solution at all sites, with alerting and notifications sent to IT administrators.
Server Environment	Review the configuration, health and security of the Server Operating System environment. Remediate issues related to host software stability.
Network Devices	Review of Networking Devices, their topology, and configuration. Change network device passwords to prevent unauthorized / untracked changes from being made.
Virtual Environment	Address issues with current virtual machine limitations and increase resources where determined necessary
Storage Environment	Evaluate health and resource utilization of storage devices.
Physical Environment	Repair, replace or install power protection devices to ensure all critical equipment is protected against power problems.
Anti-Virus Landscape	Implement a cohesive solution with reporting and notifications of detections sent to IT administrators

There are a number of technical concerns that must be addressed in order to provide stability and increase capacity in the environment. Until they are resolved, these issues will continue to create a barrier to fulfilling the overall vision of the district as it relates to increased technology use in the classroom. As technologies that are more complex are introduced into the District to fulfill the daily business obligations, an increased level of support is recommended to ensure that technology continues to be a business asset and not a source of frustration and liability.

The District has made great strides in recognizing these challenges by implementing a proactive approach to managing the environment. Leveraging a managed IT service partner provides a single point of contact for all issues, a high level of monitoring and reporting, and access to highly specialized engineers. This provides the internal staff the tools, flexibility and resources to focus on higher value objectives that will directly benefit the students, teachers and staff.