

# Network Performance, Security and Reliability Assessment



## **VERTEKS** **VOICE & DATA** **NETWORKS**

*Presented to:*

**CLIENT NAME OMITTED**

*Drafted by:*

**Verteks Consulting, Inc.**  
2102 SW 20<sup>th</sup> Place, Suite 602  
Ocala, FL 34474  
352-401-0909

**Microsoft**  
**GOLD CERTIFIED**  
*Partner*

Advanced Infrastructure Solutions  
Networking Infrastructure Solutions

## ASSESSMENT SCORECARD

Verteks Consulting has examined 114 aspects of your business technology operations. In order to clearly present the findings, we organize each area of investigation into four categories: Security, Productivity and Performance, Downtime Exposure and Manageability. The letter grades presented here were determined by using a weighted scale for each aspect based on its relative impact to your operations.

Assessment Scorecard	
<b>Security</b>	C
<b>Productivity and Performance</b>	C
<b>Downtime Exposure</b>	F
<b>Manageability</b>	D

## ASSESSMENT EXECUTIVE SUMMARY

Overall, our assessment found that your network lacks some of the security, reliability and performance most businesses demand from their IT systems. Based on our assessment, the current condition of your technology environment is primarily due to a lack of quality IT consulting and support, and secondarily due to some additional configurations changes required to establish the appropriate security and stability. In every area we examined, we found major issues and concerns that we recommend addressing immediately.

The most alarming concerns are the lack of redundant drives in some of your branch servers, the lack of appropriate share and folder permissions, the improper configuration of Active Directory Organizational Units, and Microsoft Exchange replication problems that result in a certificate error. These gaps go far beyond the normal weak passwords and other less serious concerns we find in many businesses.

Many of the issues we found can be addressed quickly by a trained and experienced IT engineer from Verteks Consulting. Additionally, an ongoing support relationship with Verteks will help alleviate the ongoing problems you've experienced – and give you a local single-point-of-contact for all your IT support needs. Within the first few weeks of our service, we will come to understand your systems and needs in complete detail, enabling us to be an extension of your company and a true IT business partner. We recommend immediately addressing the major concerns found by our assessment – including locking down your security, adding a data backup solution, and reconfiguring other systems so they work correctly. The results of our efforts will be a dramatic improvement in the security, reliability and performance of your computer network.

### **Data Preservation and Security Critical Concerns**

Our network assessment noted several critical concerns in the areas of data preservation and security that need to be addressed immediately, including:

- Your vital business data is being backed up but is not being tested for correct restores. It is imperative that data can be restored and the procedure verified before an actual emergency occurs. The procedure to restore backed up data needs to be tested and the results documented on a quarterly basis. Some regulatory agencies recommend that a monthly test restore be conducted and documented.
- Business critical servers need to have drive redundancy configured in case of drive failure. Without redundant drives, there is the potential for large amounts of revenue loss due to the repair, reloading of the OS, reloading of the applications and the restoring of data from backup. Without redundant drives, you risk excessive downtime – which can result in lost revenue and an impact on business reputation as well. Currently, you have failed redundant drives on branch servers in at least 2 locations.
- UPS testing is not being conducted. It is imperative that the UPS systems are properly tested for battery life as well as inverter operation. The UPS should be tested on a quarterly basis and the results documented. Some regulatory agencies recommend that a monthly UPS test be conducted and documented.
- UPS communication software is not configured on servers. When UPS communication software is configured properly on the server, after being on battery power for a predetermined amount of time the server will be shutdown in a controlled manner preventing software corruption as well as preventing damage to hardware.

### **Productivity & Performance Critical Concerns**

Our network assessment noted several critical concerns in the areas of productivity and performance that need to be addressed immediately, including:

- Group policies are not configured properly and share permissions are not standardized. Group policies enable one-to-many management of users and computers through the enterprise, they automate enforcement of IT policies, they simplify administrative tasks and they consistently implement security settings across the enterprise.
- Users have limited training concerning the Windows XP operating system. Verteks can provide on-site training for Windows operating systems as well as the Microsoft Office suite of products – resulting in greater efficiency for your users, improved customer service, and a reduced burden on in-house IT resources.

### **Downtime Exposure Critical Concerns**

Our network assessment noted several critical concerns in the area of downtime exposure that need to be addressed immediately, including:

- The current IT service partner does not seem to have the technical expertise that your business requires. This can result in unnecessary risks and unplanned downtime – as well as more downtime than necessary in critical situations.
- The current IT provider is extremely slow to respond to your needs. In the event of an urgent issue you need backup support immediately – helping you to restore your systems quickly to prevent loss of revenue and harm to your business reputation.
- Currently there is not a documented redundant Internet failover testing procedure or documentation in place. With so many critical functions on the Internet, its important that this vital link be regularly tested.

- There is no written disaster recovery procedure in place and there is no quarterly disaster recovery testing documented. Recovering your vital business systems and data in the event of a disaster is a time of great stress and anxiety – it's absolutely critical that you have a well planned approach that has been tested. With proper planning you'll reduce the amount of downtime in the event of a disaster, and reduce the impact on your customers, your revenue and your business reputation.

### **Manageability Critical Concerns**

Our network assessment noted several concerns in the area of manageability that we recommend addressing immediately, including:

- Organizational units and group policies are not configured correctly. Reconfiguring these important settings will result in improved security, easier system management, and faster resolution of issues related to OUs and GPOs.
- Too many users have administrative rights. This can be a warning sign in a regulatory audit, and can signal that applications have been setup improperly. Ideally IT security will be setup so that no user has full administrative access – and that special administrative accounts are used when these activities take place. This way when a former administrator leaves it's much easier to quickly change security and lockout the prior user.
- There is no change order or hardware updating process in place. With a network that spans multiple locations and many users, it's important to have a systematic approach to asset retirement and replacement. This way, your business will get the most out of its IT equipment investments, and also have a more predictable capital expenditure budget.
- There are no server hardware service agreements in place. Having backup and/or warranty service on servers is especially important – since an outage of one server will affect multiple (or possibly all) users. We recommend that servers have manufacturer support for hardware, and backup support from an IT services company if possible.
- Routers and switches have no firmware or system update plan in place. These devices are often left without updates for a significant time – resulting in weaker security and degraded performance. At least once each quarter these infrastructure components should be reviewed and updated to the latest firmware or software to keep the network at optimum health and performance.

### **CONCLUSION**

Thank you for giving us the opportunity to review your IT infrastructure and complete this assessment. We're confident that the issues we found can be addressed quickly, resulting in improved security, better system management, increased performance, and greater productivity for your users. With some work from our experienced IT professionals, and your internal staff's input and support, we believe a substantial improvement can be gained in a short period of time.



**Assessment Scorecard - Area 1: Security**

Area 1: Security Scorecard Summary	Weight	Score
Data Preservation	40%	3.8
Network Security	30%	5.0
System Security	30%	2.0
Compliance	0%	0.0
<b>Weighted Average Score (0=low to 5=high)</b>	<b>3.64 / 73%</b>	
<b>Overall Security Rating</b>	<b>C</b>	

Data Preservation	Pass	Fail
Backup system with offsite data portability functional	X	
Adequate, current and supported backup software	X	
Data centralized through roaming profiles/redirected folders	X	
Backup software configured properly to backup company data	X	
Backup software configured properly to backup system states	X	
Backup software configured properly for notifications/reporting	X	
Adequate media rotation including archive volumes	X	
Offsite and offline storage of backup volumes	X	
Adequate media capacity for data volume		X
Backup software configured properly to backup OS/Applications		X
Existing sample restoration routine processes		X
Availability of installation media	X	
Daily review of backup notifications	X	
<b>Data Preservation Rating (0=low to 5=high)</b>	<b>3.8</b>	

Network Security	Pass	Fail
Firewall hardware functional	X	
Firewall configured with at least basic protection	X	
Wireless system secured (if applicable)	X	
Centrally managed antispam software available	X	
Centrally managed antivirus software available	X	
Antivirus software thoroughly deployed and updating	X	
Antispam software thoroughly deployed and updating properly	X	
Wireless system secured with VPN	X	
Gateway-level antispymware system available, configured and updating	X	
Gateway-level intrusion prevention system online, configured and updating	X	
Password policies (complexity, history, expiration)	X	
<b>Network Security Rating (0=low to 5=high)</b>	<b>5.0</b>	

System Security	Pass	Fail
File/share permissions for employee access control		X
Restrictions on confidential/proprietary data transmission		X
Server and server-based application updates current	X	
Workstation OS updates current	X	
RAID configured on all mission-critical servers		X
Adequate environmental facilities (AC, Power, etc)	X	
Adequate UPS battery capacity for equipment	X	
UPS Communication system installed		X
UPS Communication system configured		X





Existing UPS testing routine process		X
<b>System Security Rating (0=low to 5=high)</b>	<b>2.0</b>	

<b>Compliance</b>	<b>Pass</b>	<b>Fail</b>
Meets security compliance requirements (PCI/FINRA/HIPAA) - N/A		X
<b>Compliance Rating (0=low to 5=high)</b>	<b>0.0</b>	

**Assessment Scorecard - Area 2: Productivity & Performance**

<b>Area 2: Productivity &amp; Performance Scorecard Summary</b>	<b>Weight</b>	<b>Score</b>
<b>System Performance</b>	30%	5.0
<b>Leveraged Software Features</b>	10%	2.5
<b>User Productivity</b>	30%	3.6
<b>Remote Access Performance and Capabilities</b>	30%	1.7
<b>Weighted Average Score (0=low to 5=high)</b>	<b>3.32 / 66%</b>	
<b>Overall Productivity &amp; Performance Rating</b>	<b>C</b>	

<b>System Performance</b>	<b>Pass</b>	<b>Fail</b>
Server systems performing adequately	X	
Network bandwidth Availability	X	
Workstation systems performing adequately	X	
Internet bandwidth Availability	X	
<b>System Performance Rating (0=low to 5=high)</b>	<b>5.0</b>	

<b>Leveraged Software Features</b>	<b>Pass</b>	<b>Fail</b>
Roaming profiles in effect for all users	X	X
Applications packaged for deployment through group policy & Active Directory		X
Distributed File System (DFS) configured	X	
Volume Shadow Copy (VSC) configured and users trained		X
SharePoint Server configured and users trained		X
Calendar sharing configured and users trained	X	
Public Folders configured and users trained	X	
<b>Leveraged Software Features Rating (0=low to 5=high)</b>	<b>2.5</b>	

<b>User Productivity</b>	<b>Pass</b>	<b>Fail</b>
Antispam controls	X	
Web content access controls	X	
Operating system navigation fluency	X	X
Office system fluency	X	X
Remote Access tool fluency	X	
<b>User Productivity Rating (0=low to 5=high)</b>	<b>3.6</b>	

<b>Remote Access Performance and Capabilities</b>	<b>Pass</b>	<b>Fail</b>
Secure access to systems remotely for all authorized users		X
Smart Phone capabilities for all appropriate personnel	X	
Dual factor authentication for remote access		X
<b>Remote Access Capabilities Rating (0=low to 5=high)</b>	<b>1.7</b>	





**Assessment Scorecard- Area 3: Downtime Exposure**

Area 3: Downtime Exposure Scorecard Summary	Weight	Score
System Support Quality	25%	0.0
System Repairability	25%	4.0
System Resilience	20%	1.7
Disaster Recoverability	30%	0.0
<b>Weighted Average Score (0=low to 5=high)</b>	<b>1.33 / 27%</b>	
<b>Overall Downtime Exposure Rating</b>	<b>F</b>	

System Support Quality	Pass	Fail
Provider skill level adequate		X
Provider responsiveness adequate		X
Provider monitoring vital systems continuously and receiving alerts		X
After hours support available		X
<b>System Support Quality Rating (0=low to 5=high)</b>	<b>0.0</b>	

System Repairability	Pass	Fail
Warranties current for vital hardware products		X
Support contracts current for vital software packages	X	
Documentation current and available	X	
OS/Application installation media available	X	
Spare Workstation(s) configured	X	
<b>System Repairability Features Rating (0=low to 5=high)</b>	<b>4.0</b>	

System Resilience	Pass	Fail
Vital system hardware stability adequate	X	
Vital Operating Systems stability adequate	X	
Vital applications stability adequate	X	
Servers configured and cabled for network switch failure resiliency		X
Redundant authentication server available	X	
Redundant Internet circuit available & configured for auto-failover		X
Redundant gateway hardware available & configured for auto-failover		X
Periodic Internet failover & gateway hardware failover testing performed		X
Redundant messaging services available & configured for auto-failover		X
Redundant file share services available & configured for auto-failover		X
Redundant remote access services available & configured for auto-failover		X
Periodic testing performed of messaging, file share & remote access failover		X
<b>System Resilience Rating (0=low to 5=high)</b>	<b>1.7</b>	

Disaster Recoverability	Pass	Fail
Offsite company data possible to meet Recovery Point Objective		X
Company data recovery possible within Recovery Time Objective		X
Vital systems capable of service restoration within Recovery Time Objective		X
Remote access to systems possible withing Recovery Time Objective		X
Recovery instructions documented		X
Remote access instructions developed for staff		X
Staff trained on disaster recovery system access procedures		X
Periodic site outage testing performed routinely		X
<b>Disaster Recoverability Rating (0=low to 5=high)</b>	<b>0.0</b>	





**Assessment Scorecard - Area 4: Manageability**

Area 4: Manageability Scorecard Summary	Weight	Score
Workstation/User Management	35%	2.8
Patch Management	35%	3.8
Administrative Tools	20%	1.7
Financial Management	10%	3.0
<b>Weighted Average Score (0=low to 5=high)</b>	<b>2.92 / 58%</b>	
<b>Overall Manageability Rating</b>	<b>D</b>	

Workstation/User Management	Pass	Fail
Issue management/ticketing system established	X	
Workstation images created	X	
Applications packaged		X
DHCP on all appropriate computers	X	
Organizational Units (OUs) configured for departments and roles		X
Application/Interface access limitations set through Group Policies		X
User-based web content filtering system in place	X	
Administrator rights removed for users		X
Data centralized through roaming profiles/redirected folders	X	
<b>Workstation/User Management Rating (0=low to 5=high)</b>	<b>2.8</b>	

Patch Management	Pass	Fail
Automated workstation update system configured (WSUS)	X	
Automated workstation update system functioning	X	
Server updating processes established with change windows	X	
Network hardware updating processes established with change windows		X
<b>Patch Management Rating (0=low to 5=high)</b>	<b>3.8</b>	

Administrative Tools	Pass	Fail
Centralized antivirus console	X	
Centralized backup management	X	
Remote interface control support tools		X
Remote KVM		X
Remote power supply access		X
Automated system down/impending failure monitoring and alerting		X
<b>Administrative Tools Rating (0=low to 5=high)</b>	<b>1.7</b>	

Financial Management	Pass	Fail
IT budget planning	X	
Automated hardware and software inventory system	X	
Software support & maintenance renewals	X	
Hardware warranty management		X
Service contract negotiation		X
<b>Financial Management Features Rating (0=low to 5=high)</b>	<b>3.0</b>	