

## ASSESSMENTS

Server Health Check	<p>Easy to understand 'Report Card' on the health of your server identifies at risk areas, providing action needed</p> <ul style="list-style-type: none"> <li>-Analyze and grade server Hardware, Security Software, Operating System, Backup Protection</li> <li>-Report card uses familiar A, B, C, D &amp; F scoring; color coded for easy visual identification</li> </ul> <p><b>Health Check includes:</b></p> <ul style="list-style-type: none"> <li>-Review hardware resource utilization, warranty and logs</li> <li>-Review operating system logs, updates and best practices</li> <li>-Review security software scans, detections and definitions</li> <li>-Review backup job status, test restore activity, media age</li> </ul>
Security Assessment Network Assessment	<p>Recurring, deep dive view of Network and Security Solutions (requires Baseline Assessment)</p> <ul style="list-style-type: none"> <li>-Analyze network and security, identify vulnerabilities, compare to baseline</li> <li>-Deliverables include updated Management Plans, Risk Assessments, and a review with engineer</li> </ul>
Risk Assessment	<p>Required by entities governed by banking and HIPAA regulations, also available for all industries.</p> <ul style="list-style-type: none"> <li>-Evaluates Physical, Technical and Administrative compliance as determined by regulations</li> <li>-Assessment is performed with your IT team</li> <li>-Written Risk Assessment includes Risk Index for line items, each of the three sections and overall</li> </ul>

## NETWORK MANAGEMENT

Proactive Monitoring	<p>Proactive Monitoring of computers identifies trends, alerting to potential problems before they disrupt business</p> <ul style="list-style-type: none"> <li>-24 x 7 monitoring and data collection of performance, system errors and alarms</li> <li>-Monitors computer resources, providing usage statistics</li> <li>-Console option available for real-time viewing of alarms and data collection</li> <li>-Alerts sent to you and/or DCR notifying of an Internet outage, server reboots or down, and registry changes</li> <li>-Reports available for hardware and software inventory, including serial number and version</li> <li>-Monthly trend report with problems identified and recommendations included</li> </ul>
Preventative Maintenance Cleaning	<p>Proactive cleaning of computer hardware will help avoid unplanned down time</p> <ul style="list-style-type: none"> <li>-Case is removed and dust cleaned from all internal components, power supply fan, and case fans</li> <li>-Internal components are inspected for visible damage or wear</li> <li>-Problems found, or recommendations, are reported to you</li> </ul>
Annual Review	<p>Plan IT expenditures and changes with input from your IT Professionals</p> <ul style="list-style-type: none"> <li>-Inventory report of server(s), security and key infrastructure with budget for warranties, software renewals</li> <li>-Discuss changes recommended to hardware and software based on evolving needs or age of technology</li> <li>-Review key areas of business dependent on technology, comparing current solution to business need</li> </ul>
Core System Updates (Servers)	<p>Servers require attention to ensure vendor recommended updates install regularly</p> <ul style="list-style-type: none"> <li>-Evaluate available vendor service packs, service patches, firmware updates to determine viability and stability</li> <li>-Apply vendor security packs, service patches, firmware updates, as needed</li> <li>-If a service packs, service patches, or firmware update pose a risk DCR will discuss with you</li> </ul> <p><b>Core systems are defined as follows:</b></p> <ul style="list-style-type: none"> <li>-Operating Systems - Pending Windows Critical Updates</li> <li>-Anti-Virus/Anti-SpyWare software - Signature Updates are current</li> <li>-Server Hardware - Firmware/driver updates Available</li> </ul>
Licensing Management	<p>Track Licensing and Domain Registration Renewals and Subscriptions, Warranty Extensions</p> <ul style="list-style-type: none"> <li>-Executive Summary of upcoming renewals, subscriptions and extensions for next calendar quarter</li> <li>-Quarterly Report sent via email to contacts of your choice</li> <li>-Full report of all renewals, subscriptions and warranties provided annually or upon request at any time</li> </ul>
HelpDesk Email	<p>Central location for end users to send support problems and requests</p> <ul style="list-style-type: none"> <li>-Setup email account dedicated to 'HelpDesk' or 'SupportDesk' functions for your company, using your email domain</li> <li>-DCR will train your LAN/Helpdesk Administrator on how to use the HelpDesk email account.</li> <li>-DCR will assist with roll out to your end users providing training and email templates used to announce this service</li> <li>-Option for you to review and prioritize email support requests, determining what to delegate to DCR, or</li> <li>-Option for DCR to review, prioritize and respond to email support requests</li> </ul> <p><b>Response Time for HelpDesk email requests assigned to DCR Support Desk</b></p> <ul style="list-style-type: none"> <li>-General support requests responded to within 24 hours of the email request being assigned to DCR</li> <li>-Goal is to resolve general support requests within in 3 to 5 business days, but, no more than 10 days of receipt</li> <li>-Mission Critical and Server Down problems, should be reported via a phone call to DCR rather than email</li> <li>-HelpDesk email coverage excludes responding on weekends and holidays</li> <li>-Resolution time can be impacted by end user or vendor availability, or environmental problems</li> </ul>

Onsite Calls	<p>Provides regular support calls to your location</p> <ul style="list-style-type: none"> <li>-DCR will spend a pre-approved number of hours at your site, call frequency, and duration customized to fit your need</li> <li>-Pre-approved list of work to be performed</li> <li>-May include application support, remediation of problems with or installation of new workstations, printers, scanners or other hardware and software, except as specifically excluded</li> <li>-Option to have DCR develop and maintain a workstation installation checklist specific to your company</li> <li>-Separate calls will be scheduled for mission critical issues, or excluded work</li> </ul> <p><b>Excludes the following:</b></p> <ul style="list-style-type: none"> <li>-Installation of servers; Installation of new or migration of applications requiring time in excess of one regular call, Installation of new or replacement hardware requiring time in excess of one regular call</li> </ul>
Data Circuit Review	<p>Expired contracts can cost you money</p> <ul style="list-style-type: none"> <li>-Review most recent data and voice contract(s)</li> <li>-Compare contracted bandwidth to actual</li> <li>-Compare contracted service and price to most recent bill</li> <li>-Report finding to your designated LAN Administrator, review, and address questions or recommendations</li> </ul>
Promon Trending Analysis	<p>Comparative analysis of Promon data by Senior Engineer</p> <ul style="list-style-type: none"> <li>-Compare current months alert summary with past alerts</li> <li>-Identify trends that indicate action is required to avoid disruption or downtime</li> <li>-Provide recommended remediation</li> </ul>

## SECURITY

Firewall Check	<p>Designed to review the overall health of the Internet gateway device, and notify you of potential problems</p> <ul style="list-style-type: none"> <li>-Review of gateway console, checking status, and reviewing logs/report for errors or issues</li> <li>-Review client usage, web security, etc.</li> <li>-Review system report. If unit is a Meraki send system report to the client</li> <li>-Check for firmware or system updates, scheduling for units supporting unattended download and install</li> <li>-Units requiring manual download on install, will require scheduling, time bills separately</li> </ul>
Security Software Check	<p>Security Software is not a 'set it and forget' solution</p> <ul style="list-style-type: none"> <li>-Review Anti-Virus/Anti-Spyware Console or Dashboard, verify AV/Spyware signatures are current</li> <li>-Verify workstations are assigned to proper policies and/or organizational units</li> <li>-Verify scans are scheduled and running properly, scheduling corrective action as applicable</li> <li>-Identify and report systems with out of date signatures</li> <li>-Monthly summary delivered via email, reporting issues or anomalies that require action</li> <li>-Remediation will be scheduled separately as approved by the client</li> </ul>
Security Review	<p>Perfect for anyone required to undergo routine audits, or submit reports to an IT Committee</p> <ul style="list-style-type: none"> <li>-Review router firewall, examining intrusion prevention, intrusion detection, and penetration testing logs</li> <li>-Review router firewall throughput, traffic, utilization, &amp; content filters</li> <li>-Review O365 and router firewall, examining email utilization, spam, white/black list</li> <li>-Provide quarterly report summary, with statistical detail</li> </ul>
External Vulnerability Scan	<p>Appropriate for audit compliance</p> <ul style="list-style-type: none"> <li>-Perimeter scan of all Public IP addresses</li> <li>-Risk Index ranks severity and provides remediation action</li> <li>-Reports are delivered electronically in format appropriate for submission to auditors</li> </ul>

## BACKUP & RECOVERY

Backup Check	<p>Backups are insurance you can recover from a disaster</p> <ul style="list-style-type: none"> <li>-Review backup jobs checking to see backups are occurring as scheduled</li> <li>-Check job status (complete, incomplete, failed, etc.)</li> <li>-Verify software is current version, checking logs for errors or failures</li> <li>-Report on status of backup job check is provided</li> <li>-Identify and report backup job issues requiring remediation</li> <li>-DCR requires permission to remediate problems as time will bill separately</li> </ul>
Restore Verification	<p>Verify your data is recoverable in the event of a file deletion or disaster</p> <ul style="list-style-type: none"> <li>-Execute test restore for each server and volume selected in backup job(s)</li> <li>-Report on status of test restore is provided</li> <li>-Failed restores are reported, and client is contacted regarding recommended remediation</li> <li>-A restore is classified as failed if the last scheduled backup job failed</li> <li>-DCR requires permission to remediate problems as time will bill separately</li> </ul>