THE BYTE DR. INC.

System Audit Protocol

Our System Audit Protocol is a methodology designed to answer the following questions about your IT infrastructure:

What is it?
Where is it?
What does it need to do?
Is it working properly?
Is it properly licensed?
Is it up to date?
Can we improve it?

In order to determine the answers to the questions above and to provide a baseline from which to improve the efficiency and functionality of your network, workstations and applications we conduct an inventory and physical testing of the equipment, configurations and user needs. The following sections summarize the type of detail that we develop so that we can provide written reports and recommendations.

1. EXAMINING HEADCOUNT
   - How many employees are there? PC users?
   - How many standalone users? Networked users?
   - How many notebooks? Desktops?

2. SIZING UP THE EXISTING NETWORK
   - Is there a network in place today? If so, what kind? Is it based on a peer-to-peer model such as Microsoft Windows 9x, LANtastic or Apple Mac OS?
   - Is it based on a centralized-server model such as Novell NetWare, Microsoft Windows NT or Microsoft Windows Server?
   - What kind of network technology is in place? Token ring? Ethernet? What speed? Switched or shared bandwidth? Wireless?
   - Are there any host-based systems, such as Sparc, VAX, AS/400, or mainframe?
   - What kind of data cabling is in place? Category 3? Category 5? Coaxial? Fiber? Was it a certified installation?
   - Are there any wide area links?

3. SCOPING OUT THE DESKTOPS
   - What are your company-wide desktop standards? Hardware? Applications? Operating systems? Printers?
   - What does the staff like and dislike about these standards? (Hint: Different groups within the company often have totally different priorities.)
   - Are there any legacy or custom applications that are redundant or obsolete?
   - Are there any orphaned applications where the ISV is no longer in business or no longer supports the product?
   - How does software license compliance look? Who's in charge of maintaining and enforcing this?

69 Ramblewood Lane, Thornhill, ON L4J 6R9 Tel: 905.771.8836 info@bytedr.ca

4. UNDERSTANDING INFORMATION TECHNOLOGY (IT) POLICY
   - Do you have a written policy on acceptable use of IT resources such as the LAN, e-mail and Web browsing?
   - Are there any EDI or similar relationships with clients or suppliers?
   - Is there a formal IT business plan in place that forecasts projects out at various time intervals?
   - What kind of documentation exists? Technical? End user? Is it adequate? Is it up to date? Is a hard copy kept off site?

5. ASSESSING LAN SERVICES
   - Does your company have basic file sharing? Printer sharing? CD-ROM sharing?
   - What about modem sharing or network-based faxing?
   - Is there internal and/or external e-mail?
   - Is there a contact management or groupware application?
   - Does anyone have access to network resources while traveling? While working from home? Which software applications?

6. DRILLING DOWN ON SECURITY
   - What kind of confidential data does your company deal with? Social security numbers? Credit card numbers? Proprietary research and development? Client lists? Payroll?
   - Is any sensitive data being kept locally on desktops, notebooks or PDAs?
   - How is data protected today? What are the biggest internal and external security risks?
   - Does everyone have his or her own logon account and password or is there just one shared password?
   - Are servers physically secured? Who has access?
   - How often are passwords changed? What kinds of policies are in place to strengthen passwords?
   - Is encryption used for any applications? Smart cards? Remote dial-back?
   - Is there a formal disaster recovery plan? How often is it tested? Revised? Who's in charge? Where's the "hot" site?

7. EVALUATING DATA PROTECTION
   - Where are Uninterruptible Power Supplies (UPS's) being used? Are data-grade surge suppressors being used on all other devices?
   - How much battery backup run-time is available for critical systems? Is UPS monitoring software utilized? What about e-mail alerts?
   - When was the last time UPS units were tested for automated shutdown? Who monitors the UPS logs?
   - How often are full system tape backups run? How many sets of tapes are maintained? How often are tapes rotated off site?
   - When was the last time the tape backup restore capability was tested at the file level? At the volume or server recovery level?
   - Are verifies done daily? Are tape backups launched manually or on a preset, automated schedule? Who monitors the tape backup logs?
   - How is data on workstations protected? What about data on notebooks and PDAs?
   - What kind of antivirus software is in place? How often is the engine updated? What about the definition files? Are the updates automated or done manually?
   - Who's responsible for monitoring the antivirus logs? Are both servers and workstations protected? Are the Web, proxy and e-mail servers protected?

- Are users trained on protecting against virus infections?

8. LOOKING AT INTERNET ACCESS, E-MAIL, WEB PRESENCE
   - How many people have Internet access? For Web browsing? For e-mail?
   - Does each person have his or her own account and modem line, or is there some kind of shared access through a router and/or proxy/firewall solution?
   - What kind of bandwidth is being used? Is it v.34 or v.90/v.92 analog? ISDN? Frame relay? T1? Cable modem? DSL?
   - Does your company have a domain name? Do you have a Web site?
   - How is the Web site maintained? Is it a static or database-driven site?
   - What kinds of Internet Service Provider (ISP) relationships are in place today for Internet access, email and Web site hosting?

9. REVIEWING TRAINING PROGRAMS
   - What kind of computer training does the staff receive? What topics? How often?
   - Is there formal classroom training? One-on-one? Peer-based? Self-study? Cross-training?
   - If so, how effective has the training been?

10. ANALYZING ASSET MANAGEMENT PROCEDURES
   - Who determines hardware/software needs and writes up the specifications?
   - How do you procure hardware and software?
   - Who determines whether items shipped match the items requisitioned on purchase orders?
   - Is hardware and software generally leased or purchased?
   - Are service agreements ordered at the time of purchase?
   - What's the typical asset life cycle? How often is hardware refreshed?
   - Who maintains the asset inventory?

Costs for the System Audit will vary based on the amount of systems and the complexity of the environment, however, the typical cost for auditing a single server network with up to 25 workstations is about $ 750.00 to $ 950.00. We will provide a quote for this service based on the information gathered at our preliminary, no cost meeting to discuss your requirements.