IT Review Checklist- Questions to ask

(Check the box if the office meets this requirement or note N/A if not applicable)

Desktops
☐ Backed Up – Are desktops backed up? What areas? Is the Lotus address book backed up? Do users know they could loose this? What software do you use? Who knows how to recover files? Do a sample recovery. Also ask users during interviews.
☐ All Win2k or XP –Do you have any Win9x machines or NT? Why?
☐ Automated OS Patch management – Do you have a SUS server? How do you know all your clients are getting update? Manual patch management also accepted but a recommendation to automate should be made. Randomly check a PC for current updates in the c\windows\update.log file.
☐ Current Software Upgrades- How are software updates request initiated, you or the users? Do you meet their demands in a timely manner? Also ask users during interviews. How do you handle deployment of new PCs? (Ghost?)
☐ File Shares not used – Do you allow shares among desktops? For what? Are you aware worms spread via file shares? How do you restrict access? Admin tools→server manger, select a machine and view the shares. Admin shares ($) and printer shares are probably ok. User shares need to be examined.
☐ Antivirus up to date and set to check files when created – Randomly check a PC for current definitions and verify that files are scanned when created, moved or edited.
☐ Disk Space Availability- Do they run defrag? It should be done at least every three month. Needed specially on machines that run Illustrator (Adobe products). Randomly check that PCs have free space on local drives.
Users – Also ask users these questions to verify information.
☐ Lock computer when walking away –automatically or manually
☐ Awareness of to Social Engineering – How are new staff made aware of office policies…do's and don'ts?
☐ Proper management of suspicious emails – how do users recognize suspicious emails and what do they do with them?

☐ Password Management – How often is crack run or are they changed every 90 days? Review crontab for scripts that might be passing passwords in plain text. Go to /var/spool/crontabs remove (crontab –r) any empty crontab files. IF they are running dwm they probably don't need the "lp" crontab, dual agin gof log files might be going on. Rtmon is left over form Y2K. http://sw2diaiwc.cr.usgs.gov/usgs/sun_tac/sa_notes/disnote.030207
☐ Procedure to delete/lock unused accounts (students)- How does the SA know when an employee no longer needs access. Who reports this to them. At the very least Admin should know to report such personnel changes to the SA. Are logs checked for last "login"?
Servers
☐ Labeling/Function Documentation – Are servers labeled with names? Are the functions of each server documented?
☐ Circuit Breakers Labeled – Do you know which circuit breaker powers the computer room?
☐ Log Review and Aging – Do you have dwm installed on Unix systems or are logs aged manually? How often and who reviews the logs- what do they look for? Which logs are reviewed? Are log messages automatically send to pagers? –not necessary but some sites are doing it with Big Brother software or home grown scripts.
Backups
☐ Servers – Are backups automated (library) or do you manually insert tapes? Show me the backup scheme? Verify that back ups are done every day. How are remote offices backed up?
☐ Desktops –REPEATED
☐ Laptops – Are laptops backed up, how, scheme, schedule?
☐ Offsite – Where are offsite backups stored? Remote field office better than at home. How regularly?
☐ Users Aware of Backup Scheme and Purpose – Also ask Users.
☐ Documented Recovery Procedure – Who knows how to recover data?

Where are the procedures documented? Do you always restore to one specific directory or back into the users work area?
☐ Organized Media – Go check that tapes are organized/labeled.
☐ Project Archival Procedures – Does the Comp staff only do disaster recovery back ups or do you also do archival? Does the office know how far back they can request that you restore data for them?
Networks
☐ LAN restricted to secure hosts – Plan on how Win9X hosts will transfer data to network because policy will soon restrict their connection to the LAN.
☐ Appropriate servers in DMZ –Only servers have house PUBLIC data should be in the DMZ.
☐ Accurate Diagrams Available -
☐ Point of Entry Known – Where does the T1 come in? How many T1s into the office? Which carries FTS2001 long distance, data and local calls? How do you know if one is down, LED indicators?
☐ Circuits clearly identified – Telecom circuits #, service phone # should be readily available. Router interfaces labeled and secure.
☐ Low rate of collisions - Look at the switches, check for collision lights.
☐ Logical Switch Distribution - ****
☐ Wireless AP – Do they have a wireless hub? Always connected or just during mtgs? Are security guidelines being followed? Try to access it from outside of the building.
Data Management
☐ None (No file server)
☐ Partial (Mixed- some data scattered some on file servers)
☐ Full (Centralized- no data stored on desktops or if stored users aware that it does not get backed up) Check % of free disk space in user areas.
Remote Access
☐ Valid Purpose- Do they have a VPN server? Offer Dial-up services to

users? Telecommuters? How do the field tech's access the office? Is Dial-up access restricted to specific users or open to the entire office? ****
☐ Encrypted and authenticated- All access into the LAN needs to be encrypted and authenticated.
☐ Limited to System Administrators
Web server
☐ Content Management – Who approves data that can be posted to the public? How many people have access to post data?
☐ Internal Pages restricted – Check that IIS (if used) is wrapped to only allow *.usgs.gov. Don't reply on the firewall only.
☐ Indexing disabled were appropriate – Check that directory browsing is disabled or ask why it is not? Check /usr/opt/apache/conf grep all files for "+Index" You will need to modify the Directory section of the site_usgs.conf file for the directory structure you are concerned with (maybe more than one). You need the "Options -Indexes" line. My line was +Indexes, but after changing to "-" it turned off indexing. I assume we should change the default (for the rpm package) to -Indexes. --Shawn <Directory "/www/htdocs/usgs"> Options -Indexes Include conf/usgs_access.conf </Directory>
Unit Management
☐ Leave Scheduling- Is a body always available at the office (exception can be made for illness or for IT meetings)
☐ Delegation of Lead SA duties when absent – Do you name an "Acting" SA when you cannot monitor email for more than 8 hours? How does the "Acting" monitor your email (Emails sent to the Lead IT person)?
☐ Emergency Home/Cell Phones in COO Plan- do you have the cell and home phones of all IT Staff?
Wiring closet
☐ Secure - Securely fastened to floor? Rack does not wobble? Screws are in place?
☐ Labeled -

☐ Neat -
Written Procedures (Contract Number and Phone)
☐ Power Failure
☐ WAN Failure
☐ PBX Failure
☐ NWIS Failure
☐ LRGS Failure
Adequate Emergency Power
☐ Network Equipment (CSU/DSU, Router)
☐ Switches/Hubs
☐ Dial-Up modems for Real-time Data Access
☐ Critical Servers (ex: NWIS/LRGS)
☐ UPS tested and Battery life checked frequently
☐ Appropriate Maintenance of Generators
Physical Environment
☐ Restricted access to Server room
☐ Restricted access to wiring closet
☐ Adequate A/C
☐ A/C sensor/pager alert system
☐ Plan of action if A/C fails – “non-critical servers are shutdown”- acceptable
☐ Sturdy/secured rack and wall mounts
☐ Equipment rest on solid surface – no stacking.
☐ Wires out of walking area
Field Offices
☐ Secure Access to Main Office- ssh, is citrix encrypted? ReflectionX tunneled through ssh? No telnet or rlogin used- protocol should be disabled on servers- not listening “netstat –a” or check vulnerability scan results.
☐ Secure Remote Control- What software is used? Does “Remote Desktop”

encrypt? How about Terminal Services? ****
Clients
☐ Secure Access to Database –only ssh is allowed
☐ MOU – Check that MOUs map to the IPs in the NWIS server host.allow.
Discussions (check if PASSED):
☐ Firewall Review – ITSOT should review before the review starts. Come to site with any concerns and plans of action to remediate.
☐ Vulnerability Scan – ITSOT should review and point out concerns.
☐ NWIS Risk Assessment Survey – Read all Q&A's for the site before review starts.
☐ ESM – Have the BITSM run a check prior review and send output to SunTAC-ask for their advice before making any of ESM's requested modifications.
☐ nwis_prep_check script
☐ solaris_security_check script
☐ check _DNS script

Interviews with (Meet with one of two people from each functional area and document satisfaction, answer to questions, concerns, who is their "go to" person and why (staff work should be equally divided):

Project Chiefs
Data Section
Admin Unit
Pub Unit
Modeling Unit
GIS Unit
Field Office

User Questions (as you interview IT staff write down questions that you want to verify with Users):

1) Does it take a long time to get your new PC once it has arrived at the office?

2) NWISWeb do they need a local NWISWeb server?

3) Are you aware that your local Lotus address book is stored on the D drive, which is not backed up?

4) Do you know which folder is your offline folder?

5) Is your software up to date? In a timely manner?

6) Supervisors and Admin- Do you protect personal data SSN, home phones?

7) Additional concerns, needs, wants, complains?

*MOU and JFAs are they reviewed to ensure that what Peoject Mgrs are promising is actually feasible by the IT environment. 24X7, 100% availability, access, etc.