

Auditor's Data Systems Checklist

How to score the answers: If the answer to a question is an unqualified 'yes', give the maximum point value for that question. If the answer is 'maybe' or 'almost', give the appropriate partial credit up to the maximum point value for that question. A definite 'no' rates a zero. Maximum score is 100 points.

A. Security Management (29pts)

Security Policy (9pts)	Max Score	Your Score
Does the institution have an established security policy? (The policy should have statements about confidentiality, personal privacy, and legal obligations.)	2	
Is the policy annually reviewed and updated with an annual signing off by all employees?	3	
Is there established funding for security?	2	
Is there an established policy ensuring the disabling of old accounts along with the returning of equipment. (like an employee separation check list)?	2	

Security Management (4pts)	Max Score	Your Score
Is there a Security Team accountable to the governing board, and does this committee meet on an annual basis?	2	
Does the Security Team include:	1	
<input type="checkbox"/> A physical security officer as recommended by Adventist Risk Management? <input type="checkbox"/> A technical advisor who can make suggestions about methods and ways to improve the data/Information security?	1	

Information Security Scope (16pts)	Max Score	Your Score
Scope: Does the scope of the Security Plan include <input type="checkbox"/> A long-term plan to improve external and internal defenses?	3	
<input type="checkbox"/> Regularly scheduled user training, as well as regular communications about security issues?	2	
Security Audit: Has there been an outside independent review of the system controls within the past two years?	2	
If an audit was completed in the past two years, have the recommendations been fully implemented?	1	

Crisis Management: Has a crisis management/operational continuity plan been written or updated within the past two years?	2	
Training and Testing: Has the crisis management plan been tested within the past year?	1	
Can current Tech Staff complete routine network management tasks?	2	
Can current Tech Staff complete security-related tasks regularly?	2	
Can current Tech Staff provide customer service at appropriate levels?	1	

B. Technology (57pts)

Perimeter Defenses (15pts)	Max Score	Your Score
Are ALL Internet and modem connections protected by a firewall or multifunction security appliance?	2	
Is the network perimeter protected by a spam/content filter?	1	
Do the firewall/multifunction devices include virus protection?	2	
Is spam, content, and virus protection enabled on email and web servers?	2	
Are all network devices that host spam, content, and virus protection regularly monitored, patched, and updated?	5	
Are all wireless access points fully encrypted (WEP at least, WPA preferred)?	2	
Are perimeter and internal defenses regularly tested for vulnerability to penetration?	1	

Network Architecture Security (7pts)	Max Score	Your Score
DMZ: Does your network design isolate web and email servers in a semi-isolated area commonly referred to as a DMZ?	3	
Segmentation: Are computer connections on your network logically organized by building, department or other hierarchical structure?	2	
Are the systems of limited control or monitoring separated from your main financial and record keeping systems?	2	

IT Management and Internal Defenses (32pts)	Max Score	Your Score
--	------------------	-------------------

Are backups	2	
<input type="checkbox"/> Performed regularly?	1	
<input type="checkbox"/> Tested routinely? (At least once a quarter)	1	
<input type="checkbox"/> Centrally managed?	2	
<input type="checkbox"/> Stored off-site on a weekly basis? (at least 5 miles away, preferably further)		
Is the network documented, and is the equipment inventory up to date?	2	
Maintenance and Monitoring Protocols:	1	
<input type="checkbox"/> network monitoring of bandwidth, connections, and file types	2	
<input type="checkbox"/> routine preventive maintenance of desktops, LAN servers, network appliances	1	
<input type="checkbox"/> scheduled testing of network performance		
Patch and Virus Management: Is virus protection software installed and automatically updated on every workstation?	4	
<input type="checkbox"/> Are software vulnerabilities patched routinely on all workstations? Add an additional point if patched automatically.	1	
Passwords: Is there a password policy in place and actively enforced?	1	
<input type="checkbox"/> <i>If all computers are password protected, give an additional 1 point.</i>		
<input type="checkbox"/> <i>If passwords must be changed periodically, (at least three times a year) give another 3 points.</i>	3	
Does the policy require unique accounts (no 'guest' accounts)? Does the policy prevent users from reusing previous passwords?	3	
Have all generic user accounts, such as ADMIN, ROOT or HOST been disabled?	3	
Is the email system encrypted or using https to ensure privacy?	2	
Are financial and medical records encrypted or accessed with an encrypted link?	3	

C. Environmental and Physical Security (5pts)

Environmental Security (2pts)	Max Score	Your Score
Environmental Disasters: Is your network infrastructure located and installed in an area protected from floods, hurricanes, tornadoes, or other regionally-relevant natural threats?	1	
Temperature and Humidity Control: Is network equipment properly ventilated? Power: Are all servers and network devices protected by uninterruptible power supply (UPS) devices?	1	

Physical Security (3pts)	Max Score	Your Score
Secure Locations: Are all network devices located in secure facilities exclusively dedicated to network operations? Secure Infrastructure: Are all switches, hubs, and wiring closets located in spaces not also used by custodians, librarians, etc.?	1	
Equipment Security: Are servers located in locked cabinets?	1	
Access Control: Are computer facilities accessible to students and staff only under controlled circumstances such that only staff/students who need access to specific systems have access?	1	

D. Staff Training/empowerment (12pts)

Staff Training and Communication (12pts)	Max Score	Your Score
Training: Is training done to increase user skill and understanding about passwords, security procedures, etc.? <input type="checkbox"/> Have a majority of users participated in these sessions?	4	
Communication: Are updates on technology and security regularly sent to stakeholders using email, newsletters, posters, and public media?	4	
Feedback: Are there regular electronic and face-to-face forums for user feedback, suggestions, and complaints? Is feedback respectfully listened to and acted upon?	4	

The answers to this audit are to the best of my knowledge and understanding accurate.

Name Interviewee

Name (Print): _____ **(Signature):** _____

This audit has been completed by:

Name (Print): _____ **(Signature):** _____

Date: _____

If the institution scores:

Below 20: Either the institution doesn't use IT to any significant degree, or the system is a disaster waiting to happen.

20 to 39: The institution's IT system is probably barely meeting the minimal basic security, but serious shortcomings remain and problems are likely to occur.

40 to 59: The institution's IT system is beginning to deal with the wide range of security requirements, but continued attention and effort will be needed to bring things up

to a more defensible state.

60 to 79: The institution's IT system is grappling with the wide range of security requirements, and while that does not guarantee that no problems will occur, they are exercising appropriate due diligence; however, some shortcomings remain and continued attention and effort will be helpful.

80 to 100: The institution's IT system is a model of good cyber security practice. Maintaining this status will require continuing attention and action.