Arkansas Division of Legislative Audit – Information Systems Best Practices Checklist

The following is a compilation of Information Systems best practices employed throughout industry and government, which have been adopted as minimal standards by the Arkansas Division of Legislative Audit (ADLA). This outline will likely be a work in progress, with changes and additions incorporated as the need arises. The purpose of compiling these best practices and then communicating them to entities throughout the state is to:

- raise awareness of technical areas which present the highest level of risk and are considered most important by ADLA (and throughout government);
- provide general guidance on minimal standards in these technical areas (which may serve as a refresher for counties more dependent on advanced technology while serving as a starting point for counties with smaller operations and less exposure to technical issues);
- provide ADLA with a documented framework to be updated and revised as necessary, based on changing best practices, to reference when recommending an entity change existing processes to comply with best practices.

Standards governing the audit profession published recently prohibit auditors from mandating the implementation of specific operational procedures since this impairs auditor independence. Simply put, management decisions must remain the responsibility of management. However, increased reliance on computer systems in everyday operations introduces significantly more complex control issues. These issues, as well as standard guidelines and acceptable risk, must be factored into management decisions to ensure proper authorization, accuracy and completeness of processed data. As stated previously, our goal is to raise awareness of potential (and real) threats and provide guidelines for management to reference when making decisions.

I.	**Application and General Controls – *Prior to the widespread availability and use of computers to capture transactions throughout the various county offices, manual processes were employed and internal controls were designed around each specific process to ensure accuracy and completeness of transaction data. The migration from manual processes to computer applications was conducted by application vendors focused on functionality required by county operations. Unfortunately, some internal controls previously established with the manual process were not considered in the design of these applications, since the development effort was not focused on controls. Although there are several key areas of concern when reviewing controls in place around applications and Information Systems, there are also general items that, when operating effectively, strengthen the overall control structure.***	
A.	Does county have Policy and Procedure document which addresses software copyright infringements (piracy), non-business use of workstations and county computer resources, internet usage guidelines, user responsibilities related to workstation security and maintenance of hardware and software (including workstation hard disk backup) and steps to follow if workstation, network or application problems are encountered?	☐
B.	Is an inventory of all network equipment (including workstations) and their locations maintained and kept current?	☐
C.	Adequate insurance maintained for production equipment?	☐
D.	If software was purchased, does county have maintenance agreement in force with vendor? Does agreement address process for requesting functionality enhancements or other program modifications from the Vendor? Does agreement address support commitments and response time guidelines?	☐

E.	If software was purchased, is vendor financially stable and does vendor hold application source code in escrow should they become insolvent and no longer be able to support the applications in use by the county?	☐
F.	If software developed and maintained internally, does county have programming staff knowledgeable with language used to write software application?	☐
G.	Is adequate and current documentation maintained relevant to operations and programming staff?	☐
H.	Are application controls sufficient to ensure the preservation of audit trail integrity? For example, can data be manipulated, modified or deleted from outside application security? Without leaving complete audit trail?	☐
I.	Are application controls sufficient to facilitate reconciliation of current balance at any given time, plus or minus documented and authorized adjustments to arrive at original charge? Without ability to reconcile balances given precise adjusting amounts the perceived reliability and accuracy of data declines. This would include prevention of ability to duplicate receipt numbers for different, unique receipts, the ability to re-use voided receipt numbers, the ability to change receipt date or any other receipt field without proper authorization and audit trail documentation.	☐
II.	**End-Users – *The success of any application is greatly dependent upon the training provided to the end-users initially and on a continuing basis. Continuing education is necessary to ensure employees are aware of, and proficient with, application enhancements and new releases. Recurring education also addresses training needs of new employees.***	
A.	Adequate training curriculum available to application users?	☐
B.	Established error identification and correction procedures?	☐
III.	**Data Access Security – *The purpose of data access security within any application is to grant users appropriate access privileges necessary for the job they perform while restricting privileges not needed for their job or that could create weaknesses in the Internal Control structure of the entity. Duties and responsibilities assigned to each job role should be defined by management that ensure adequate segregation of duties. Those job role definitions can then be used to establish specific application permissions granted and/or restricted. Data access security should also provide an audit trail, which could be utilized to identify specific users that made individual changes to the data. Network environments which allow users to access the data directly (typically via a database utility such as Paradox or MS Access), effectively voids data access security within the application and should not be allowed. This type of access allows users full update capability with no audit trail.***	
A.	Reasonable number of Data Security Administrators (typically 1 primary and 1 alternate)?	☐
B.	Established and effective process for timely removal of security access privileges from terminated employees? Process for periodic review of security assignments to ensure access privileges assigned remain current with job role access needs?	☐
C.	Effective security change request process? Standard form? Authorization required?	☐
D.	Effective user identification & authorization process (userID & password):	
	1. all user accounts should require use of passwords	☐
	2. require password change at initial logon	☐

	3. require password change on periodic, recurring basis not to exceed 90 days	☐
	4. lock user account after 3 unsuccessful logon attempts and remain locked until support is contacted for assistance	☐
	5. maintain password history file preventing re-use of last 5 passwords minimum	☐
	6. passwords should be required to meet minimum formatting standards (re: must contain combination of alpha and numeric characters and minimum of 8 characters), no repeating characters	☐
	7. documented policy manual which addresses use and care of passwords (exp. users should not write password on post-it note beside monitor and users should not share their passwords with other users) and "social engineering awareness"	☐
	8. sessions should timeout after 30 minutes of no activity and require userID and password entry to log back on to session	☐
E.	Security which governs application access cannot be circumvented using other utility programs (data manipulation such as adds, changes and deletes must be entered through application, ensuring accuracy and integrity of Audit Trail)?	☐
F.	Security assignments follow standard by job role (as opposed to unique access privileges for each individual which is more difficult to manage)?	☐
IV.	**Network Security – *This higher level of security would typically grant users the ability to access an application, then administration of the specific application security would be utilized to grant and/or restrict data access as necessary within the application. Networks become more complex as more efficient, effective and secure products are made available through advances in Information Systems technology. Preventive measures can reduce the risk associated with threats inherently caused by advances in technology.***	
A.	Is Virus Protection/Prevention software utilized and kept current? Is there a documented process in place to address steps necessary if a virus is identified on workstations or network equipment?	☐
B.	Is Intrusion Detection/Prevention software utilized and kept current to prevent unauthorized personnel from penetrating local network (this includes both access attempts from the internet and from dial-up access via modem)? Is there a documented process in place to address intrusions or intrusion attempts?	☐
V.	**Data Integrity – *The purpose of data integrity is to ensure complete and accurate data, which can be reported in any manner users require, with all fields formatted according to data definition rules and within established ranges (date fields should not allow month>12, day>31, and a code field should only be populated with valid values). The risk of internal fraud increases if individuals are granted the ability to modify program logic as well as production data.***	
A.	Adequate data input edits in place to prevent data corruption (on-line or batch)?	☐
B.	No programming personnel with ability to update application data.	☐
VI.	**Program Change Control – *The purpose of program change control is to ensure that only appropriate changes to program logic are made, performed in a timely manner, do not negatively impact other logic and ultimately produce the results expected by the user that requested the change.***	

A.	Effective process in place for tracking submission, approval and prioritization of program modification requests?	☐
B.	All changes to source code tracked with previous versions archived?	☐
C.	Access to source code adequately controlled?	☐
D.	Test process in place for program modifications?	☐
E.	User approval of test results required before modifications implemented?	☐
VII.	**System Interfaces – *The endless pursuit of efficiency gains has resulted in the ability to transfer data from one system to another electronically rather than expending time keying data into both systems. The exchange of data from one business application to another is considered an interface. The accuracy and completeness of data files transmitted to, or received from, other applications should be assured by a quality control process consistent with the receiving application's edit standards.***	
A.	Adequate balancing controls in place for files received and sent by software application to ensure accurate and complete transfer of data.	☐
VIII.	**Backup, Recovery and Business Continuity – *Disaster Recovery Planning is often not sufficiently addressed or is low on the priority list, as there is no immediate, detrimental impact to the entity, until a disaster or other situation preventing normal operations arises. The business entity should develop a Disaster Recovery Plan (DRP) that will cope with the unavailability of the computer application(s) during an unexpected outage. This plan should be written, approved by management and tested on a regular basis. The plan would address how the entity would recover from short or long-term outages, as well as how operations would continue during the recovery effort.*** At a minimum the plan should:	
A.	Identify the Disaster Recovery team. This could be the entity's Information System employees or software vendor personnel or a combination of both.	☐
B.	Identify critical applications that must be restored.	☐
C.	Identify software and data file backups needed to restore these applications. Backup retention periods and a secure off-site storage location should also be identified.	☐
D.	Address the acquisition of replacement hardware should it be needed.	☐
E.	Identify an alternate processing site should it be needed.	☐
F.	Test Disaster Recovery Plan on a reasonable, recurring basis. Deficiencies identified during the testing process should be used to make improvements and modifications to the plan as necessary.	☐
G.	Identify alternate procedures the users can use to cope with the unavailability of the computer application during the recovery period.	☐

IX. Wireless Network Security – (this section taken from Volume 3, 2004 of the Information Systems Audit and Control Association (ISACA) Journal and was authored by Susan Kennedy, CISA, CIW) ***Networking technology is dramatically changing the world of computing, creating considerable business opportunities as well as increasing security risks. One such technology, wireless networks, also known as broadcast networks or WLANs, are increasing in popularity at the institutional and consumer levels, primarily due to their ease of installation and their affordability. WLANs, which use radio frequencies to broadcast in the unlicensed 2.4 GHz frequency band, can be as simple as the use of two computers equipped with wireless network interface cards (NICs) or as complex as hundreds of computers outfitted with wireless NICs communicating through wireless access points (WAPs). Wireless technologies may empower users with easier and greater access to data at reduced costs and with low access barriers, but these conveniences also leave them vulnerable to data compromise and security breaches. This technology introduces a magnitude of critical security risks and challenges, and it is critical to implement strong security measures to mitigate significant risks. The following are potential risks and associated best practices to help organizations attain a more secure environment and greater understanding of WLANs' characteristics.***	
A. Insufficient Policies, Training and Awareness - Lack of sufficient policies to govern wireless networks and their use leaves unaddressed a number of configuration features and settings, which the end user must determine independently. While it appears to be a basic requirement, institutions often fail to guide their employees on their use of wireless networks and the risks associated with not using a wireless network in accordance with the policies. Once policies are implemented, it is critical to communicate them to the community to increase their awareness and understanding. To mitigate these risks:	
1. Develop institution-wide policies with detailed procedures regarding wireless devices and usage.	☐
2. Maintain these policies and procedures to keep current with technology and trends. While each institution has its specific requirements, they should, at a minimum, require the registration of all wireless networks as part of overall security strategy. A policy is not effective if its users are not in compliance.	☐
3. Monitor the institution's network to ensure the end users are following the policy as intended.	☐
B. Access Constraints - By design and out of necessity, WAPs repeatedly send out signals to announce themselves so end users can find them to initiate connectivity. This could make it easy for unauthorized users to learn the network name in an attempt to conduct an attack or intrusion. The WAPs' service set identifier (SSID) is a name or description that is used to differentiate networks from one another. Adhering to the following best practices will reduce the risks that SSIDs could present:	
1. Enable available security features to reap their benefit because embedded security features are disabled by default.	☐
2. Change the default settings. Default SSIDs are set according to the manufacturer. For example, CISCO's WAP default SSID is "tsunami" and Linksys' WAP default SSID is "linksys." Not changing the default SSID makes it easier and faster for an unauthorized user (a hacker) to gain access to the WAP.	☐

3. Use a closed network instead of an open network, so the SSID is not broadcast. End users type the SSID into the client application, instead of selecting the SSID from a listing when they click the scan button. This feature makes it slightly more difficult for the end user to gain access, but education on this risk mitigation strategy can reduce potential resistance. To gain maximum advantage of a closed network, change the SSID with some regularity to account for employees who have been terminated and no longer have authorized access to the network. Therefore, develop and implement an SSID management process to change the SSID regularly and to inform authorized employees of the new SSID.	☐
4. Track employees who have WLANs in their home or remote site. Require within the institutional policy that wireless networks be placed behind their own routed interface, so the institution can shut them off if necessary. If WLANs are utilized at home, policy should require specific security configurations, including encryption and VPN tunneling.	☐
C. Rogue Access Points **-** Rogue WAPs are WAPs that have been installed by end users without coordinating their implementation with the information systems team. Because they are becoming a more common occurrence due to their low cost and easy installation, users can easily and inexpensively purchase an access point and place it on the network without authorization or detection. Rogue WAPs are often poorly configured and might permit traffic that can be hard for intrusion detection software to pinpoint.	☐
D. Traffic Analysis and Eavesdropping - Without actually gaining access to the network, unauthorized parties can passively capture the confidential data traversing the network via airwaves, and can easily read the data because they are sent in cleartext. Thus, message modification is possible, such that an attacker may alter a legitimate message by deleting, adding to, changing or reordering the message, or the attacker can monitor transmissions and retransmit the message as a legitimate user. By default, wireless networks send unencrypted or poorly encrypted messages (using the Wired Equivalent Privacy standard) over the airwaves that can be easily intercepted and/or altered. Currently, wireless networks are beset by weak 802.11x access control mechanisms, resulting in weak message authentication. To mitigate these risks:	
1. Encrypt all traffic over the WLAN. There are a variety of methods to select from:	☐
2. Use application encryption, such as PGP (pretty good privacy), SSH (secure shell) or SSL (secure sockets layer).	☐
a. Use Wi-Fi Protected Access 2 (WPA2). WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1X-based authentication. (Note: WPA or WPA2 may require a software or firmware update/upgrade.)	☐
b. Require the use of a virtual private network (VPN) running at least FIPS-141 triple DES and encrypting all traffic, not only the ID and password. Segment all wireless network traffic behind a firewall, configure each client with a VPN client and tunnel over the wireless network to a VPN concentrator on the wired network. Configure it so users communicate only with the VPN concentration point. Evaluate the following features when purchasing VPN technologies: interoperability with existing infrastructure, support for a wireless and dial-up networking, packet-filtering or stateful-inspection firewall, automatic security updates and a centralized management console.	☐
3. Restrict LAN access rights by role.	☐

E. Hacker Attacks - Because wireless networks are insecure, they are prone to attacks. Such attacks can include spreading viruses, loss of confidentiality and data integrity, data extraction without detection, privacy violations and identity theft. To mitigate these risks:	
1. Utilize and maintain antivirus software. Push out antivirus software upgrades to clients from servers.	☐
2. Create frequent backups of data and perform periodic restorations.	☐
F. MAC Spoofing and Session Hijacking - Wireless 802.11 networks do not authenticate frames, which may result in altered frames, hijacked authorized sessions or stolen authentication credentials by an imposter impersonating the network. Therefore, the data contained within their frames cannot be assured as authentic, as there is no protection against forgery of frame source addresses. Since attackers can observe MAC addresses of stations in use on the network, they can adopt those addresses for malicious transmission. Finally, station addresses, not the users themselves, are identified, which is not a strong authentication technique and can be compromised by an unauthorized party. To mitigate these risks:	
1. Limit the WAP access to specific MAC addresses that are filtered via a firewall. This technique is not completely secure, as MAC addresses can be duped, but it does increase security in the overall security strategy. Another difficulty with this technique is the maintenance effort required. A MAC address is tied to a hardware device, so every time an authorized device is added to, or removed from, the network, the MAC address has to be registered into the database.	☐
2. Monitor logs weekly and scan critical host logs daily.	☐
3. Use proven data link layer cryptography, such as SSH, transport-level security (TLS) or IPSec.	☐