Arkansas Legislative Audit

Information Systems Best Practices

January 2018

TABLE OF CONTENTS

Page

PURPOSE

Arkansas Legislative Audit (ALA) has established the following Information System (IS) Best Practices, utilized throughout industry and government, to provide practical information about internal controls and encourage entities to develop, implement, and maintain IS policies and procedures that conform to current best practices. These guidelines can be utilized as a self-monitoring tool to understand, assess, and mitigate potential information security risks to the entity's operations and assets. These best practices should be used as a resource to improve the design of existing internal controls and to implement new policies and procedures required by changes in risk to assets and operations. Optimally, control policies and procedures should be described in a written document and distributed to all employees since the application of these control procedures is every employee's responsibility. Successful internal controls depend on management and staff commitment to the protection of resources.

Internal Controls

Internal controls are necessary for the effective and efficient operation of all levels of government. Internal controls are policies or procedures put in place to provide reasonable assurance that operations are achieving stated objectives. Properly designed and functioning controls reduce the likelihood that significant errors or fraud will occur and remain undetected.

Information technology (IT) is an integrated part of state and local government financial operations and should be considered in conjunction with overall internal controls planning. IT internal controls affect many aspects of financial operations and should be implemented and reviewed in conjunction with each office, department, or functional area of responsibility.

To execute responsibilities effectively, management needs to understand how an integrated internal control framework should work. Standards for Internal Control in the Federal Government "Green Book" (which may be found at https://www.gao.gov/products/GAO-14-704G) may also be adopted by state and local governmental entities.

Assessing Risk

Each governmental entity has its own unique set of circumstances and risks that will affect the design and implementation of its controls. Before determining which controls should be implemented, entities should assess the risk of fraud or error occurring and remaining undetected.

After identifying risks, entities should implement controls to mitigate or reduce those risks. During the design process, the relationship between the cost of implementing the control and the benefits to be gained should be considered. When it is not practical or cost-effective to implement certain controls, other controls should be considered as ways to mitigate risk.

Monitoring

Identifying risks and implementing control procedures will not protect assets and produce reliable financial information if employees do not follow established procedures. Policies and procedures should be regularly reviewed to confirm that controls are being executed as designed. It is also important to consider feedback received from employees. Some control procedures may appear to be good solutions to an identified risk but, once implemented, may cause unforeseen problems or inefficiencies. At the same time, other activities may not appear to need controls, yet upon further analysis, some type of control may be warranted.

While this document is intended to establish minimum levels of compliance for auditing purposes, it is not all-inclusive. Because the IT environment is rapidly changing, these guidelines will be modified periodically to reflect industry changes as closely as possible. Guidelines have been generalized, where possible, to allow for broad application to various types and sizes of entities. Current IT trends, business processes, and cost considerations specific to the individual entity should be considered when applying these guidelines.

INTRODUCTION

General Controls and Application Controls are the two principal classes of controls applicable to the IS environment. All IS controls throughout the industry may be broadly categorized as such and are presented here as follows:

Part One: General Controls

General Controls are mechanisms established to provide reasonable assurance that the information technology in use by an entity operates as intended to produce properly authorized, reliable data and that the entity is in compliance with applicable laws and regulations. Typically, General Controls include the following elements:

IS Management	(Best Practices 1-1)
Contract/Vendor Management	(Best Practices 1-2)
Network Security	(Best Practices 1-3)
Wireless Networking Security	(Best Practices 1-4)
Physical Access Security	(Best Practices 1-5)
Logical Access Security	(Best Practices 1-6)
Disaster Recovery/Business Continuity	(Best Practices 1-7)

Part Two: Application Controls

Application Controls relate to the transactions and data for each computer-based automation system; they are, therefore, specific to each application. Application controls are designed to ensure the completeness and accuracy of accounting records and the validity of entries made. In general, Application Controls contain the following components:

Data Input	(Best Practices 2-1)
Data Processing	(Best Practices 2-2)
Data Output	(Best Practices 2-3)
Application-Level General Controls	(Best Practices 2-4 through 2-7)

Part Three: Other Technology

Each entity has its own unique set of circumstances and risks that will affect the design and implementation of its controls. Before determining which controls should be implemented, management should assess the risk of fraud or errors occurring and remaining undetected.

Electronic Signatures and Digital Signatures	(Best Practices 3-1)
Payment Cards (Debit or Credit)	(Best Practices 4-1)
Bring Your Own Device (BYOD)	(Best Practices 5-1)
Electronic Banking	(Best Practices 6-1)

BEST PRACTICES – GENERAL CONTROLS

IS Management

1-1: IS management must ensure adequate internal controls are in place to achieve the organization's established objectives.

1-1.1: Develop an IS Department organizational chart and update as the environment changes.

1-1.2: Conduct an overall risk assessment of the organization's goals, functions, and reputation to identify risks associated with the use of information technology. Gain an understanding of current practices in addressing these risks and mitigating negative impacts.

1-1.3: Develop and maintain a formally-approved IS Operational Policy and Procedure Manual. The manual can be one document or several documents but should be reviewed and updated as the operating environment changes.

1-1.4: Ensure that duties of software developers and IS operators are distinctly segregated and clearly documented.

1-1.5: Develop policies and procedures addressing non-business use of entity equipment, facilities, and internet services.

1-1.6: Obtain proper replacement insurance for the production hardware/equipment.

1-1.7: Develop and document database and network backup processes.

1-1.8: Assign and communicate network backup responsibilities to designated staff.

1-1.9: Establish access to an environmentally safe, secure off-site location to retain network backups.

1-1.10: Establish and formally document frequency of backups, ensuring that minimum industry standards (i.e., daily, weekly, monthly, annually) are met. Backups should occur daily for critical processes or at longer intervals based on the significance of the information and frequency of changes.

1-1.11: Establish and formally document the method of backup:

a. Full Back up: Includes all files and software.
b. Incremental Backup: Copies files that have been changed since the previous backup.
c. Differential Backup: that's Copies all the data been changed since the last full backup.
d. Mirror Backup: Straight copy of the selected folders and files at a given instant in time.

1-1.12: Ensure that the selected backup process and retention policy are in compliance with laws and regulations.

1-1.13: Routinely copy operating system software, application software, hardware configurations, and production information to backup media based on frequencies set by management. This applies to all systems (e.g., local area network [LAN] or wide area network [WAN] servers, client/server database servers, special-purpose computers, etc.).

1-1.14: Frequently test data backups to ensure data are restored and recoverable. Also ensure backup settings are in compliance with entity policies.

1-1.15: Ensure administrator/super user accounts are limited and properly approved.

1-1.16: Regularly evaluate network availability and provide ongoing improvements to services and security as needed.

1-1.17: Establish and maintain a formal cybersecurity awareness program that ensures end users are aware of current cyber security threats the importance of protecting assets, and the related risks.

1-1.18: Make employees aware of social engineering threats, which are attacks carried out by persuading authorized users or administrators to reveal confidential information to people they don't know over the phone or through emails from unknown parties. Employees should be trained to never open or download suspicious attachments.

1-1.19: Periodically host cybersecurity training for employees. Training may consist of table top discussions on cybersecurity or security policy review. Relevant discussion and training on emerging cybersecurity threats, trending social engineering methods, limiting the types of sensitive information collected, transported and stored. Discuss viruses, malware and ransomware and the hazards of downloading email attachments, accessing malicious web sites and downloading files from the Internet.

Contract/Vendor Management

1-2: Outsourced IT vendors must adhere to laws, regulations, and the organization's policies and procedures.

1-2.1: Conduct a risk assessment to identify risks associated with outsourcing IT services. Based on the results of the risk assessment, determine the appropriate course of action to respond to the identified risk.

1-2.2: Review all contract(s) prior to approval to ensure that business processes and any applicable legal requirements are adequately addressed and documented.

1-2.3: Involve end-users in the project.

1-2.4: Establish a Service Level Agreement for the maintenance and support of the contract, carefully defining specific performance expectations for each party.

1-2.5: Test the vendor's business processes for fitness and adequacy to gain assurance that network and application security controls are properly understood and established within the entity.

1-2.6: Confirm that the vendor is a going concern. Ensure that provisions are made to hold application source code in escrow.

1-2.7: Limit vendor access to entity resources, and document monitoring and evaluation of access reasons and results.

1-2.8: Vendors of cloud computing services or other types of hosted solutions should comply with ALA IS Best Practices and the State of Arkansas information security standards through service level agreements and contracts.

1-2.9: Prior to transferring data or application services to the cloud computing environment, it is vital to understand applicable laws, regulations, duties and responsibilities imposed on both management and the vendor (e.g., data retention, data protection, jurisdictional issue, disclosures).

Network Security

1-3: Network Security ensures that network architecture includes controls over hardware, software, and data.

1-3.1: Establish a security policy for the network that is clearly documented and formally approved. Ensure that policies describe potential security risks (identified in section 1-1.2) and are clearly communicated to users. Provide for monitoring of emerging security threats to ensure policies are kept current.

1-3.2: Ensure that network devices (e.g., firewalls, routers, etc.) are appropriately placed and configured to adequately protect both internal and external access to devices, applications, and services.

1-3.3: Limit physical and logical access to network devices (e.g., firewalls, routers, servers, etc.), and ensure that changes to these devices are properly managed. Establish policies for proper tracking, authorization, testing, and approval of changes.

1-3.4: Obtain anti-virus, anti-malware, and advanced persistent threats software and provide for their continued use. Ensure programs are set for automatic updates, and scan devices on an established schedule. Also scan any media that is inserted into hardware (e.g., USB and external hard drives). Ensure that the network security policy covers use of external devices (e.g., USB drives, Smart Devices, etc.).

1-3.5: Establish a routine schedule for the performance and review of network vulnerability scanning, including documentation of critical risks identified and addressed.

1-3.6: Conduct a risk assessment to identify risks associated with allowing remote access to entity resources. Gain an understanding of current practices for addressing these risks and mitigating negative impacts.

1-3.7: Develop remote access authentication policies and procedures and encryption protocols (considering the risks identified above). Consider the use of virtual private networking (VPN) technology. Include procedures for usage restrictions, configuration/connection requirements, implementation guidance for each type of remote access allowed, and monitoring and handling of questionable activity.

1-3.8: Establish encryption methods for sensitive data transmitted externally and across the network, including procedures for keeping protocols current.

1-3.9: Ensure that all IT administration duties outsourced to a vendor are evaluated for risks associated with vendor access to your network and that vendor access is restricted only to files and applications needed to perform its duties. The contract with the vendor should provide that the vendor agrees to perform services in compliance with the entity's security policies and legal requirements.

1-3.10: Ensure operating systems are set to automatic updates. Turning off or rebooting computers regularly supports the installation of updates and refreshes system resources. Updates and patches for server operating systems are critical and should be reviewed and updated on a regular schedule.

Wireless Networking Security

1-4: Wireless security provides a secure network connection to prevent harm to the network and inappropriate access to resources.

1-4.1: Conduct a risk assessment to identify risks associated with the use of wireless networking. Gain an understanding of current practices for addressing these risks and mitigating negative impacts.

1-4.2: Establish security policies and procedures that ensure wireless usage restrictions, configuration, connection and password requirements, and implementation guidance for wireless access are authorized and protected. Address the use of wireless technology to ensure compliance with IEEE 802.11i Security Standard. Document policies to include the risks (identified above) associated with this technology, and ensure that policies are clearly communicated to users.

1-4.3: Ensure that the Service Set Identifier (SSID) is changed from the default value and a naming convention that excludes all identifiable information about the entity and the technology is in use. The SSID name should be communicated to entity employees.

1-4.4: Establish routine application of security patches for wireless access devices, ensuring that upgrades are applied as released.

1-4.5: Establish physical access controls over wireless devices to prevent unauthorized access, such that wireless devices are secured with locking mechanisms or kept in a restricted area where access is granted to authorized personnel only.

1-4.6: Review perimeter (external) security established in section 1-3.2, and ensure that the risks identified for wireless networking (see section 1-4.1) are adequately addressed in the placement and configuration of network devices.

1-4.7: Establish policies that appropriately limit and control remote wireless access, considering the risks identified above. Ensure that policies cover user identification and authentication, including procedures to ensure that all user accounts are properly authorized.

1-4-8: Ensure that entity-approved guest access allows users access to only the Internet, requires guest users to agree to terms of use, and states that user activity on the wireless network is monitored.

Physical Access Security

1-5: Physical access security controls are implemented to protect system resources and the facilities used to support their operation.

1-5.1: Develop a Physical Access Security Policy based on criticality of network devices and their physical placement. The policy should include access key/keycard management; authorization procedures for visitors, new employees, contractors, etc.; and provisions for cessation of access for terminated employees, consultants, security professionals, etc.

1-5.2: Ensure that the server room is adequately segregated from user areas and located in a discreet area inaccessible to outsiders and restricted to authorized personnel.

1-5.3: Ensure that data processing areas are properly segregated from public access and restricted to authorized personnel. Any devices that contain data should be physically secured in a locked room, cage, or other secure area.

1-5.4: Implement the following physical security controls:

a. Entrance and exit controls.
b. Visitor escorting.
c. Vendor escorting.
d. Logging of entry and exit dates and times.
e. Surveillance cameras.

1-5.5: Implement the following environmental controls, where possible:

a. Fire suppression system.
b. Smoke detector.
c. Temperature/Humidity detector.
d. Uninterruptible power supply (UPS).
e. Emergency power generator.
f. Raised floor.
g. Water detection.

1-5.6: Conduct a key/keycard inventory to identify those with physical access to facilities and to determine that terminated employee access has been properly removed. If unauthorized access exists, rekey doors, and change security codes to establish proper authentication. Develop specific procedures to ensure that terminated employee access is immediately disabled and to control issuance/revocation of access keys/keycards.

1-5.7: Develop a monitoring system for physical access, ensuring that access violations are detected and that both violations and corrective actions are documented.

1-5.8: Ensure that any data storage device, workstations, or other mobile equipment no longer in operation are reformatted/wiped based on current data sanitization methodologies or the hard drive physically destroyed to minimize the risk of exposure. Any paper documents containing personally identifiable information that are no longer in use should be shredded to minimize the risk of exposure.

Logical Access Security

1-6: Logical access security controls defend IT systems and data by verifying and validating the identity of authorized users.

1-6.1: Develop and document a Logical Access Security Policy, based on identified risk areas, to protect high-risk system resources. The policy should establish user identification, authentication, and account control mechanisms as well as protect system administration tools and utilities from unauthorized access. Include provisions for monitoring of access security best practices to ensure policies remain current.

1-6.2: Establish user security access on the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned duties in accordance with the entity's business process and functions.

1-6.3: Establish security administration procedures that ensure proper authorization of changes and additions to user accounts, including periodic review of user access security by resource owners (e.g., elected officials, directors, or their designees) and investigation of questionable authorizations. Access to security administration and other sensitive system resources should be narrowly limited to only users with a documented business purpose; all unnecessary accounts (e.g., system/admin default, guest, terminated users, etc.) should be removed or disabled.

1-6.4: Ensure that, at a minimum, the following password parameters for logical security controls are required:

a. User identification and password are required.
b. Users are systematically forced to change passwords on a periodic, recurring basis not more than 90 days.
c. Passwords are systematically required to be composed of a mixture of alpha and numeric characters and a minimum of 8 characters, with no repeating characters.
d. New users are forced by the system to change their initially assigned password.
e. A password history file systematically prevents reuse of at least the last five passwords.
f. The user account is locked after three unsuccessful logon attempts and remains locked until reset by an administrator or in a reasonable period of time.
g. Computer sessions timeout after a reasonable period of no activity, requiring user authentication to restore session.
h. Passwords are not revealed to anyone, including management, help desk personnel, security administrators, family members, or co-workers.
i. Management establishes and monitors user Activity Log/Audit Trail.

Note: Most operating systems and applications have configurable password settings that systematically require passwords to conform to the requirements listed above. Password settings are not considered enforced unless systematically required.

1-6.5: Implement checks and balances by users independent of security administration to ensure that procedures (established in section 1.6.2) are being followed (e.g., terminated employee accounts are immediately disabled).

1-6.6: Ensure that access attempts are logged and reviewed for violations. Document identified violations and associated corrective actions as a part of incident handling procedures.

1-6.7: Other technologies for user identification and authentication, such as biometrics (e.g., finger-print verification, signature verification) and use of hardware tokens (e.g., smart cards), are available and should be considered, if appropriate.

1-6.8: Systems using both user ID/password and ID/biometrics should enforce the same password parameters described at 1-6.4. Systems using ID/biometrics with password access disabled achieve the same level of security while eliminating physical credential and password management.

1-6.9: Restrict administrator privileges from running on workstations. Running in administrator mode increases exposure to security threats, which can lead to the entire network being compromised; administrative mode should be disabled by default.

Disaster Recovery/Business Continuity

1-7: Disaster recovery/business continuity planning directly supports an organization's goal of continued operations. Organizations should develop a Disaster Recovery and Business Continuity plan so that the effects of a disaster will be minimized. Adequate planning addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small.

1-7.1: Document and approve a Disaster Recovery and Business Continuity Plan that, at a minimum, achieves the following:

a. Ensures that disaster recovery roles and responsibilities are clearly defined.
b. Includes detailed instructions and procedures for restoring all critical systems (i.e., networking, operating system, and critical applications).
c. Identifies the alternate work/office location and the offsite backup storage facility.
d. Includes necessary contact information for employees, vendors, etc.
e. Includes manual operating procedures to be used until IT operations are restored.
f. Includes application-level contingency planning (established in section 2.7).
g. Covers all systems and operational areas.
h. Has been approved by appropriate governance.

1-7.2: Ensure that a copy of the Disaster Recovery/Business Continuity Plan is stored at the off-site backup location.

1-7.3: Ensure that the Disaster Recovery/Business Continuity Plan is relevant, addresses current risk, and is updated as conditions and risk change.

1-7.4: Conduct and document annual testing of the Disaster Recovery/Business Continuity Plan, to the fullest extent possible. Document in sufficient detail and evaluate test results, modifying the plan if necessary.

Note: The Arkansas Continuity of Operations Program (ACOOP) provides a methodology, hardware, software, training, and user assistance for the development, maintenance, and testing of disaster recovery plans for Arkansas agencies, boards, commissions, school districts, counties, and cities. These plans are intended to ensure that essential services continue to be provided after any disruptive event. For more information: http://www.dis.arkansas.gov/arkansas-continuity-of-operations-program-acoop

BEST PRACTICES – APPLICATION CONTROLS

Data Input

2-1: Data input controls are necessary to validate the integrity of data entered into an application.

2-1.1: After reviewing the following Application Control Best Practices, conduct a risk assessment to identify risks associated with the core financial applications in use. Gain an understanding of current practice for addressing these risks and mitigating negative impacts, either through enhancing automated controls or adding compensating controls to the existing processes.

2-1.2: Ensure that a properly designed database has been established to reduce redundancies and ensure effective transaction processing. Poor data quality may lead to failure of system controls, process inefficiencies, and/or inaccurate reporting.

[Example: The County Financial Manual may supply the data structure incorporated into the automated system and followed by users who classify data and perform data entry.]

Manual or automated controls should be incorporated into the data structure to prevent the following:

a. Recording or processing of duplicate transactions.
b. Unpopulated data fields.
c. Data formatting inconsistencies.
d. Improper coding to departments, business units, or accounts.

2-1.3: Establish input approval and review policies and procedures. Management should have procedures to identify and correct any errors that occur during the data entry process, providing reasonable assurance that errors and irregularities are detected, reported, and corrected:

a. Ensure that data input is done in a controlled manner (e.g., proper authorization controls exist, both systematic and manual).
b. Ensure that all inputs have been processed and accounted for.
c. Ensure checks and receipts are systematically pre-numbered and sequenced.
d. Ensure an audit trail is available and enabled with sufficient detail to identify the transactions and events as they happen by tracking transactions from their source.
e. Identify and investigate missing or unaccounted for source documents or input transactions.
f. Periodically review audit logs to evaluate the extent and status of data errors.
g. Require exception resolution within a specific time period.

Data Processing

2-2: Data processing controls provide an automated means to ensure processing is complete, accurate, and authorized.

2-2.1: Based on risk assessment, establish necessary controls over data processing (both automated and manual).

2-2.2: Ensure that processing errors are identified, logged, and resolved and that incorrect information is identified, rejected, and corrected for subsequent processing:

a. Edit reports should be produced by the system at critical processing stages (e.g., check runs, transaction posting, etc.), and corrections should be required before associated processes are completed.
b. Transaction or table logs should be available to compare to source documents.
c. Processing logs should be available to identify incompletely or incorrectly processed transactions.
d. Overrides applied to transaction processing should be tracked and monitored.
e. The application should perform online edit and validation checks on data being processed.
f. Warning and error messages should be produced during processing phases.
g. Transactions with errors should be rejected or suspended from processing until the error is corrected.

2-2.3: Establish input approval, and review policies and procedures. Management should have procedures in place to identify and correct any errors that occur during the data entry process. These procedures should reasonably assure that errors and irregularities are detected, reported, and corrected:

a. Ensure that data input is done in a controlled manner (e.g., proper authorization controls exist, both systematic and manual).
b. Ensure that all data inputs have been processed and accounted for.
c. Identify and investigate missing or unaccounted for source documents or data input transactions.
d. Periodically review user error logs to evaluate the extent and status of data errors.
e. Require data exception resolution within a specific time period.

2-2.4: Establish procedures to ensure that periodic reconciliations are performed between subsidiary ledgers and the general ledger, to include exception handling.

2-2.5: Establish monitoring procedures to include the following:

a. Reconciliation of data inputs to data processed by the application.
b. Maintenance of a processing log that is reviewed for unusual or unauthorized activity.
c. Monitoring of overrides applied to transactions.

2-2.6: Ensure that the software/application has the capability to prevent alteration of data when they are transferred from one process to another process.

2-2.7: Ensure that the software/application has the capability to identify and resume processing at the point where interruption occurred.

Data Output

2-3: Data output controls ensure the integrity and reliability of output information as well as the accuracy and timely distribution of all output produced.

2-3.1: Based on risk assessment, establish necessary controls over data output (both automated and manual).

2-3.2: Develop procedures for system output and reporting to ensure the following:

a. Consistency of content, format, and availability with end users' need.
b. Sensitivity and confidentiality of data.
c. Appropriate user access to output data.

2-3.3: Establish key reports and procedures to enable business process monitoring and tracking of results, including review of system-generated outputs/reports, to assure the integrity of production data and transaction processing. This review should be performed periodically.

2-3.4: Establish procedures to ensure that output is in compliance with applicable laws and regulations and that legally required reporting is complete and accurate. Review system-generated outputs/reports to assure the integrity of production data and transaction processing. This review should be performed periodically.

Application-Level General Controls

Application Security Management

2-4: Application security management identifies criteria and techniques associated with the design and use of applications for the computing environment that can be easily modified to respond quickly to the entity's changing business needs.

2-4.1: Based on risks identified in section 2.1.1, identify sensitive transactions for financial processes and sub-processes that application security policies should address. Develop a security policy for financial applications that achieves the following:

a. Establishes security administration procedures.
b. Depicts the methodology for developing the access structure and related security roles.
c. Outlines ongoing security role management (including monitoring and maintenance procedures).
d. Addresses the roles and responsibilities of the software vendor, if database/network administration services are contracted, in relation to transactional and master table update and the ways third party activity within the application will be tracked and monitored.
e. Defines maintenance procedures for application user security masters, incorporating procedures to ensure that updates, additions, and deletions are properly authorized and supported by a documented business purpose.
f. Periodically verifies that only authorized users have access and that their access privileges are appropriate.
g. Addresses encryption of sensitive application data (including authentication credentials), both stored and transmitted.
h. Considers application interdependencies and system interfaces, both internal within and external to the organization.
i. Documents critical data processing and transmission points and establishes procedures for security and verification of data at each juncture.
j. Demonstrates coordination with overall network security policy.
k. Provides a methodology for analysis of deficiencies by application and performance of corrective action.

2-4.2: Ensure that application access controls (e.g., unique user ID, password configuration, etc.) align with network access security policies established in section 1.6 and IS best practices.

2-4.3: Ensure that public access to applications is controlled via the following measures:

a. Restricted access to production systems and data.
b. Distinct security policy covering public access workstations that appropriately restricts data access and prevents access to local and network system resources and file directory structures.

2-4.4: Establish procedures for auditing and monitoring application security, including the following:

a. Identification and logging of reportable security exceptions and violations.
b. Setup of logging and other parameters to notify administrators of security violations as they occur.
c. Review of exception reports and recommended corrective action by process managers and security administrators.

2-4.5: Ensure that physical access to application resources has been secured and addressed by security policies.

Application Configuration Management

2-5: Configuration management establishes and maintains the integrity of the application throughout its life cycle.

2-5.1: Based on risk assessment, establish controls over programming to assure that changes to application functionality in production are authorized and appropriate and that unauthorized changes are detected and reported promptly.

Segregation of Duties

2-6: Segregation of duties is a basic internal control that attempts to ensure that no single individual has the authority to execute two or more conflicting transactions with the potential to impact financial transactions.

2-6.1: Ensure that process owners have identified and documented incompatible activities and transactions based on identified business process and application security risks. Ensure that application security policies address these areas and that users are systematically prevented from executing incompatible transactions.

2-6.2: Confirm that user access to transactions or activities that have segregation of duties conflicts is appropriately controlled.

a. Access to incompatible activities is assigned only when supported by a business need.
b. User access authorizations are periodically reviewed by process owners and security administrators for segregation of duties conflicts, considering position and process changes and updating access to current job assignments.
c. Users with authorized segregation of duties conflicts are documented, and their activity is monitored via transaction and audit logs.
d. Management retains documentation that segregation of duties risk has been mitigated through effective controls and monitoring.
e. Develop a Segregation of Duties grid by using the “roles and responsibilities” or security master report function within software applications wherever possible, and maintain an SOD grid for all key business processes.

Application Contingency Planning

2-7: Provide procedures and capabilities for recovering a major application or general support system. See Disaster Recovery/Business Continuity at 1-7.

2-7.1: Determine mission-critical functions performed by the financial applications, documenting associated key data and programs. Identify the impacts of automated process disruption and maximum allowable outage times for each application, and establish recovery time objectives.

2-7.2: Set backup retention policy for each application based on recovery time objectives, ensuring that backup intervals retained support necessary restoration periods. Current application programs and data should be copied according to this policy and securely stored at a geographically distant off-site location.

2-7.3: Establish manual procedures for continuing operations during outage times for the critical functions identified in section 2-7.1. Incorporate the application-level contingency planning and procedures (including backup policy) into the organization’s Disaster Recovery Plan.

2-7.4: Provide for periodic testing of the application contingency planning to include documentation of test results and corrective actions (including resulting changes to the plan) to be incorporated into organization-wide Disaster Recovery Plan testing and planning.

BEST PRACTICES – OTHER TECHNOLOGY

Electronic Signatures and Digital Signatures

3-1: Electronic confirmation of signatures is used to authenticate the content of a document.

3-1.1: If electronic signatures or digital signatures are used, management must understand the technology and associated risks, develop and implement controls to address risks identified and comply with applicable laws and regulations.

3-1.2: Resources include the following: Electronic Signatures in Global and National Commerce Act (15 USC 7001); Arkansas Electronic Records and Signatures Act (Ark. Code Ann. § 25-31-101); Uniform Electronic Transactions Act or UETA (Ark. Code Ann. § 25-32-101); and Arkansas Department of Information Systems Electronic Signature Standard SS-70-011.

3-1.3: Ensure that implementation of the electronic equivalent of a written signature, which can be recognized as having the same legal status as a written signature, provides adequate security. A digitized written signature can easily be copied from one electronic document to another, with no way to determine whether it is legitimate. Electronic signatures, on the other hand, are unique to the message being signed and will not verify if they are copied to another document.

3-1.4: A software application that creates a signature on checks and affixes the signature to the check should have an associated access control mechanism. Access controls should only be known by the cash custodian.

Payment Cards (Debit or Credit)

4-1: Payment cards enable the owner (cardholder) to make a payment by electronic funds transfer.

4-1.1: If payment cards are accepted for payment, management must understand the technology and associated risks, develop and implement controls to address risks identified, and comply with applicable laws and regulations.

4-1.2: Resources include the Payment Card Industry (PCI) Data Security Standards (DSS).

Bring Your Own Device (BYOD)

5-1: Bring Your Own Device (BYOD) is the use of personal electronic devices to access entity systems, data, and resources. Such devices include, but are not limited to, smart phones, tablets, laptops, and similar technologies.

5-1.1: If BYOD is allowed, management must understand the technology and associated risks, develop and implement controls to address risks identified, and comply with applicable laws and regulations.

5-1.2: Ensure use of the device security features, such as a PIN, password/passphrase, and automatic lock to help protect the device when not in use.

5-1.3: Keep the device software up to date. Devices should be set to update automatically.

5-1.4: Activate and use encryption services and anti-virus protection if your device features such services. Install and configure tracking and/or wiping services, such as Apple's "Find My iPhone," Android's "Where's My Droid," or Windows' "Find My Phone," if the device has this feature.

5-1.5: Remove any entity information stored on your device, including deleting copies of attachments to emails, such as documents, spreadsheets, and data sets, as soon as you have finished using it.

5-1.6: Remove all entity information from your device and return it to the manufacturer's settings before you sell, exchange, or dispose of your device.

5-1.7: In the event that your device is lost or stolen or its security is compromised, you must promptly report this to entity management.

5-1.8: Establish a comprehensive BYOD policy that provides policies, standards, and rules of behavior for the use of personally-owned devices. These policies must be adhered to in order to access organizational resources.

Electronic Banking

6-1: **Electronic banking enables bank customers to perform account management and enact account transactions directly with the bank over the Internet. Despite security controls, there is no absolute way to guarantee the safety of online electronic transactions. Entities should research and understand the risk involved before commencing online electronic transactions.**

6-1.1: Develop comprehensive policies and procedures for all electronic transactions (e-transactions), online banking, and EFT activities. Policies and procedures should include statutory and other legal requirements and responsibilities, as well as the following:

a. Documentation of proper segregation of functions (i.e., initiator cannot be an approver, etc.).
b. Online banking and EFT activities that will be used.
c. Person(s) authorized to initiate e-transactions.
d. Person who approves e-transactions.
e. Person who transmits e-transactions.
f. Person who records e-transactions.
g. Person who reviews and reconciles e-transactions and how frequently reviews are performed.

6-1.2: Establish a dedicated “hardened” computer with only application/services loaded that are necessary to perform online banking transactions. This computer should not be used for any other purpose. However, in cases where a dedicated computer is not available, entities must be able to reduce online banking risks to an acceptable level through a combination of other controls.

6-1.3: Install on the computer antivirus, anti-spyware, and malware and adware detection software that is current and set to automatically update.

6-1.4: Ensure all updates and patches to software, operating systems, and hardware are installed timely.

6-1.5: Install firewalls and intrusion detection and prevention systems with continuous monitoring. Any unauthorized and/or suspicious behavior or traffic should be investigated and, if necessary, blocked using access control lists in conjunction with a firewall.

6-1.6: Employ two-factor authentication, require password complexity using unique login ids and passwords, and ensure computers and browsers are not allowed to save passwords.

6-1.7: Frequently delete browsing history, temporary Internet files, and cookies. In the event the system is compromised, any information captured will not be stolen by a hacker or malware program.

6-1.8: Check that the session is secure before undertaking any online banking.

6-1.9: Regularly monitor bank accounts for unauthorized or suspicious activity, and report any suspicious activity immediately.

6-1.10: Ensure written agreements with banks provide appropriate controls for all electronic or wire transfers.

6-1.11: Ensure computer is disconnected from the Internet by unplugging the Ethernet/DSL cable when not in use.

6-1.12: Employ dual-authorization of transactions, enforced by bank security where possible (requiring at least two user accounts to submit and approve electronic transactions). #4 on EFT Approval Request.

6-1.13: Disallow online account management functions (such as adding users or modifying user security). Account changes should be conducted in person, or at least in writing, with the bank.

6-1.14: When possible, implement use of out-of-band transaction verification (such as text message or other security message to an approver with the entity).

6-1.15: Use a clearing bank account when paying electronically rather than paying directly from primary account.

6-1.16: Put transaction and daily limits in place to lower loss potential.

6-1.17: Consider the cost benefit of breach or fraud insurance.

6-1.18: Restrict browser(s) to sites necessary for EFT.

6-1.19: Ensure that users performing banking transactions use only non-administrative user accounts.

6-1.20: Implement use of controls such as “positive pay,” when possible and feasible, to ensure that the bank only processes authorized transactions it has been instructed to perform.

6-1.21: Implement use of processing calendar with the bank, if possible, to ensure the bank only processes transactions on pre-established days throughout the year.

6-1.22: Comply with all security requirements outlined in the Service Level Agreement with the bank and all other prudent security measures.