Arkansas Legislative Audit

Information Systems Best Practices

October 2024

TABLE OF CONTENTS

Page

PURPOSE

Arkansas Legislative Audit (ALA) has established Information System (IS) Best Practices that are widely used in both industry and government. These best practices provide practical information about internal controls and are meant to encourage organizations to develop, implement, and maintain IS policies and procedures that adhere to current best practices. ALA recommends that entity management conduct a formal risk assessment and use the results to determine which best practices are suitable for their specific environment. Since each situation is unique, management should use these guidelines as a self-monitoring tool to understand, assess, and mitigate potential information security risks to the organization's operations and assets. These best practices should be used as a resource to enhance the design of existing internal controls and to implement new policies and procedures required by changes in risk to assets and operations. It's important to note that these best practices are not comprehensive, and they do not replace locally developed internal control policies and procedures. Ideally, control policies and procedures should be documented and distributed to all employees, as the application of these control procedures is the responsibility of every employee. The effectiveness of internal controls depends on the commitment of both management and staff to protecting resources.

ALA encourages organizations to adopt the CIS 18 Critical Security Controls developed by the Center for Internet Security. These controls, available at https://www.cisecurity.org/controls/cis-controls-list, provide best practices to strengthen cybersecurity posture and protect against prevalent threats. They address vulnerabilities caused by poor cyber hygiene and help establish good cyber hygiene to defend against cyber threats. Note: If links in this document are not clickable, please copy and paste them into a web browser.

Internal Controls

Management is responsible for ensuring proper controls and functioning as intended. Therefore, internal controls are essential for the effective and efficient operation at all levels of government. Internal controls encompass activities, policies, and procedures designed to reasonably ensure that operations meet stated objectives. Well-designed and functioning controls assist an organization in adapting to changing situations, demands, and threats while reducing the likelihood of significant errors or fraud occurring and going undetected.

External auditors are not responsible for the design and effectiveness of internal controls, but they evaluate them as part of their audit planning process. Management is responsible for ensuring proper internal controls are in place and performing as intended. A governing body's responsibility is to adopt written policies established by management to provide oversight, authorization, and ethical leadership. Additionally, management should be aware of the impact information technology (IT) has on the internal control framework and the challenges associated with a digital environment.

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. Internal IT controls affect financial operations and should be implemented and reviewed by each office, department, or functional area of responsibility.

To execute responsibilities effectively, management must understand how an integrated internal control framework should work. State and local governmental entities may also adopt the Standards for Internal Control in the Federal Government "Green Book," which can be found at https://www.gao.gov/greenbook.

Assessing Risk

Each governmental entity remains unique in its circumstances and risks that affect the design and implementation of internal controls. Before determining which controls should be implemented, entities should conduct a formal risk assessment to identify, analyze, and respond to potential risks, fraud, or errors that may occur and remain undetected.

After identifying risks, entities should implement controls to mitigate or reduce those risks. The relationship between the cost of implementing controls and the benefits gained during the design process should be considered. When implementing specific controls is not practical or cost-effective, other controls should be considered to mitigate risk.

Monitoring

Identifying risks and implementing adequate controls will only protect assets and produce reliable financial information if management and employees 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 reasonable solutions to an identified risk; however, they may cause unforeseen problems or inefficiencies once implemented. At the same time, other activities may not need controls, yet upon further analysis, some 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 dynamic and ever-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 and Application Controls are the main control activities 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 established to provide reasonable assurance that the information technology an entity uses operates as intended to produce properly authorized, reliable data when needed and that the entity complies 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 produced by each computer-based automation system; they are, therefore, specific to each application. Application controls should be designed to ensure accounting records' confidentiality, completeness, accuracy, and the validity of entries made. Typically, Application Controls contain the following elements:

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

To manage risk with other technology, entities must understand it and its associated risks. Risk can be managed by being technologically proficient and establishing practices related to governance. Other technology elements include:

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)

Note: Items underlined have been modified since the last published date of August 2023.

BEST PRACTICES – GENERAL CONTROLS

IS Management

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

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

1-1.2: Conduct a formal, organization-wide IT risk assessment utilizing a standard risk assessment framework to:

- Identify "what could go wrong" events resulting from malicious or unintentional acts that can lead to negative consequences.
- Determine the levels of cybersecurity risk and the probability of exposure or loss resulting from an organization's security event or data breach.
- Dedicate adequate resources to implement safeguards to mitigate risks.
- Conduct a risk assessment involving engaging employees at all levels to identify risks and how those risks affect organizational objectives.

IS management should monitor and manage ongoing risks associated with information technology, understand current practices, and involve end users in addressing these risks and mitigating negative impacts.

1-1.3: Develop and maintain a process to identify and address hardware and software security vulnerabilities.

1-1.4: Develop and maintain a formally approved IS Operational Policy and Procedure Manual. The manual may be one or more documents and should be reviewed and updated annually and as the operating environment changes.

1-1.5: Ensure that the duties of software developers and end users are distinctly segregated and documented.

1-1.6: Develop policies and procedures addressing non-business use of entity equipment, facilities, and Internet services. Require employees to sign a technology use policy. This policy should clarify that information processed and stored on government computers is not considered private. Stipulate that computers and other government resources should not be used for personal purposes, the policy may allow for incidental personal use, and penalties for misuse of equipment should be outlined.

1-1.7: Develop and maintain an up-to-date inventory of all hardware devices attached to the network physically, virtually, or remotely. Ensure only authorized devices are allowed to connect. Establish a process to identify and address unauthorized devices. Include information about the asset (location, tag number, owner, operating system, IP, and MAC address, if applicable). Review and update bi-annually.

1-1.8: Develop and maintain an accurate inventory of all software running on your systems and network. Identify unauthorized and unmanaged software and prevent its installation or execution. If appropriate, include vendor name, version, install date, and asset tag. Review and update bi-annually.

1-1.9: Obtain proper replacement insurance for production software and hardware/equipment.

1-1.10: Establish and maintain a data management policy/process that addresses data sensitivity, ownership, retention periods, location, storage, and disposal.

1-1.11: Develop and document database and network backup processes, including how often data are backed up and how copies of backups will be maintained.

1-1.12: Assign and communicate database and network backup responsibilities to designated staff.

1-1.13: Establish access to an environmentally safe, geographically separate, secure off-site location to retain database and network backups.

1-1.14: Establish and formally document the frequency of backups, ensuring that minimum industry standards (e.g., daily, weekly, monthly, annually) are met. For critical processes, backups should occur daily or at longer intervals based on the significance of the information and the rate of changes.

1-1.15: Establish and formally document the method of backup:

a. Full Backup: All files and software.
b. Incremental Backup: Files that have changed since the previous backup.
c. Differential Backup: All the data that have changed since the last full backup.
d. Mirror Backup: Straight copy of the selected folders and files at a given time.
e. Maintain offline copies of backups in case a cyberattack renders online files unusable.

1-1.16: Ensure the selected backup process and retention policy comply with laws and regulations. Retention policy may include retaining periodic snapshots of data backups if data becomes corrupted and contaminates the backup.

1-1.17: Maintain documented security configuration standards for all hardware and software update documentation annually or when significant enterprise changes could impact this safeguard.

1-1.18: 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.).

1-1.19: Maintain and annually test offline data backups of critical systems and data storage.

1-1.20: Establish and maintain user and administrative accounts inventory. At a minimum, the inventory should contain the person's name, username, start/stop dates, and department.

1-1.21: Ensure administrator/super user accounts are limited and properly approved.

1-1.22: Develop a breach notification policy that requires individuals to be notified when a security incident occurs and confidential information is compromised.

1-1.23: Regularly evaluate network availability and reliability and provide ongoing improvements to services and security as needed.

1-1.24: Establish and maintain a formal cybersecurity awareness program to ensure that all end users receive education on current and emerging cybersecurity threats, the importance of protecting assets and the associated risks.

1-1.25: Ensure employees are aware of social engineering threats, which are attacks that involve 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 never to open or download suspicious attachments.

1-1.26: Periodically host cybersecurity training for employees. Examples of relevant discussion and training topics include but are not limited to:

a. Tabletop discussions on cybersecurity or security policy review.
b. Emerging cybersecurity threats.
c. Trending social engineering methods.
d. Limiting the types of sensitive information collected, transported, and stored.
e. Hazards of viruses, malware, ransomware, and spyware.
f. Accessing malicious websites.
g. Download files from the Internet or clicking links.
h. Embedded email links and downloading attachments that may appear reasonably valid.

1-1.27: Establish a formal Security Incident Response plan. This plan should outline the strategy for responding to information security incidents. Given the wide variety of security incidents that an organization could face and the rapidly evolving threats, this document should be designed to guide a response to security incidents, determine the scope and risk of security events, and ensure an appropriate response to information security incidents, including communication of incidents to the relevant parties. Please refer to NIST 800-61 revision 2 for guidance on developing a security incident plan.

1-1.28: In accordance with Arkansas Act 260 of the 2021 Regular Session, a public entity or a contractual provider of a public entity is required to provide a written initial report of known facts regarding a security incident to the Legislative Auditor within five business days of becoming aware of the incident. Furthermore, the public entity must provide regular updates. Any report, update, notification, or list created or maintained under this section is exempt from the Freedom of Information Act (FOIA) as it is considered a security function under Ark. Code Ann §25-19-105(b)(11).

The Security Incident Reporting form is located at www.arklegaudit.gov

Contract/Vendor Management

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

1-2.1: Ensure that all contracts are reviewed before approval to guarantee compliance with Ark. Code Ann. § 10-4-424, which grants Arkansas Legislative Audit access and authority to audit computer applications supplied by vendors. It is also crucial to confirm that business processes and applicable legal requirements are thoroughly addressed and documented.

1-2.2: Establish a service level agreement for the maintenance and support of each contract, specifically defining each party's performance expectations.

1-2.3: Confirm that the vendor is a going concern. Ensure that provisions are made to hold application source code in escrow.

1-2.4: Limit vendor access to entity resources. Log access, monitor vendor activity, and review for appropriateness.

1-2.5: Vendors of cloud computing services or other hosted solutions should comply with ALA IS Best Practices and the State of Arkansas information security standards through service level agreements and contracts and provide a Service Organization Control Report (SOC), if available.

1-2.6: Prior to transferring data or application services to or from a cloud computing environment, it is vital to understand applicable laws, regulations, duties, and responsibilities imposed on both management and the vendor (e.g., data ownership, data stewardship, data retention, data protection, jurisdictional issues, disclosures).

Network Security

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

1-3.1: Establish a network security policy that is clearly documented and formally approved. Ensure the policy describes potential security risks (identified in sections 1-1.2) and communicates risks to users. Policies should be kept current through regular review and updated to address emerging security threats.

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

1-3.3: Implement DNS (Domain Name System) filtering to block malicious websites and filter out harmful or inappropriate content.

1-3.4: 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.

1-3.5: State of Arkansas governmental entities should transition to the government-restricted ".gov" top-level domain. The .gov domain establishes itself as a trusted source for online services like websites or emails. It identifies an entity as a government agency, improves security and trust in services provided at any level of government, and is available at no cost at https://get.gov/registration/

1-3.6: Implement email authentication technology to protect users from spam, phishing scams, and other malicious emails.

1-3.7: Ensure a process exists to identify, detect, and address unauthorized assets on the network.

1-3.8: Obtain anti-virus, anti-malware, and advanced persistent threat software and provide for their continued use. Ensure programs are set for automatic updates and scan devices on an established schedule. Scan any media inserted into hardware (e.g., USB and external hard drives). Ensure the network security policy covers external devices (e.g., USB drives, Smart Devices, etc.).

1-3.9: Establish and maintain a process for performing internal and external network vulnerability scanning, including a remediation process to address critical risks identified.

1-3.10: Develop remote access authentication policies, procedures, and encryption protocols (considering the above-mentioned risks). 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.

1-3.11: Establish encryption methods for sensitive data transmitted externally and across the network, including procedures for keeping protocols current and effective.

1-3.12: Ensure all IT administration duties outsourced to a vendor are evaluated for associated risks. Vendor access to your network should be restricted to files and applications needed to perform the vendor's 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.

1-3.13: 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.

1-3.14: Enable and monitor network audit logs to identify potential misuse of system resources or information. Logging activities shall include regularly monitoring system access to prevent attempts at unauthorized access and confirm access control systems are effective.

1-3.15: Consider a defense-in-depth methodology by implementing multiple layers of security to protect data, networks, and systems. Successive layers of defense mechanisms can reduce the risk of a successful attack by someone with malicious intent. A combination of controls ensures that systems do not become overly dependent on any one control or layer of security and provides added protection in case a layer fails to function correctly or does not prevent or stop a threat to your data or systems.

1-3.16: Apply critical updates and patches to systems and hardware within 14 days. Apply all other updates and patches to systems and hardware not designated as essential within 30 days. Obtain patches, system upgrades, or other vendor releases from trusted sources. Periodically audit and remediate systems and appliances that are missing updates.

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: Establish security policies and procedures that ensure wireless usage restrictions, configuration, connection, and password requirements, as well as implementation guidance for wireless access, are appropriate. Policies and procedures should identify information resources that should and should not be available to users and the types of prohibited communications, especially when sensitive and/or critical data are involved. 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 communicated to users.

1-4.2: Ensure that the Administrator credentials and Service Set Identifier (SSID) are changed from the default value and a naming convention that excludes all identifiable information about the entity and the technology in use. The SSID name should be communicated to entity employees but not publicly broadcast.

1-4.3: Establish routine security patch applications for wireless access devices, ensuring that upgrades are applied as they are released.

1-4.4: Maintain an inventory of authorized access points (APs) and periodically conduct site inspections to determine that no unauthorized APs are in use.

1-4.5: Establish physical security controls over wireless network devices to prevent unauthorized access. For example, all devices should be secured with locking mechanisms or kept in a restricted area where only authorized personnel can access.

1-4.6: Review perimeter (external) security established in sections 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: Ensure that entity-approved guest access only allows Internet browsing and requires guest users to agree to terms of use, state 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 network devices' criticality and physical placement. The policy should include access key/keycard management, authorization procedures for visitors, new employees, contractors, etc.; and provisions for removing access for terminated employees, consultants, security professionals, etc.

1-5.2: Ensure that the server room and data processing areas are adequately restricted to authorized personnel and located in a discreet area inaccessible to outsiders.

1-5.3: 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.

1-5.4: Implement the following environmental controls, where possible:

a. Fire suppression system.
b. Smoke detector.
c. Temperature/Humidity monitor.
d. Adequate ventilation and air conditioning systems.
e. Uninterruptible power supply (UPS).
f. Emergency power generator.
g. Raised floor.
h. Water detection.

1-5.5: Develop specific procedures to immediately disable terminated employee access and control the issuance/revocation of access keys/keycards. Conduct an annual inventory of keys/keycards to identify facility access and ensure terminated employee access is revoked. If unauthorized access is found, rekey doors and change security codes.

1-5.6: Develop a monitoring system for physical access, ensuring that access violations are detected and violations and corrective actions are documented.

1-5.7: To minimize the risk of exposure, securely wipe or destroy unused data storage devices such as workstations or mobile devices and paper documents containing personal information.

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 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 and protect system administration tools and utilities from unauthorized access. Include provisions for monitoring access security best practices to ensure policies remain current.

1-6.2: Establish user security access based on the principle of least privilege, allowing only authorized access necessary for assigned duties in line with the entity's business processes.

1-6.3: Establish a process for granting access to enterprise assets for new hires and role changes, ensuring proper authorization and periodic review by resource owners. Investigate questionable authorizations and limit access to sensitive system resources to users with documented business purposes. Remove or disable unnecessary and unauthorized accounts.

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

a. User identification and a password are required.
b. Users are required to change passwords every 90 days, with passwords of at least 12 characters changed every 185 days.
c. Passwords must be at least 8 characters long, mixed with letters and numbers, and not repeating characters. We strongly recommend using 12 characters.
d. The system forces new users to change their initially assigned password.
e. A password history file systematically prevents the reuse of at least the last 24 passwords/phrases.
f. The user account will be locked after five unsuccessful login attempts and will remain locked until reset by an administrator or within a reasonable period of time. After a reasonable period of no activity, computer session timeout requires user authentication to restore the session.
g. Passwords are not revealed to anyone, including management, help desk personnel, security administrators, family members, or co-workers.
h. Passwords should not be stored in plaintext, which means storing a password in clear, readable text.
i. Management establishes and monitors the user Security Event Log.
j. Ensure all employees with access to essential systems and services use multifactor authentication (MFA). This requirement includes access to web-based platforms, such as financial institutions, third-party applications, and webmail services. All administrative accounts, except service accounts, should use MFA.

Note 1: Most operating systems and applications have configurable password settings that systematically require passwords to conform to the above mentioned requirements. Password settings are not considered enforced unless systematically required.

Note 2: Any deviations from established password best practices are evaluated case-by-case.

1-6.5: Ensure Security Event Logs are regularly reviewed for violations. Document any identified violations and associated corrective actions as part of incident handling procedures.

1-6.6: Other technologies for user identification and authentication, such as biometrics (e.g., fingerprint verification, signature verification) and use of hardware tokens (e.g., smart cards) are available and should be considered, if appropriate.

1-6.7: Systems using user ID/password and ID/biometrics should enforce the same password parameters described at 1-6.4.

1-6.8: Restrict administrator privileges from running on workstations. Running in administrator mode increases exposure to security threats, which can compromise the entire network; administrative mode should be disabled by default or, at a minimum, protected with strong credentials and utilized only when necessary to perform administrator functions.

Disaster Recovery/Business Continuity

1-7: Disaster recovery and business continuity planning involves creating plans, policies, procedures, and technical measures to help restore IT operations after an unexpected incident. Organizations should develop a comprehensive plan to minimize the impact of a disaster. Adequate planning should address how to keep critical functions operating in the event of large and small disruptions, ensuring the organization can continue its operations as usual.

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 technical instructions and procedures for restoring mission-critical processes and 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. Ensures manual operating procedures and resources are in place if IT operations are unavailable.
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.
i. Includes details concerning how the plan will be periodically tested.

1-7.2: Ensure a copy of the Disaster Recovery/Business Continuity Plan is stored at the off-site backup location. A copy should also be available to management and employees in either electronic or hardcopy form.

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

1-7.4: Conduct and document annual test scenarios of the Disaster Recovery/Business Continuity Plan. Evaluate test results and update the plan as necessary.

Note: Effective July 1, 2021, management of the Arkansas Continuity of Operations Program (ACOOP) will transfer from the Department of Transformation and Shared Services (TSS) Division of Information Services (DIS) to the Arkansas Division of Emergency Management (ADEM) due to the recent approval of Act 70 of 2021.

Several formats, guidance documents, and other assistance are available for writing and maintaining continuity plans. One example is the FEMA Continuity Plan Template and Instructions for Non-Federal Entities found at this link: https://www.fema.gov/pdf/about/org/ncp/coop/continuity_plan_non_federal.pdf

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: Establish a properly designed database to reduce redundancies and ensure effective transaction processing. Poor data quality may lead to system control failure, process inefficiencies, and/or inaccurate reporting.

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

Manual and/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.

2-1.2: 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 controlled (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 by tracking them 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 and changes.
g. Require a monthly exception resolution and ensure all exceptions are resolved before year-end closing.

Data Processing

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

2-2.1: Ensure that processing errors are identified, logged, and resolved and that incorrect information is identified, rejected, and corrected for subsequent processing. The system should produce edit reports at essential processing stages to trace transactions from beginning to end (e.g., check runs, transaction posting, etc.), and corrections should be required before associated processes are completed.

a. Database transactions or table logs should be available to compare to source documents.
b. Processing logs should be available to identify incomplete or incorrectly processed transactions.
c. Transaction processing overrides should be tracked and monitored.
d. Application should perform edit and validation checks during data processing.
e. Warning and error messages should be produced during all processing phases.
f. Transactions with errors should be rejected or suspended from processing until the error is corrected.

2-2.2: Management should have policies and procedures in place to identify and correct any errors that occur during the data entry process. These policies and procedures should reasonably assure that errors and irregularities are detected, reported, and corrected timely:

a. Ensure that data input controls are in place (e.g., proper authorization controls exist, both systematic and manual).
b. Periodically review user error logs to evaluate the extent and status of data errors.
c. Ensure that all data inputs have been processed and accounted for.
d. Investigate missing source documents or data transactions.
e. Data exception resolution is required before year-end closing.

2-2.3: Establish procedures to ensure that periodic and timely reconciliations and error corrections are performed between the subsidiary and general ledgers.

2-2.4: Establish monitoring procedures to include:

a. Reconciling data inputs to data processed.
b. Maintaining a processing log and reviewing for unusual or unauthorized activity.
c. Monitoring all overrides to transactions.

2-2.5: Ensure that the software/application can prevent data alteration when they are transferred from one process to another.

2-2.6: Ensure that the application can resume processing at the point of interruption.

Data Output

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

2-3.1: Develop procedures for system output and reporting to ensure:

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

2-3.2: Establish procedures to enable business process monitoring and tracking of results. Review system-generated reports to ensure the integrity of production data and transaction processing. Review should be performed timely and periodically.

2-3.3: Establish procedures to ensure that output complies with applicable laws and regulations and that legally required reporting is complete and accurate. Review system-generated reports to ensure the integrity of production data and transaction processing. Reviews should be performed timely and periodically.

Application-Level General Controls

Application Security Management

2-4: Application security management identifies criteria and techniques associated with designing and using applications that can be modified to respond to the entity's changing needs.

2-4.1: Identify transactions for financial processes and sub-processes that application security policies should address. Develop a security policy for financial applications that achieves:

a. Establishes security administration procedures.
b. Develop an application access structure based on the principle of least privilege.
c. Outlines ongoing security role management (including monitoring and maintenance procedures).
d. Addresses the roles, responsibilities, and monitoring of third-party vendors.
e. Ensures access security 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 for their job functions.
g. Addresses encryption of application data (including authentication credentials), both stored and transmitted.
h. Establishes procedures for documenting security and data verification for internal and external system interfaces.
i. Coordinates with overall network securitypolicy.
j. Analyzes application deficiencies and documents corrective actions taken.

2-4.2: Ensure that application access controls (e.g., unique user ID, password configuration, etc.) align with network access security policies established in sections 1-6.

2-4.3: Ensure that public access to applications is controlled by:

a. Restricting access to production systems and data.
b. Distinct security policy covering public access workstations that appropriately restricts access.

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

a. Identification and logging of security exceptions and violations.
b. Set up logging and other parameters to notify administrators of security violations as they occur.
c. Periodic review of exception reports and recommended corrective action by management and security administrators.

2-4.5: Ensure that physical access to application resources has been secured and addressed by security policies as outlined in sections 1-5.

Application Configuration Management

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

2-5.1: Establish controls over programming to ensure 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 an essential internal control that attempts to ensure that no single individual has the authority to execute two or more conflicting transactions.

2-6.1: Ensure management identifies and documents 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. See 1-6.2.

2-6.2: Small governments with limited staff and resources have a reduced capacity to segregate duties. Therefore, Compensating controls should be designed to reduce the risk of error or fraud not being detected. 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. Management periodically reviews user access authorizations for segregation of duties conflicts, considering the position and process changes and updating access to current job assignments.
c. Users with segregation of duties conflicts are documented, and their activity is monitored and reviewed periodically via transaction and audit logs.
d. Management retains documentation that the segregation of duties risk has been mitigated through effective compensating controls.
e. A segregation of duties grid is developed using the "roles and responsibilities" or security master report function within software applications.

Application Contingency Planning

2-7: Application contingency planning provides 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 vital 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 a backup retention policy for each application based on recovery time objectives. Ensure that backup intervals 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 sections 2-7.1. Incorporate the application-level contingency planning and procedures (including backup policy) into the organization's Disaster Recovery/Business Continuity Plan.

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

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 or digital signatures are used, management must understand the technology and associated risks. Develop and implement controls to address identified risks 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. On the other hand, electronic signatures 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. The access control mechanism should only be known by the check custodian and signatory.

3-1.5: Electronic signature disks or any other forms of electronic, digitized, or facsimile signatures should be in a secured location under the control of the signatory. Signature disks or other electronic, digitized, or facsimile signatures should only be used under the direct approval of the official (or deputy) whose signature is on the disk.

Payment Cards (Debit or Credit)

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

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

4-1.2: Develop and maintain written comprehensive policies and procedures that cover the process by which payment cards are accepted and payment card data are processed. Policies and procedures should include but are not limited to:

a. Segregation of duties.
b. Physical security.
c. Storage, transmission, and disposal of the payment card information.
d. Employee criminal background checks.
e. Technology security policies and procedures.
f. Incident response plan.

4-1.3: Adherence to industry standards includes credit card brands' compliance programs and 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, smartphones, 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 identified risks, and comply with applicable laws and regulations.

5-1.2: Ensure the 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 promptly after use any entity information stored on your device, including deleting copies of attachments to emails, such as documents, spreadsheets, and data sets.

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

5-1.7: Promptly report to entity management if your device is lost or stolen or its security is compromised.

5-1.8: Establish a comprehensive BYOD policy that provides standards and behavior rules for using personally owned devices. This policy must be adhered to access organizational resources.

Electronic Banking, Electronic Commerce, and other Electronic Transfer of Funds

6.1: Electronic banking and other electronic funds transfer (EFT) allow bank customers to perform account management and financial transactions over the Internet that directly or indirectly affect funds held by the bank. Despite security controls, there is no absolute way to guarantee the safety of online electronic transactions. Entities should comply with applicable laws and research and understand the risks involved before commencing online electronic transactions.

6-1.1: Develop comprehensive written 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, but not limited to:

a. Documentation of proper segregation of functions (i.e., the initiator cannot be an approver, etc.).
b. Online banking and EFT activities utilized.
c. Personnel who initiate, approve, transmit, record, review, or reconcile e-transactions.
d. Personnel who approve e-transactions.
e. Personnel who transmit e-transactions.
f. Personnel who record e-transactions.
g. Personnel who review and reconcile e-transactions.
h. Prompt removal or changes to access security for local and online access.
i. Properly maintain all documentation to support transactions for historical review and audit purposes.

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

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

6-1.4: Install firewalls and intrusion prevention systems with continuous monitoring. Any unauthorized and/or suspicious behavior, traffic, or unnecessary file types should be investigated and, if necessary, blocked using access control lists in conjunction with a firewall.

6-1.5: Ensure all employees with access to essential systems and services use multifactor authentication (MFA). This requirement includes access to web-based platforms, such as financial institutions, third-party applications, and webmail services. All administrative accounts, except service accounts, should use MFA.

6-1.6: Limit Internet access to only business-related programs. Frequently delete browsing history, temporary Internet files, and cookies. A hacker or malware program would capture minimal information if the system were compromised.

6-1.7: Ensure the session is secure before undertaking online banking.

6-1.8: Monitor and reconcile bank accounts daily (when feasible).

6-1.9: Periodically (daily, weekly, monthly) review accounts for unauthorized or suspicious activity and report immediately.

6-1.10: Ensure written agreements with banks and/or other payment solutions are reviewed by legal counsel. Ensure written agreements with banks provide appropriate controls for all electronic funds or wire transfers.

6-1.11: Ensure the 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).

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: Implement out-of-band transaction verification (such as text messages or other security messages to an approver with the entity). Take advantage of other system alerts, including:

a. Balance alerts.
b. Transfer alerts.
c. Password change alerts.
d. Login failure alerts.

6-1.15: Ensure that blank check stock, check reorder forms, canceled checks, check images, and signature stamps are properly safeguarded.

6-1.16: When paying electronically, use a clearing bank account rather than paying directly from the primary account.

6-1.17: Establish transaction and daily limits to lower loss potential.

6-1.18: Consider the cost-benefit of obtaining cybersecurity and data breach insurance. 6-1.21: 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 fraud controls, when possible and feasible, to ensure that the bank only processes authorized transactions. Features to consider include:

Implement fraud controls whenever possible and feasible to ensure that the bank only processes authorized transactions. Features to consider include:

a. Positive Pay.
b. Reverse Positive Pay.
c. ACH Positive Pay.
d. ACH Debit Block and Debit Filters.
e. Direct Deposit.

Instruct financial institutions to deny and return all nonconforming transactions as the default procedure.

6-1.21: If possible, implement a processing calendar with the bank to ensure the bank only processes transactions on pre-determined 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.

6-1.23: Allow electronic delivery of statements and account information. Ensure any statements or documents containing account information are properly maintained.

6-1.24: Limit access to sensitive information and never share confidential information, tax IDs, Social Security numbers, or account numbers via email.

6-1.25: Establish procedures to verify new or altered employee payroll direct deposit information. Changes should be verified directly with the employee.