

Guidelines for Arkansas Sheriffs

SHERIFF'S FINANCIAL RECORD KEEPING AND DISTRICT COURT ACCOUNTING LAW



Legislative Joint Auditing Committee
www.arklegaudit.gov
DIVISION OF LEGISLATIVE AUDIT
December 3, 2014



OUTLINE OF BASIC OFFICE PROCEDURES
AS REQUIRED BY ARKANSAS CODE

SELECTED LEGISLATIVE ACTS PERTAINING
TO THE SHERIFF'S OFFICE

Division of Legislative Audit
Supervisory Personnel for County Government Audits

www.arklegaudit.gov

Little Rock Office: June Barron, CPA, CFE..... 501-683-8600
Deputy Legislative Auditor

Tim Jones, CPA..... 501-683-8600
Audit Manager

Regional Supervisors:

Arkadelphia:	Marti Steel, CPA	501-683-8600 Ext. 1072
Greers Ferry:	Jerry McCarty, CPA, CFE, CFF	501-683-8600 Ext. 1052
Harrison:	Joe Stacey, CPA, CFE	501-683-8600 Ext. 1054
Jonesboro:	Kevin Baldrige, CPA, CFE	501-683-8600 Ext. 1060
Little Rock:	Tim Thompson, CPA, CFF	501-683-8600 Ext. 1031
Little Rock:	Jimmy Garrett, CPA, CFF	501-683-8600 Ext. 1030
Monticello:	Theresa Outlaw, CPA, CFE	501-683-8600 Ext. 4632
Ozark:	Albert Leding, CPA, CFE	501-683-8600 Ext. 1051
Ozark:	John Elser, CPA, CFE	501-683-8600 Ext. 1050

SHERIFF'S OFFICE BASIC FINANCIAL RECORDKEEPING PROCEDURES
IN ACCORDANCE WITH ARKANSAS CODE

	<u>Page</u>
INTRODUCTION	2
OUTLINE	3
EXAMPLES OF RECORDS	17
CERTAIN LEGISLATIVE ACTS	29
CASH ADVANCES FOR TRAVEL-RELATED EXPENSES	32
DEBIT CARDS TO CLOSE INMATE'S COMMISSARY TRUST ACCOUNT	33
INFORMATION SYSTEMS BEST PRACTICES	Appendix

Introduction

Concerning the finances of the Sheriff's Office, there can be no more important issue than proper internal controls.

Your first priority, as it concerns the financial business of the Sheriff's Office, is to create an environment that makes it as difficult as possible for any single person to take advantage of the accounting system and thereby perpetrate fraud. That is what internal control is all about. You cannot base your accounting system on an evaluation of your bookkeeper's integrity.

A pillar of good internal control is proper segregation of duties. Areas to address when segregating duties include, but are not limited to, the following:

- Receipting.
- Preparing and making the deposit.
- Reconciling.
- Approving the reconciliation.
- Posting the journals.
- Signing and co-signing disbursements.
- Initiating purchases.
- Receiving goods.
- Assigning custody of investments.
- Maintaining capital asset records.

Avoid situations in which only one person has access to **ALL** accounting and financial duties.

Once you have established an environment of proper accounting controls, the next step is to be vigilant in maintaining them. Without complete and accurate financial records and inventory controls, the function of your office will not be complete.

Your primary focus may be in areas other than financial, but as Sheriff, you remain responsible and accountable for the financial activities of your office. Hopefully, this manual will provide guidance for maintaining your accounting records.

Outline

- I. **Basic Accounting Procedures (Ark. Code Ann. §§ 14-25-102 – 14-25-109, 14-25-112, 16-10-201 – 16-10-211)**
 - A. If the Sheriff collects bonds and fines for District Court, a bank account to be used exclusively for these bonds and fines is required.
 - B. At least two more bank accounts should be maintained.
 - 1. Fees - To account for fees collected that, in turn, are remitted to the County Treasurer.
 - 2. Other - To handle foreign bonds and miscellaneous business.
 - C. A separate cash receipt and disbursement journal is to be maintained for each bank account (see example at Exhibit 1).
 - D. A bank reconciliation is to be prepared monthly for each bank account (see example at Exhibit 2).
 - E. The Bond and Fine Account will probably have a balance of cash at the end of each month. For this account to be reconciled, the balance must be identified to receipts issued but not yet remitted to the District Court Clerk.
 - F. Receipts (Ark. Code Ann. §§ 14-25-108, 16-10-207)
 - 1. Receipts must be prenumbered and should be personalized with, at minimum, the name of the county.
 - 2. A printer's certificate is to be retained to verify the range of receipts purchased.
 - 3. A different set of receipts is to be maintained for each bank account.
 - 4. Receipts for bonds and fines are issued in the name of the violator and upon collection of monies. Receipts should also indicate the name of the person paying the bond if someone other than the violator tenders payment.
 - 5. Receipts are to indicate the method of payment used: cash, check, money order, or credit card.
 - 6. Receipt numbers are to be written on the face of checks received.
 - 7. Voided receipts should be clearly marked as VOID, and all copies of voided receipts should remain attached in the receipt book.

I. Basic Accounting Procedures (Ark. Code Ann. §§ 14-25-102 – 14-25-109, 14-25-112, 16-10-201 – 16-10-211) (continued)

F. Receipts (Ark. Code Ann. §§ 14-25-108, 16-10-207) (continued)

8. If an electronic receipting system is used, the system must be in compliance with the Information Systems Best Practices Checklist provided by the Legislative Joint Auditing Committee.

G. Deposits (Ark. Code Ann. §§ 14-25-103, 16-10-207)

1. All deposits are to be made intact (i.e., in the same form and manner as received upon collection). In the case of the Bond and Fine Account, deposits should be made daily. Check cashing for accommodation purposes should not be allowed.
2. Deposit slips are to indicate the range of receipts issued being deposited.

H. Disbursements (Ark. Code Ann. §§ 14-25-104, 16-10-204)

1. Prenumbered checks are required.
2. Dual signatures (the Sheriff's and one other authorized signature) are required for disbursements from the Bond and Fine Account.
3. Voided and spoiled checks are to be retained and clearly marked "VOID."

II. Arkansas District Courts Accounting Law (Ark. Code Ann. §§ 16-10-201 – 16-10-211)

A. All of the above requirements concerning bank accounts are to be met.

B. An overview of District Courts Accounting Law requirements

1. Uniform traffic citations issued for violations of all municipal and state laws
 - a. The law requires an original and three copies:
Hard Copy - Violator
White Copy - Office
Yellow Copy - District Court Clerk
Pink Copy - Remains in Citation Book
 - b. Citations are to be prenumbered and a printer's certificate retained.
 - c. All copies of voided or spoiled citations are to be attached to the hard copy and remain in the citation book.

II. Arkansas District Courts Accounting Law (Ark. Code Ann. §§ 16-10-201 – 16-10-211) (continued)

B. An overview of District Courts Accounting Law requirements (continued)

1. Uniform traffic citations issued for violations of all municipal and state laws (continued)
 - d. Sheriff's Office copy of a citation is to be filed alphabetically or numerically.
 - e. A citation book log is to be maintained. Officers should sign out individual citation books in numerical sequence and sign in the books upon completion of all citations therein. The citation log should list all citations in stock by book and number range within that book (see example at Exhibit 3).
 - f. Completed citation books are to be filed immediately with the District Court Clerk.
 - g. Electronic citation systems must be in compliance with the Information Systems Best Practices Checklist provided by the Legislative Joint Auditing Committee.
2. The Sheriff's Office is responsible for issued citations that will be processed through the County Division of District Court.
3. Citations are accumulated in the Sheriff's Office by court date.
 - a. These citations are issued by Sheriff's deputies, by State Troopers outside of any incorporated area of the county, and possibly by other law enforcement agencies such as Game and Fish, Highway Police, etc.
 - b. It is very important to establish a deadline to turn in issued citations to the Sheriff's Office.
4. Accumulated citations are entered on an arrest report (see example at Exhibit 4).
5. At least 7 business days before the court date, the appropriate arrest report should be totaled and a check made out to the District Court Clerk for the amount of that particular arrest report only. A copy of the arrest report, accompanied by payment, should be delivered to the District Court Clerk.

II. **Arkansas District Courts Accounting Law (Ark. Code Ann. §§ 16-10-201 – 16-10-211)** (continued)

B. An overview of District Courts Accounting Law requirements (continued)

6. Installment payments may be authorized only by the presiding judge.

- a. If so designated by Ark. Code Ann. § 16-13-709, installment payments are collected by the Sheriff's Office and remitted to the Court Clerk as collected. They are to be added to the arrest report for the week's court in which they are collected.
- b. If the Sheriff's Office collects installment payments, installment payment ledger cards are to be maintained. These cards are actually duplicates of the Court Clerk's records. Installment payment records maintained by the Court Clerk and the Sheriff's Office should be reconciled monthly (see example at Exhibit 5).
- c. In addition to the fine and any other assessments, an installment fee of \$5.00 per month shall be assessed on each person who is authorized to pay a fine on an installment basis, per Ark. Code Ann. § 16-13-704.

C. Computer Software

1. You may choose to purchase a commercially-available software package to assist in maintaining your bond and fine records. However, please be aware that all systems do not comply with the requirements of District Courts Accounting Law. Do not rely on the representations of the salesperson. Ensuring compliance remains **YOUR** responsibility.

Updates of an existing software system or a replacement of an existing one should also be evaluated for compliance.

2. If a computer system is utilized for bookkeeping purposes, it is recommended that the attached Arkansas Division of Legislative Audit – Information Systems Best Practice Checklist be reviewed.

D. All District Court Accounting laws apply unless your District Court has been granted an exemption by the Legislative Joint Auditing Committee. Details of such an exemption can be provided by your District Court Clerk or by contacting the Division of Legislative Audit.

III. Drug Enforcement Funds - (Ark. Code Ann. §§ 14-21-201 – 14-21-204)

- A. A Drug Enforcement Fund may only be established by Quorum Court ordinance. The fund is subject to audit by the Division of Legislative Audit, and accounting records are to be maintained in the manner established by the Division.
- B. The maximum amount allowed in the fund is \$50,000.
- C. The source of all funds deposited in this account shall be appropriated by the Quorum Court. No other funds from other sources, including seized property, shall be deposited into the fund.
- D. Funds are to be kept in a separate bank account and administered by the County Sheriff.
 - 1. Revenues are to be receipted on prenumbered receipts in the same manner as any other account.
 - 2. Disbursements are to be made by prenumbered check in the same manner as any other account.
 - 3. A cash receipts and disbursements journal is to be maintained in the same manner as any other account.
- E. Very specific restrictions for the use of these funds are provided in Ark. Code Ann. § 14-21-202.
- F. Drug enforcement funds may be distributed to a designated officer in charge of the funds and/or an undercover officer.
 - 1. For funds disbursed to a designated officer in charge of the funds, a “Cash on Hand Report” should be maintained. Prenumbered checks drawn to the custodian of the fund and cashed for subsequent disbursement to an undercover officer would be entered as debits on this report. Cash remitted to the undercover officer would be entered as a credit on this report. The balance on this report would be the amount of cash on hand with the fund custodian at any given time (see example at Exhibit 6).
 - 2. For funds disbursed to an undercover officer, either by the cash fund custodian, as in F.1. above, or by check from the Drug Enforcement bank account, an undercover officer log book is to be maintained. The undercover officer should file a monthly Undercover Officer's Report with the Sheriff. The monthly report would be a recap of the officer's log book. When possible, invoices should be attached to the report to document disbursements, (see example at Exhibit 7).

III. Drug Enforcement Funds (Ark. Code Ann. §§ 14-21-201 – 14-21-204)
(continued)

- F. Drug enforcement funds may be distributed to a designated officer in charge of the fund and/or an undercover officer (continued)
3. The County Sheriff or the designated officer in charge of the Drug Enforcement Fund should maintain a Transaction Card on each undercover officer, regardless of the manner in which the undercover officer receives drug enforcement funds. The Transaction Card should contain the officer's name, transaction date, transaction description, transaction amount, and balance. The Transaction Card balance should be reconciled to the Undercover Officer Report balance monthly (see example at Exhibit 8).
 4. Undercover Officer Reports should be filed by the undercover officer's name. As an alternative, the undercover officer may be assigned a unique number or name and the report filed accordingly. The cross indexing of code names and/or numbers to actual officers' names could be maintained in a secure location, separate from other accounting records. Records could also be similarly maintained for informants.
 5. If feasible, a receipt should be obtained from an informant by the undercover officer when funds are paid to an informant (see example at Exhibit 9).
- G. A note concerning Drug Enforcement Funds

The Division of Legislative Audit has no desire to become part of the evidence chain in any criminal case or to compromise the safety of any law enforcement officer or confidential informant. However, as established by Arkansas Code, the Division has a responsibility to audit Drug Enforcement Funds, and Sheriffs have a fiduciary responsibility to citizens to properly account for a government's funds. Although this can be a difficult line to walk, a little planning, common sense, and reason will go a long way in helping both the Division and you, the County Sheriff, accomplish proper accounting of Drug Enforcement Funds. The last thing the Division wants to do is disrupt your ability to enforce the law and remove a criminal from mainstream society. We must, however, do our job, just as you must do yours, and our job is to audit.

IV. Communications Facility and Equipment Fund (Ark. Code Ann. §§ 21-6-307, 12-41-105)

- A. Ark. Code Ann. § 21-6-307
1. 75% of fees collected are to be deposited to County General Fund.
 2. 25% of fees collected are to be deposited to Communications Facility and Equipment Fund. (Fees are not permissible for finger printing services provided by the Sheriff's Office.)

IV. Communications Facility and Equipment Fund (Ark. Code Ann. §§ 21-6-307, 12-41-105) (continued)

A. Ark. Code Ann. § 21-6-307 (continued)

3. Fund may be maintained by Sheriff and/or County Treasurer. If maintained by the Sheriff, the funds shall be invested in an interest-bearing account or CD.
4. If maintained by the Sheriff, all requirements discussed for general record keeping would apply.
5. If maintained by the County Treasurer, normal expenditure controls would apply (expenditures by claim per county appropriation).
6. Ark. Code Ann. § 21-6-307(b)(2)(C) lists allowable uses of the Communications Facility and Equipment Fund.

B. Ark. Code Ann. § 12-41-105

1. Commissions from prisoner telephone services are to be deposited to the County Treasury and then remitted to the Communications Facility and Equipment Fund.
2. 50% of commissions may be allocated for maintenance and operation of the jail.

V. Minimum Accounting Procedures Relating to the Service of Process

A. Service of Process Ledger to be maintained by the Sheriff

The Sheriff of each County should establish, maintain, and duly record each process delivered to the Sheriff for service on a Service of Process Ledger. The Service of Process Ledger should contain, at minimum, the following information under separate columnar headings for all processes to be served by the Sheriff or other authorized employees of the Sheriff's Office (see example at Exhibit 10):

1. Date process received.
2. Case number.
3. Style of case.
4. Person to be served.
5. Issuing county.

V. Minimum Accounting Procedures Relating to the Service of Process
(continued)

A. Service of Process Ledger to be maintained by the Sheriff (continued)

6. Type of process (summons, subpoena, type of writ, etc.).
7. Party requesting service.
8. Service fee.
9. Date served.
10. Receipt number or notation of posting to accounts receivable ledger or notation of no charge for service.

The use of mechanical devices, which provide the same information as the Service of Process Ledger, is acceptable and encouraged where such equipment is utilized.

B. Prenumbered Receipts

All items received by the Sheriff relating to service of process are to be formally receipted using the prenumbered receipts or mechanical receipting devices currently in use for the various fees of the Sheriff's Office.

C. Deposit of Funds

All funds received should be promptly deposited in the respective official's fee account and paid to the County Treasurer in the manner provided by law. All deposits should be cross-referenced to the receipt numbers.

D. Credit Business (Ark. Code Ann. § 21-7-209)

1. Extending credit for fees is generally prohibited. However, Sheriffs are specifically allowed, under certain conditions, to extend credit for the payment of court costs and fees to licensed attorneys, financial institutions, improvement districts, and state and federal agencies.
2. The official should prepare and mail to each credit customer monthly, or no less than quarterly, a statement detailing the business activity for the month. This statement should be a prenumbered, two-part form. One copy should be sent to the customer and the remaining copy retained by the official and filed numerically by month. The statement should include a specific reference to the service performed on account by the official/department and the charge for each service, with the total due on account also being reflected.

V. Minimum Accounting Procedures Relating to the Service of Process
(continued)

E. Accounts Receivable Ledger

An accounts receivable ledger for each credit customer should be maintained with the following columnar headings, at minimum (see example at Exhibit 11):

1. Date of service, return, receipt, or billing.
2. Style of case/receipt number.
3. Amount of fee.
4. Amount of payment.
5. Balance of account.

The receipts issued for payments of accounts should reflect the statement number from which the payment was received. The accounts receivable ledger should be posted from the Service and Process Ledger timely.

VI. Commissary Fund

- A. A Commissary Fund may be established by ordinance on the County Treasurer's books and a Sheriff's commissary bank account opened.
- B. Claims will be filed on the Treasurer's Commissary Fund for all expenditures/disbursements of the Commissary Fund, except for refunds of inmate monies. The Commissary Fund shall be appropriated by the Quorum Court.
- C. All funds collected from inmates are to be deposited daily in the Sheriff's Commissary Fund bank account.
- D. All proceeds from Commissary Fund sales shall be remitted to the County Treasurer to be deposited in the Treasurer's Commissary Fund monthly.
- E. An alternative method would be to allow a private organization to operate the Commissary Fund, with approval of the Quorum Court.
- F. Debit cards can be issued to close an inmate's commissary trust account.

VII. General Information

- A. Monthly settlements made with the County Treasurer are required by the 10th working day of the subsequent month (Ark. Code Ann. § 26-39-201).
- B. Fixed assets should be periodically observed and a detailed record maintained that lists, at minimum, a brief description, serial number, location of property, date of acquisition, cost and property item number (if a property item number system is used by the County) (Ark. Code Ann. §14-25-106).
- C. The Quorum Court may designate one county official to maintain the entire County's fixed asset records; however, the Sheriff is still required to notify this designated official at the time of all additions and deletions. The Quorum Court shall adopt a policy setting a dollar figure requirement for equipment to be included on the fixed asset listing; however, this does not prevent items of a sensitive nature, such as weapons, from being included on the listing (Ark. Code Ann. § 14-25-106).
- D. All voided documents (receipts, checks, citations, etc.) should remain intact, with all copies remaining in the respective book.
- E. Insufficient checks, bank errors, and other bank charges.
 - 1. Require the bank to charge all returns against the bank balance.
 - 2. Make redeposits on separate deposit slips.
 - 3. If an item is considered uncollectible, retain the returned check in your files.
 - 4. Upon receiving notice of a hot check, void the receipt written. If the individual makes his/her check good, issue another receipt.
- F. Bank Imaging

A financial institution serving as a depository of public funds and wishing to provide only imaged documents is required by Ark. Code Ann. §§ 19-2-501 – 19-2-507, 19-2-509 to meet certain requirements. One requirement is that the method chosen be approved by the Division of Legislative Audit.

If your financial institution is not providing all original cancelled checks, you should obtain from that institution a copy of the Division's letter of authorization of an alternative method.

VII. General Information (continued)

G. Controlled Substance Act (Seized and Forfeited Property - Ark. Code Ann. § 5-64-505)

1. Inventory of property seized - referred to Prosecuting Attorney

a. Confiscation report containing the following information should be prepared and filed within 48 hours:

- (1) A detailed description of the property seized, including any serial or model numbers.
- (2) Date of seizure.
- (3) Name and address of the person from whom the property was seized.
- (4) Reason for the seizure.
- (5) Location where the property will be held.
- (6) Seizing officer's name.
- (7) A signed statement by the seizing officer stating that the report is true and complete.

b. Within three business days, file a copy with:

- (1) Prosecuting Attorney.
- (2) Arkansas Drug Director.

c. Inventory list of seized property

A detailed listing of all seized property should be maintained to include the following (see example at Exhibit 12):

- (1) Date of seizure.
- (2) Description of property.
- (3) Serial number.
- (4) Estimated value.
- (5) Location.
- (6) Disposition.

VII. General Information (continued)

G. Controlled Substance Act (Seized and forfeited property - Ark. Code Ann. § 5-64-505) (continued)

2. Property forfeited

a. By Circuit Court order

(1) The property may be retained for official use by the law enforcement agency or the Prosecuting Attorney, except for aircraft, which must be turned over to the State Drug Director. See Ark. Code Ann. § 5-64-505 for applicable time restrictions.

(2) The property may be sold.

Proceeds of the sale and/or monies forfeited are to be deposited in the Special Asset Forfeiture Fund of the Prosecuting Attorney and distributed in the following order:

a) Satisfy any security interest or lien.

b) Pay any expenses of the sale.

c) Balance of money under \$250,000 distributed to the appropriate local and/or state law enforcement agency and/or the prosecutorial agency in a ratio proportionate to the participation in the activity that resulted in the forfeiture.

d) Balance of money over \$250,000 to the State Drug Director to be transferred to the State Treasury.

3. A Drug Control Fund is created on the books of the law enforcement agencies and the Prosecuting Attorneys. This fund is subject to audit by the Division of Legislative Audit.

4. The Drug Control Fund of the Sheriff is maintained by the County Treasurer.

5. Twice a year, a report is due to the State Drug Director detailing all monies received and expenditures made from the Drug Control Fund.

H. Sheriff's Office may collect Circuit Court fines, if so designated by the Quorum Court (Ark. Code Ann. § 16-13-709).

VII. General Information (continued)

- I. The basic rule is that all funds coming into the hands of a public official are to be remitted to the County Treasurer (Ark. Code Ann. §§ 14-25-103, 14-14-1313).
- J. Court costs are governed by Ark. Code Ann. § 16-10-305. Generally, no costs may be assessed other than those authorized by Ark. Code Ann. § 16-10-305.
- K. Contracts and Soliciting Bids

The County Court is required to approve by County Court order all bids and contracts entered into on behalf of the County. Bids are required to be solicited on all purchases in excess of \$20,000 by Ark. Code Ann. §§ 14-22-101 – 14-22-115.

- L. Credit Card Payments

Payment of fines may be accepted by an approved credit or debit card, pursuant to Ark. Code Ann. § 16-13-706. When the offender pays fines by credit card or debit card, the court may assess the offender a transaction fee. The Quorum Court may establish a transaction fee to be charged for the collection of fines assessed in a Circuit Court for any electronic payment of a fine by an approved credit or debit card. Each governing body that contributes to the expenses of a District Court may establish the transaction fee for District Court fines (Ark. Code Ann. § 16-92-118).

- M. Unclaimed Property

Ark. Code Ann. § 18-28-201 and www.auditor.ar.gov should be referenced for guidance in handling unclaimed property. Unclaimed property would include, but not be limited to, seized items and stale-dated outstanding checks.

- N. Uniform Allowances

A policy regarding uniform allowances should be approved by the Quorum Court. In some cases, uniforms could be considered taxable income (e.g., if apparel is suitable for street wear). The Internal Revenue Service recommends reviewing the following:

- Fringe Benefit Guide – Office of Federal, State and Local Governments located at www.irs.gov/Government-Entities/Federal.
- State & Local Governments and Fringe Benefit Guide, Publication 5137 at www.irs.gov/pub/irs-pdf/p5137.pdf.

VII. General Information (continued)

N. Uniform Allowances (continued)

Additional guidance can be obtained by contacting:

Internal Revenue Service
Jan Germany
FSLG Specialist
700 W. Capitol Ave. MS: 4210
Little Rock, Arkansas 72201
(501) 396-5816
Jan.F.Germany@irs.gov.

COUNTY SHERIFF'S OFFICE
CASH RECEIPTS JOURNAL

<u>Date</u>	<u>Receipt Number</u>	<u>Issued To</u>	<u>Total</u>	<u>Service Fees</u>	<u>Commissioner's Sale</u>	<u>Other</u>	<u>Other Descriptions</u>
01-03-14	001	A & A Attorneys	\$ 50.00	\$ 50.00			
01-05-14	002	District Court Clerk	80.00	80.00			
01-07-14	003	John Smith	50.00	50.00			
01-12-14	004	B & B Attorneys	100.00	100.00			
01-22-14	005	Void					
01-31-14	006	Jane Smith	50.00	50.00			
01-31-14	007	Jimmy Smith	50.00	50.00			
01-31-14	008	District Court Clerk	50.00	50.00			
01-31-14	009	John Q. Public	5,000.00	500.00	\$ 4,500.00		
	Monthly Totals		<u>5,430.00</u>	<u>\$ 930.00</u>	<u>\$ 4,500.00</u>		
	Year-to-date Totals		<u>\$ 5,430.00</u>	<u>\$ 930.00</u>	<u>\$ 4,500.00</u>		

COUNTY SHERIFF'S OFFICE
CASH DISBURSEMENTS JOURNAL

<u>Date</u>	<u>Check Number</u>	<u>Issued To</u>	<u>Total</u>	<u>County Treasurer</u>	<u>Comm. Fac. & Equip. Fd.</u>	<u>Other</u>	<u>Other Descriptions</u>
01-31-14	101	County Treasurer	\$ 697.50	\$ 697.50			
01-31-14	102	Comm. Fac. And Equip. Fd.	232.50		\$ 232.50		
01-31-14	103	Mary Jones	4,500.00			\$ 4,500.00	Commissioner's sale
	Monthly Totals		<u>5,430.00</u>	<u>697.50</u>	<u>232.50</u>	<u>4,500.00</u>	
	Year-to-date Totals		<u>5,430.00</u>	<u>697.50</u>	<u>232.50</u>	<u>4,500.00</u>	

NOTE: This is a sample cash receipts and disbursements journal for a fee account. For each type of account maintained, this would be the proper format. Of course, columnar headings would change to reflect types of revenues collected and types of disbursements. Monthly and year-to-date totals are required.

_____ COUNTY SHERIFF'S OFFICE
MONTHLY BANK RECONCILIATION

Exhibit 2

Bank Balance Per Bank Statement January 31, 2014	\$	430.00
Additions:		
Deposits in transit		
Deductions:		
Outstanding check #101		<u>(430.00)</u>
Adjusted Bank Balance	\$	<u>.00</u>
Balance Per Cash Receipts and Disbursements Journal	\$	<u>.00</u>

APPROVED BY: _____

COUNTY SHERIFF'S OFFICE
ARREST REPORT
COURT DATE FEBRUARY 4, 2014

Exhibit 4

Uniform Traffic Citation Number	Violator's Name	Offense	Officer	Receipt Number	Fines and Costs	Other
A 1000	Jones, Robert	Speeding	Smith	101	\$ 49.50	
A 1001	Stewart, John	Speeding	Smith	121	49.50	
A 1053	Jackson, Thomas	DOH	Jones	116	115.50	
A 1076	Starr, Bart	No DL	Watson			
A 2001	Meredith, Don	Speeding	Meeks	105	<u>49.50</u>	
					<u>\$ 264.00</u>	

COUNTY SHERIFF'S CASH ON HAND REPORT

Exhibit 6

County Sheriff Name (Dayrider) - Maintained by County Sheriff

<u>Date</u>	<u>Transaction</u>	<u>Debit</u>	<u>Credit</u>	<u>Balance</u>
08/01/14	Check # _____	\$ 1,000.00		\$ 1,000.00
08/01/14	Given to (Name of officer - Nightrider)		\$ 500.00	500.00
08/15/14	Check # _____	500.00		1,000.00
08/15/14	Given to (Name of officer - Nightrider)		600.00	400.00

NOTE: This report is to be used ONLY to account for "cash" activities.

UNDERCOVER OFFICER'S TRANSACTION CARD

Exhibit 8

Nightrider/# - Maintained by County Sheriff/Person in Charge of Fund

<u>Date</u>	<u>Transaction</u>	<u>Debit</u>	<u>Credit</u>	<u>Balance</u>
08-01-14	Advance to officer	\$ 500.00		\$ 500.00
08-15-14	Advance to officer	600.00		1,100.00
08-31-14	Report submitted		\$ 58.00	1,042.00

RECEIPT

For, and in consideration of, the sale and delivery of the Prosecuting Attorney information and/or evidence identified as follows:

Purchase of Cocaine
Purchase of Marijuana

I hereby acknowledge receipt of \$ 200.00 paid to me by the County Sheriff.

Date: 8-21-10 Signature: John Doe

Witnessed by:

m. Nightinder

Debit slip kept in investigator's file

SERVICE OF PROCESS LEDGER

 COUNTY SHERIFF'S OFFICE

Exhibit 10

<u>Date Process Received</u>	<u>Case Number</u>	<u>Style of Case</u>	<u>Person to be Served</u>	<u>Issuing County</u>	<u>Type of Process</u>	<u>Party Requesting Service</u>	<u>Service Fee</u>	<u>Date Served</u>	<u>Receipt Number</u>
06-15-14	CIV-12-100	Robb vs. Heard	Heard	Pulaski	Summons	Perry Mason	\$ 50.00	06-26-14	A/R
06-19-14	CIV-12-101	McGee vs. McGee	McGee	Pulaski	Summons	Perry Mason	50.00	06-27-14	A/R
06-20-14	CIV-12-102	Cook vs. Watson	Watson	Pulaski	Summons	Arnie Becker	50.00	06-27-14	102
06-21-14	CR-12-013	State vs. Spratt	Spratt	Pulaski	Subpoena	Hamilton Berger	50.00	06-28-14	N/C
06-29-14	CIV-12-104	Cook vs. Cook	Cook	Pulaski	Summons	Perry Mason	50.00	06-29-14	A/R

ACCOUNTS RECEIVABLE LEDGER

Exhibit 11

NAME: Perry Mason
ADDRESS: #1 Mason Centre
 Los Angeles, CA 11111
PHONE NUMBER: 1-800-DEF-ENSE

<u>Date</u>	<u>Style of Case/Receipt Number</u>	<u>Amount of Fee</u>	<u>Payment Amount</u>	<u>Balance</u>
06-26-14	CIV-12-100	\$ 50.00		\$ 50.00
06-27-14	CIV-12-101	50.00		100.00
06-28-14	Billing Statement No. 001			
06-29-14	CIV-12-104	50.00		150.00
07-01-14	Receipt No. 105		\$ 50.00	100.00

_____ COUNTY SHERIFF'S OFFICE

SEIZED AND FORFEITED PROPERTY INVENTORY LIST

<u>Date of Seizure</u>	<u>Description of Property</u>	<u>Serial Number</u>	<u>Estimated Value</u>	<u>Location</u>	<u>Disposition</u>
------------------------	--------------------------------	----------------------	------------------------	-----------------	--------------------

**CERTAIN ARKANSAS CODES RELATING TO THE FINANCIAL RECORDS
OF THE
SHERIFF'S OFFICE**

The following Arkansas Codes have not been reproduced for inclusion in this booklet. The list should not be considered comprehensive but should be used in conjunction with the Arkansas Code of 1987 Annotated. Copies of the applicable Arkansas Code may be accessed at the following web-address:

<http://www.lexisnexis.com/hottopics/arcodes/Default.asp>

Selected Arkansas Codes:

Ark. Code Ann. § 5-64-505

Property subject to forfeiture – procedure – disposition of property (Uniform Controlled Substances)

Ark. Code Ann. § 12-15-301

Sale of county-issued firearms to deputies

Ark. Code Ann. § 12-41-105

Commissions from prisoner telephone services

Ark. Code Ann. § 12-41-505

County jails – prisoner expenses and support – booking and administration fee

Ark. Code Ann. §§ 13-4-401 — 13-4-411 (Also see Ark. Code Ann. § 16-10-211)

Sheriff's office records retention schedule

Ark. Code Ann. § 14-14-113

Review of audit report by quorum court

Ark. Code Ann. § 14-14-1202

Ethics for county government officers and employees

Ark. Code Ann. § 14-14-1203

Compensation and expense reimbursements generally (including travel expense reimbursement)

Ark. Code Ann. § 14-14-1207

Reimbursement of allowable expenses

Ark. Code Ann. § 14-14-1209

Uniform and equipment allowance for sheriff's department

Ark. Code Ann. § 14-14-1313

Remittance of public funds

Ark. Code Ann. §§ 14-21-201 — 14-21-204

Drug Enforcement Fund (Establishment, restrictions on use, approval of claims, accounting records)

Ark. Code Ann. §§ 14-22-101 — 14-22-115

County purchasing procedures (including bidding process; purchases in excess of \$20,000, unless exempt, should be bid)

Ark. Code Ann. §§ 14-25-101 — 14-25-108, 14-25-112

County Accounting Law (bank accounts, deposit of funds, prenumbered checks, petty cash funds, fixed asset records, reconciliation of bank accounts, prenumbered receipts, Sheriff's accounts)

Ark. Code Ann. §§ 16-10-201 — 16-10-211

Arkansas District Courts Accounting Law (includes sections relating to bond and fine accounts; uniform traffic citations (including electronic traffic citations); arrest reports; collection, receipt and deposit procedures; records retention)

Ark. Code Ann. § 16-10-305

Court costs

Ark. Code Ann. §§ 16-13-703 – 16-13-704

Court fines – installment payments

Ark. Code Ann. § 16-13-706

Credit/debit card payment of fines

Ark. Code Ann. § 16-13-709 (also see Ark. Code Ann. § 16-92-118)

Designation of responsibility for collection of fines

Ark. Code Ann. § 16-13-712

Judicial Fine Collection Enhancement Fund

Ark. Code Ann. § 16-90-119

Confiscation of deadly weapons (confiscation and disposition)

Ark. Code Ann. § 16-92-118

Electronic collection and deposit of fines

Ark. Code Ann. §§ 18-28-201, 18-28-207 - 18-28-208

Unclaimed property

Ark. Code Ann. §§ 19-2-501 — 19-2-507, 19-2-509

Requirements for photographic copies or digital images of financial transactions (bank statements, cancelled checks, etc.)

Ark. Code Ann. § 21-6-307

Fee schedule for Sheriffs; Communications Facility and Equipment Fund

Ark. Code Ann. § 21-7-209

Extending credit for court costs and fees prohibited except for licensed attorneys, financial institutions, improvement districts, state and federal agencies, and recording fees of the Commissioner of State Lands

Ark. Code Ann. § 26-39-201

Monthly settlements with the county treasurer to be on the first of each month, or within ten (10) working days thereafter

Ark. Code Ann. § 27-53-210

Fee allowed for each copy of a basic accident report

CASH ADVANCES FOR TRAVEL-RELATED EXPENSES

The Legislative Joint Auditing Committee, at its September 9, 2011 meeting, adopted the rules below in accordance with Act 614 of 2011 which amended ACA 14-14-1203 concerning cash advances for travel-related expenses for county employees.

Each Quorum Court may by ordinance establish a travel advance fund(s). The ordinance shall set a maximum amount for the fund(s) and shall designate the custodian of each fund. The travel advance fund(s) may be maintained by the custodian(s) as a cash fund or in a bank account. The source of the funds for the travel advance fund shall be funds appropriated by the quorum court. The initial funding and any subsequent reimbursements to the fund shall be appropriated by the quorum court and subject to the disbursement procedures required by law.

After a quorum court has approved a proper ordinance establishing a travel advance fund, set the maximum amount for the fund, designated the custodian of the fund, and appropriated funds for the fund, the county judge may approve a county claim for the initial establishment of the travel advance fund. If adequate appropriations and funds are available, the travel advance fund may be replenished upon presentation and approval of a claim which will include supporting documentation as provided in the county disbursement procedures. The total amount of funds held in the travel advance fund shall not exceed the maximum amount established by the quorum court.

Accounting records shall be maintained by the custodian for the receipt, disbursement, accounting, documentation, and reconciling of funds.

The travel advance funds shall only be used to make advances of expenses associated with authorized travel by employees of the county. Upon completion of the travel, the employee shall provide documentation of the expenses associated with the travel advance to the custodian of the fund. If documentation is not provided, or if the travel advance exceeds the actual expenses incurred, the employee must repay the balance to the travel advance fund within 7 calendar days of the trip return. The county shall withhold any undocumented or excess advance not repaid within 7 calendar days of trip return from the employee's next paycheck.

Travel expenses paid from the travel advance fund shall be in accordance with the county's travel policy. Meals for travel without overnight stay must be included on employee's W-2 form.

DEBIT CARDS TO CLOSE INMATE'S COMMISSARY TRUST ACCOUNT

The Legislative Joint Auditing Committee, at its September 13, 2013 meeting, adopted the procedures below in accordance with Act 1158 of 2013 which amended ACA 14-25-112 for Sheriffs to issue debit cards to clear inmate's commissary accounts.

Establish a written policy for the use of debit cards to close an inmate's commissary trust account.

The amount on the debit card shall be the balance in the inmate's account.

Debit cards shall be prenumbered and identifiable with the inmate's account.

The inmate shall sign a form when receiving a debit card. The form shall contain the inmate name, date, amount of debit card, debit card number, and signature of inmate. The form is to be retained by the Sheriff's office and available for audit. If possible, the inmate should change the PIN upon release.

The Sheriff's Commissary bank account shall not be debited by any outside vendor without prior documented approval from the Sheriff's office.

Debit cards shall be recorded in the cash disbursements journal or ledger for the commissary fund.

The computer software application to be used in the issuing of debit cards shall be in compliance with the Information Systems Best Practices Checklist provided by the Legislative Joint Auditing Committee.



Arkansas Division of Legislative Audit Information Systems Best Practices

January 2012



TABLE OF CONTENTS

	Page
Purpose	3
Introduction	3
Best Practices - General Controls Section	4
IS Management.....	4
Contract/Vendor Management	6
Network Security	7
Wireless Networking Security.....	8
Physical Access Security.....	9
Logical Access Security	10
Disaster Recovery/Business Continuity	12
Best Practices - Application Controls Section	13
Data Input	13
Data Processing	15
Data Output	16
Application Level General Controls Section	17
Application Security Management	17
Application Configuration Management	19
Segregation of Duties	20
Application Contingency Planning.....	20

PURPOSE

The Division of Legislative Audit establishes the following best practices employed throughout industry and government to encourage government entities to develop, implement, and maintain information systems policies 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. While this document is intended to establish minimum levels of compliance for auditing purposes, it is not all-inclusive, and the following should be noted:

Because information technology is a rapidly changing environment, 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 information technology 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 Information Systems environment. All information systems controls throughout the industry may be broadly categorized as such, and are presented accordingly 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)	see note above
Contract/Vendor Management	(Best Practices 1-2)	
Network Security	(Best Practices 1-3)	
Wireless Networking Security	(Best Practices 1-4)	
Physical Access Security	(Section 1-5)	
Logical Access Security	(Section 1-6)	
Disaster Recovery/Business Continuity	(Section 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 such application. Application controls are designed to ensure the completeness and accuracy of the accounting records and the validity of the entries made. In general, Application Controls contain the following components:

Data Input	(Section 2-1)	see note above
Data Processing	(Section 2-2)	
Data Output	(Section 2-3)	
Application Level General Controls	(Sections 2-4 through 2-7)	





1-1: IS Management

- 1-1.1: Develop an Information Systems Department Organizational Chart and update as the environment changes.
- 1-1.2: Conduct an overall risk assessment to identify risks associated with the use of information technology. Gain an understanding of current practice in addressing these risks and mitigating negative impacts.
- 1-1.3: Develop and maintain a formally approved Information Systems Operational Policy and Procedure Manual. The manual can be one document or several documents but should be reviewed and changed as the operating environment changes.
- 1-1.4: Ensure that duties of developers and 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 network backup processes, including data and applications.
- 1-1.8: Assign and communicate network backup responsibilities to designated staff.
- 1-1.9: Establish access to a secure off-site location to retain network backups.
- 1-1.10: Establish and formally document frequency of backups, ensuring that minimum industry standards (daily-weekly-monthly-annually) are met Backups should occur on a daily basis for core 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:
- * Full Backup
 - * Incremental Backup
 - * Differential Backup
 - * Mirror Backup
- 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 software, application software, 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.).

General Controls



1-1: IS Management (cont.)

- 1-1.14: Review administrator access privileges and ensure that access is limited and properly approved.
- 1-1.15: Establish periodic user training.
- 1-1.16: Regularly evaluate network availability and provide ongoing improvements to services as needed.

1-2: Contract/Vendor Management

- 1-2.1: Conduct a risk assessment to identify risks associated with contracting network and database administration to a third party. Gain an understanding of current practice in addressing these risks and mitigating negative impacts.
- 1-2.2: Review the contract prior to approval to ensure that business process requirements are adequately addressed and documented.
- 1-2.2: Involve end-users in the project.
- 1-2.3: Establish a Service Level Agreement for the maintenance and support of the contract, carefully defining specific performance for each party.
- 1-2.4: 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.
- 1-2.5: Confirm that the vendor is financially stable. Ensure that provisions are made to hold application source code in escrow.
- 1-2.6: Limit vendor access to entity resources and document monitoring and evaluation of access reasons and results.

1-3: Network Security

- 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 1-1.2 above) 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 (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 (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 software and provide for its continued use, including application of software updates as released. Ensure that the network security policy covers use of external devices (USB drives, 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 practice in addressing these risks and mitigating negative impacts.

General Controls

**1-3: Network Security (cont.)**

1-3.7: Establish remote access authentication procedures and encryption protocols (considering the risks identified above). Consider the use of virtual private networking (VPN) technology. Include procedures for monitoring and documenting of remote access and handling questionable activity.

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

1-4 Wireless Security

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

1-4.2: Establish security policies that address the use of wireless technology in 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: Establish routine application of security patches for wireless access devices, ensuring that upgrades are applied as released.

1-4.4: Establish physical access controls over wireless devices to prevent unauthorized access.

1-4.5: Review perimeter (external) security established in number 1-3.2, and ensure that the risks identified for wireless networking (1-4.1) are adequately addressed in the placement and configuration of network devices.

1-4.6: 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.

**1-5: Physical Access Security**

1-5.1: Considering criticality of network devices and their physical placement, develop a Physical Access Security Policy. 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.

1-5.3: Ensure that data processing areas are properly segregated from public access and limited to approved personnel only.

1-5.4: Implement the following physical security controls:

- * Entrance and Exit Controls
- * Visitor Escorting
- * Vendor Escorting
- * Surveillance Cameras

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

- * Fire Suppression System
- * Smoke Detector
- * Temperature/Humidity Detector
- * Uninterruptible Power Supply (UPS)
- * Emergency Power Generator
- * Rising-Floor
- * Water Seeker

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.



1-6: Logical Access Security

- 1-6.1: Based on identified risk areas, develop and document a Logical Access Security Policy 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 security administration procedures that ensure proper authorization of changes and additions to user accounts, including periodic review of user access by resource owners (e.g., department managers) 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 (system/admin default, guest, terminated users, etc.) should be removed or disabled.
- 1-6.3: Ensure that, at a minimum, the following best practices for logical security controls are implemented:
- * User identification and password are required.
 - * Users are systematically forced to change passwords on a periodic, recurring basis not less than 90 days.
 - * 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.
 - * New users are forced by the system to change their initially assigned password.
 - * A password history file, preventing reuse of at least the last five passwords, is retained.
 - * The user account is locked after three unsuccessful logon attempts and remains locked until reset by an administrator.
 - * Computer sessions timeout after 15 minutes of no activity, requiring user authentication to restore session.
 - * Management establishes and monitors user Activity Log/Audit Trail.
- 1-6.4: Implement checks and balances by users independent of security administration to ensure that procedures (established in 1.6.2) are being followed (e.g., terminated employee accounts are immediately disabled).
- 1-6.5: Ensure that access attempts are logged and reviewed for violations. Document identified violations and associated corrective actions as a part of incident handling procedures.

1-7: Disaster Recovery/Business Continuity

- 1-7.1: Document and approve a Disaster Recovery/Business Continuity Plan that, at a minimum, achieves the following:
- * Clearly assigns responsibilities for recovery.
 - * Includes detailed instructions for restoring operations (both operating system and critical applications).
 - * Identifies the alternate processing facility and the offsite backup storage facility.
 - * Includes necessary contact numbers.
 - * Includes appropriate system-recovery instructions.
 - * Includes manual/peripheral processing procedures for use until security management and program operations are restored.
 - * Includes application level contingency planning established in Section 2.7 of this document.
 - * Reflects current conditions and includes system interdependencies.
 - * Has been approved by key affected groups, including planning, senior management, information security and data center management, and program managers.
- 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 updated as conditions change.
- 1-7.4: Conduct and document testing of the Disaster Recovery/Business Continuity Plan at least once annually. Document and analyze test results, modifying the plan if necessary.

Note: Arkansas Continuity of Operations Program (ACOO) 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, visit.

<http://www.dis.arkansas.gov/security/PagesContinuityofOperationsProgram.aspx>



2-1: Data Input

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 manual controls to the existing processes.

2-1.2: Ensure that a transaction data structure is established and followed to reduce redundancies and to ensure effective transaction processing. Poor data quality may lead to failure of system controls, process inefficiencies, 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:

- * Recording or processing of duplicate transactions.
- * Unpopulated data fields.
- * Data formatting inconsistencies.
- * 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:

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

2-2: Data Processing

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; incorrect information should be identified, rejected, and corrected for subsequent processing:

- * 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.
- * Transaction or table logs should be available to compare to source documents.
- * Processing logs should be available to identify incompletely or incorrectly processed transactions.
- * Overrides applied to transaction processing should be tracked and monitored.
- * The application should perform online edit and validation checks on data being processed.
- * Warning and error messages should be produced during processing phases.
- * 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:

- * Ensure that data input is done in a controlled manner (e.g., proper authorization controls exist, both systematic and manual).
- * Ensure that all inputs have been processed and accounted for.
- * Identify and investigate missing or unaccounted for source documents or input transactions are identified and investigated.
- * Periodically review user error logs to evaluate the extent and status of data errors.
- * Require of 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:

- * Reconciliation of data inputs to data processed by the application.
- * Maintenance of a processing log that is reviewed for unusual or unauthorized activity.
- * 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.

Application Controls

2-3: Data Output

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:

- * Consistency of content and availability with end users' need.
- * Sensitivity and confidentiality of data.
- * 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 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 should be performed periodically.

Application Controls**2-4: Application Security Management**



- 2-4.1: Based on risks identified in 2.1.1, identify sensitive transactions for financial processes and sub-processes that application security policies should address. Develop security policy for financial applications that achieves the following:
- * Establishes security administration procedures.
 - * Depicts the methodology for developing the access structure and related security roles.
 - * Outlines ongoing security role management (including monitoring and maintenance procedures).
 - * 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.
 - * Defines maintenance procedures for application user security masters, incorporating procedures to ensure that additions, changes and deletions are properly authorized and supported by a documented business purpose.
 - * Periodically reviews user access lists to ensure that all active user IDs have a current need for access.
 - * Addresses encryption of sensitive application data (including authentication credentials), both stored and transmitted.
 - * Considers application interdependencies and system interfaces both internal within and external to the organization.
 - * Documents critical data processing and transmission points and establishes procedures for security and verification of data at each juncture.
 - * Demonstrates coordination with overall network security policy.
 - * 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 above and IS Best Practices.
- 2-4.3: Ensure that public access to applications is controlled via the following measures:
- * Use of digital signatures.
 - * Prohibition of direct access to production data.
 - * Distinct security policy covering public access workstations that restrict 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:
- * Identification and logging of reportable security exceptions and violations.
 - * Setup of logging and other parameters to notify administrators of security violations as they occur.
 - * 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 Level General Controls



2-5: Application Configuration Management

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.

2-6: Segregation of Duties

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.

- * Access to incompatible activities is assigned only when supported by a business need.

- * 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.

- * Users with authorized segregation of duties conflicts are documented, and their activity is monitored via transaction and audit logs.

- * Management retains documentation that segregation of duties risk has been mitigated through effective controls and monitoring.

2-7: Application Contingency Planning

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 priorities.

2-7.2: Set backup retention policy for each application based on the allowable outage times above, ensuring that backup intervals retained support necessary restoration periods outlined in contingency planning. 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 2-7.1. Incorporate the application level contingency planning and procedures (including backup policy) into the organization's Disaster Recovery Plan (DRP).

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 DRP testing and planning.

Application Level General Controls