

**ALL ABOUT AUDITS
AND
MUNICIPAL ACCOUNTING BASICS**



MAY 1, 2015

TABLE OF CONTENTS

	Page
Information about Legislative Audit	1
Records Necessary for an Audit.....	5
Budgeting Laws.....	8
Publishing Requirements Law	9
Segregation of Duties	10
Municipal Accounting Law	12
Municipal Ethics Law	24
Check Imaging Law	26
Purchasing Laws	29
Sale of Assets Law	32
	Appendix
Information Systems Best Practices.....	A
Sample Fixed Assets Listing	B
Sample Cash Receipts Journal	C
Sample Cash Disbursements Journal	D
Municipal Department Classifications	E
Act 582 of 2015.....	F

ARKANSAS LEGISLATIVE AUDIT

MAIN OFFICE

STATE CAPITOL

500 WOODLANE, STE 172

LITTLE ROCK, AR 72201-1099

501-683-8600

www.arklegaudit.gov

Roger Norman, JD, CPA, CFE, CFF

Legislative Auditor

roger.norman@arklegaudit.gov

June Barron, CPA, CFE

Deputy Legislative Auditor

june.barron@arklegaudit.gov

Tim Jones, CPA, CFF

Audit Manager

tim.jones@arklegaudit.gov

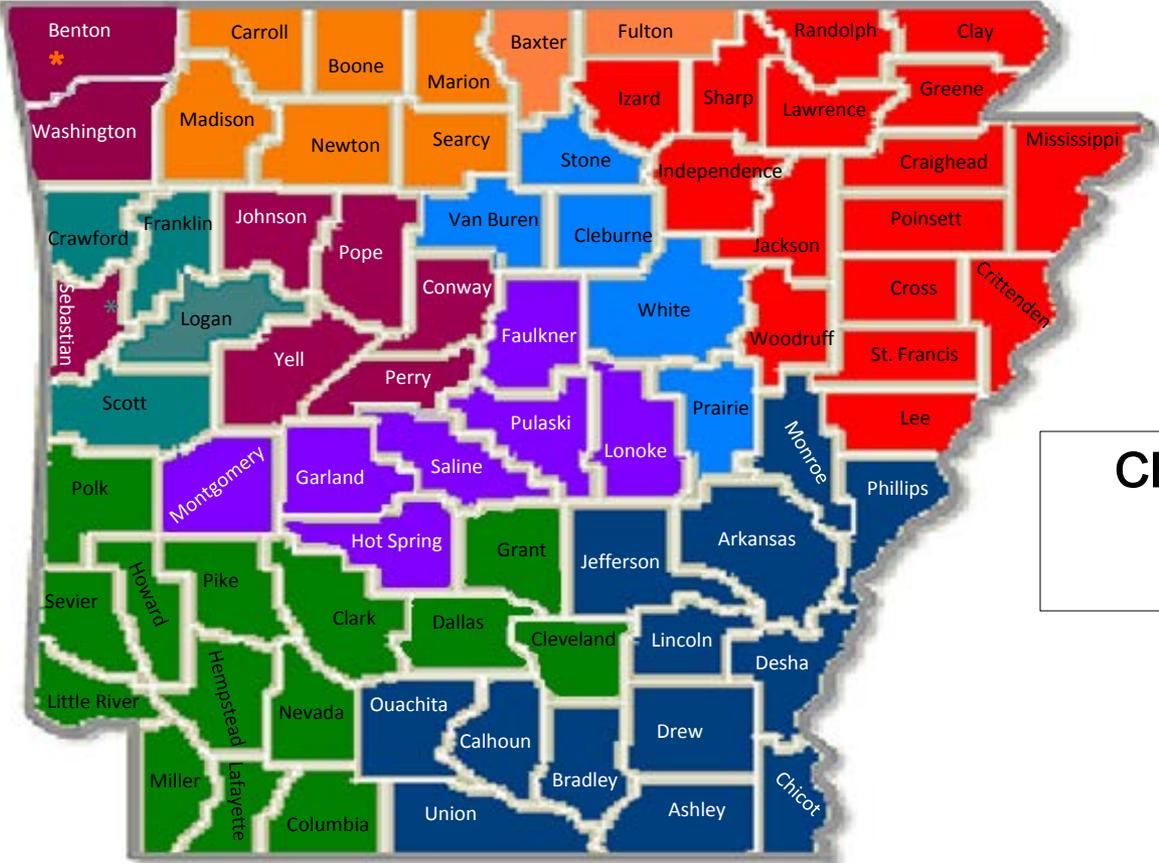
NORTH CENTRAL REGION

John Elser Joe Stacey
Jerry McCarty Albert Leding

- * (Leding has Benton Co & Stacey has municipalities within)
- * (Leding has Sebastian Co & Elser has municipalities within)

NORTHEASTERN REGION

Kevin Baldrige



CENTRAL REGION

Tim Thompson
Jimmy Garrett

SOUTHERN REGION

Marti Steel Theresa Outlaw

North Central Region:

Darrel Wheeler, CPA, CFE, CFF

Regional Manager

(501) 683-8600 Ext. 1023

darrel.wheeler@arklegaudit.gov

John Elser, CPA, CFE

Field Audit Supervisor

(501) 683-8600 Ext. 1050

john.elser@arklegaudit.gov

Albert Leding, CPA, CFE

Field Audit Supervisor

(501) 683-8600 Ext. 1051

albert.leding@arklegaudit.gov

Jerry McCarty, CPA, CFE, CFF

Field Audit Supervisor

(501) 683-8600 Ext. 1052

jerry.mccarty@arklegaudit.gov

Joe Stacey, CPA, CFE

Field Audit Supervisor

(501) 683-8600 Ext. 1054

joe.stacey@arklegaudit.gov

Central Region:

Tim Thompson, CPA, CFF

Field Audit Supervisor

(501) 683-8600 Ext. 1031

tim.thompson@arklegaudit.gov

Jimmy Garrett, CPA, CFF

Field Audit Supervisor

(501) 683-8600 Ext. 1030

jimmy.garrett@arklegaudit.gov

Northeast Region:

Kevin Baldrige, CPA, CFE

Field Audit Supervisor

(501) 683-8600 Ext. 1060

kevin.baldrige@arklegaudit.gov

Southern Region:

Jerry Woodall, CPA, CFE, CFF

Regional Manager

(501) 683-8600 Ext. 1024

jerry.woodall@arklegaudit.gov

Marti Steel, CPA

Field Audit Supervisor

(501) 683-8600 Ext. 1072

marti.steel@arklegaudit.gov

Theresa Outlaw, CPA, CFE

Field Audit Supervisor

(501) 683-8600 Ext. 4632

theresa.outlaw@arklegaudit.gov

RECORDS NECESSARY FOR AN AUDIT

All funds

Bank statements for entire year plus Jan. & Feb. of succeeding year

Receipt books for entire year plus Jan. & Feb. of succeeding year

Cash receipt and disbursement journals

For manual records:

Total monthly and year to date

Add across and down

For computerized records:

Maintain printout of transaction records every month (receipts listing and check register)

Maintain printout of detail general ledger every month

Check stubs or extra copy of check

Deposit books

Receipt ranges should be indicated on each deposit ticket

Investment records

Detail of certificates of deposits, interest rates and renewal dates

Form 1099 interest statements

Bank reconciliations for every month

Paid invoices

Separate by fund and by year

General ledger

Print a general ledger every month and at the end of the year print a detail general ledger

Agency funds

Police bond and fine fund and Court fund

Arrest reports
Distribution reports
Citation log
Court dockets
Installment payment records
Monthly settlements
Completed citation books
Records relating to the collection of hot checks
Printer's certificates for citation books
Detailed listing of pending balances

Payroll fund

Individual payroll records
Quarterly 941 payroll reports
W-2s, W-3s, W-4s, 1099s
Time sheets
Monthly federal/state tax remittances
Payroll tax electronic deposit confirmations

Other miscellaneous records

Council minutes up to the present date

Pension Board minutes up to the present date

Annual financial statements and proofs of publication/posting

Insurance policies

Lease agreements and other debt agreements

Fixed asset records:

- Description of item
- Cost of item
- Date purchased
- Serial number, if available

Personnel policies

- Vacation & sick leave
- Travel reimbursement

Budgets

Ordinances and resolutions

Franchise fee records

Audit reports of funds performed by other auditors

Act 833 reports (Fire Training and Equipment)

Listing of all credit cards and authorized users

First class cities only

- Mayor's end of the year report
- Quarterly financial reports
- Bids and proofs of publication

BUDGETING LAWS

14-58-201. Annual submission.

On or before December 1 of each year, the mayor of all cities and incorporated towns having the mayor-council form of government shall submit to the governing body of the city or town, for its approval or disapproval, a proposed budget for operation of the city or town from January 1 to December 31 of the forthcoming year.

HISTORY: Acts 1959, No. 28, § 1; 1981, No. 344, § 1; A.S.A. 1947, § 19-4421.

14-58-202. Adoption.

Under this subchapter, the governing body of the municipality shall, on or before February 1 of each year, adopt a budget by ordinance or resolution for operation of the city or town.

HISTORY: Acts 1959, No. 28, § 2; 1981, No. 344, § 2; A.S.A. 1947, § 19-4422; Acts 2011, No. 622, § 1.

14-58-203. Appropriations and changes.

(a) The approval by the municipal governing body of the budget under this subchapter shall, for the purposes of the budget from time to time amount to an appropriation of funds which are lawfully applicable to the items therein contained.

(b) The governing body may alter or revise the budget and unpledged funds appropriated by the governing body for any purpose may be subsequently, by action of the governing body, appropriated to another purpose, subject to the following exceptions:

(1) Funds resulting from taxes levied under statutes or ordinances for specific purposes may not be diverted to another purpose;

(2) Appropriated funds may not be diverted to another purpose where any creditor of the municipality would be prejudiced thereby.

HISTORY: Acts 1959, No. 28, § 3; A.S.A. 1947, § 19-4423.

PUBLISHING REQUIREMENTS LAW

14-55-206. Publishing or posting requirements.

(a) (1) (A) All bylaws or ordinances of a general or permanent nature and all those imposing any fine, penalty, or forfeiture shall be published in some newspaper published in the municipality.

(B) In municipalities in which no newspaper is published, written or printed notice posted in five (5) of the most public places designated by the governing body in an ordinance or minutes of the governing body shall be deemed a sufficient publication of any law or ordinance.

(2) It shall be deemed a sufficient defense to any suit or prosecution of such fine, penalty, or forfeiture to show that no notice was given as provided herein.

(b) As to ordinances establishing rules and regulations for zoning, construction of buildings, the installation of plumbing, the installation of electric wiring, or other similar work, where such rules and regulations have been printed as a code in book form, the code or provisions thereof may be published by the municipality by reference to title of the code without further publication or posting thereof. However, no fewer than three (3) copies of the code shall be filed for use and examination by the public in the office of the clerk or recorder of the municipality after the adoption thereof if there is no electronic form of the code available for examination by the public.

HISTORY: Acts 1949, No. 36, § 1; A.S.A. 1947, § 19-2404; Acts 1993, No. 295, § 2; 2009, No. 25, § 1.

SEGREGATION OF DUTIES

CASH/RECEIPTS

- | | |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a. Mail | 1.) One employee opens the mail and 2.) another employee writes the receipts or enters the check or cash collected into a book or journal to be receipted later. |
| b. Collections | Employee(s) writes the receipts as funds are received. |
| c. Deposits | Employee prepares and makes the deposit. |
| d. Reconciles | Employee receives unopened bank statements and reconciles bank balance and deposits with book balance and cash receipts journal. |
| e. Posts | Employee posts the cash receipts journal. |

COMPATIBLE FUNCTIONS

Employee (1)	Employee (2)
a.(1.), c. and e.	a.(2.), b., d. and e.

DISBURSEMENTS/ RECEIVING

- | | |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a. Purchasing | Employee(s) orders goods from vendors. |
| b. Receiving | Employee(s) receives goods from vendor and documents that the goods have been received by signing and dating the invoice or a receiving report. |
| c. Processing | Employee prepares the check and verifies the accuracy of the invoice for payment and cosigns the check. |
| d. Approving | 1.) Employee reviews and approves invoices for payment by initialing and dating the invoice. 2.) The approver or another employee cosigns the check and mails the payment. |
| e. Reconciles | Employee receives unopened bank statements and reconciles bank balance and withdrawals with the book balance and disbursements journal. |
| f. Posts | Employee posts the cash disbursements journal. |

COMPATIBLE FUNCTIONS

Employee (1)	Employee (2)	Employee (3)
a. and c.	d.	b., e., and f.
a., c., e. and f.	d.	b.
a., c. and e.	d. and f.	b.

SEGREGATION OF DUTIES

PAYROLL

- | | |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a. Individual Personnel Files | Employee has custody of individual personnel files including, but not limited to, W-4's, health ins., and other withholding information and establishes new employees for payroll purposes. |
| b. Individual Payroll Records | Employee has custody of individual payroll record (name, identification #, pay period, hours, rate of pay, amount, withholdings, etc.) |
| c. Time Records | Employee(s) prepares time record for work performed for each pay period including time charged for vacation, sick and other leave. |
| d. Approval | Employee(s) other than the preparer of the time record approves the time record and gives the original to the employee processing payroll. |
| e. Processing | Employee(s) process payroll from the time and payroll records including calculation of each individual's pay based on these records and prepares the check or information for direct deposit to each individual account. |
| f. Posts | Employee post payroll to the individual payroll records and to the proper accounts in the cash disbursements journal. |
| g. Reconciles | Employee reconciles payroll to the appropriate federal and state reports and to the individual payroll records and cash disbursements journal. |
| h. Payroll Distribution | Payroll employee delivers checks to department supervisor for distribution or payroll employee reviews distribution and direct deposits made to each employees account. |

COMPATIBLE FUNCTIONS

	PAYROLL			DEPARTMENT	
Employee (1)	Employee (2)	Employee (3)	Employee (1)	Supervisor	
a., b. and f.	e.	g. and h.	c.	d.	
a., b. and g.	e.	f. and h.	c.	d.	
a. and b.	e. and f.	h.	c.	d.	

Municipal Accounting Law

14-59-101. Title.

This chapter shall be known and cited as the "Arkansas Municipal Accounting Law".

HISTORY: Acts 1973, No. 159, § 1; A.S.A. 1947, § 19-5301; Acts 2011, No. 621, § 1.

14-59-102. Applicability.

This chapter shall apply to all funds under the budgetary control of the council or board of directors of the various municipalities of this state, except water and sewer departments.

HISTORY: Acts 1973, No. 159, § 2; A.S.A. 1947, § 19-5302; Acts 2001, No. 1062, § 1.

14-59-103. Exemption for other systems.

(a) In the event any municipality feels its system of bookkeeping is such that it equals or exceeds the basic system prescribed by this chapter, the municipality may request a review by the Legislative Joint Auditing Committee.

(b) Upon the committee's concurrence with these facts, it may issue a certificate to the municipality stating that the municipality's accounting system is of a degree of sophistication such that the basic requirements of this chapter are being met and exempting the municipality from the requirements of the particulars of the system prescribed by this chapter.

HISTORY: Acts 1973, No. 159, § 14; A.S.A. 1947, § 19-5314.

14-59-104. Bank accounts.

(a) All municipalities of this state receiving state aid in the form of either turnback of general revenues or highways revenues shall maintain all funds in depositories approved for such purposes by law.

(b) The municipalities shall maintain separate bank accounts for general funds and street funds.

(c) The accounts shall be maintained in the name of the municipality.

HISTORY: Acts 1973, No. 159, § 3; A.S.A. 1947, § 19-5303.

14-59-105. Prenumbered checks -- Electronic funds transfers.

(a) All disbursements of municipal funds, except those described in this section and as noted in § 14-59-106, petty cash funds, are to be made by prenumbered checks drawn upon the bank account of that municipality.

(b) The checks shall be of the form normally provided by commercial banking institutions and shall contain as a minimum the following information:

(1) Date of issue;

(2) Check number;

(3) Payee;

(4) Amount; and

(5) Signature of two (2) authorized disbursing officers of the city.

(c) Disbursements of municipal funds used for payment of salaries and wages of municipal officials and employees may be made by electronic funds transfer provided that the municipal employee or official responsible for disbursements maintains a ledger containing at least the:

(1) Name, address, and social security number of the employee receiving payment of salary or wages;

(2) Routing number from the bank in which the funds are held;

(3) Account number;

(4) Accounts clearing house trace number pertaining to the transfer;

(5) Date and amount transferred; and

(6) Proof that the employee has been notified of direct deposit of his or her salary or wages by electronic funds transfer.

(d) Disbursements of municipal funds used for payments to federal or state governmental entities may be made by electronic funds transfer.

(e) (1) Disbursements of municipal funds, other than for payments under subsections (c) and (d) of this section, may be made by electronic funds transfer provided that:

(A) The governing body of the municipality shall establish by ordinance an electronic funds payment system directly into payees' accounts in financial institutions in payment of any account allowed against the municipality;

(B) For purposes of this subsection, municipalities opting for an electronic funds payment system shall establish an electronic payment method that provides for internal accounting controls and documentation for audit and accounting purposes; and

(C) Each electronic payment method established under subdivision (e)(2) of this section shall be approved by the Legislative Joint Auditing Committee before implementation by the municipality.

(2) A single electronic funds payment may contain payments to multiple payees, appropriations, characters, or funds.

(f) A disbursement of municipal funds shall have adequate supporting documentation for the disbursement.

HISTORY: Acts 1973, No. 159, § 5; A.S.A. 1947, § 19-5305; Acts 1997, No. 543, § 1; 2009, No. 316, § 1; 2011, No. 621, § 2.

14-59-106. Petty cash funds.

(a) Municipalities are permitted to establish petty cash funds, so long as the funds are maintained as set forth in this section.

(b) (1) The establishment of such a fund must be approved by the city council.

(2) (A) In establishing such a fund, a check is to be drawn upon the general fund of the municipality payable to "petty cash."

(B) That amount may be maintained in the municipal offices for the handling of small expenditures for items such as postage, light bulbs, delivery fees, etc.

(c) (1) A paid-out slip is to be prepared for each item of expenditure from the fund and signed by the person receiving the moneys.

(2) These paid-out slips shall be maintained with the petty cash. When the fund becomes depleted, the municipality may then draw another check payable to "petty cash" in an amount which equals the total paid-out slips issued. At that time, the paid-out slips shall be removed from the "petty cash fund," and utilized as invoice support for the check replenishing petty cash.

HISTORY: Acts 1973, No. 159, § 6; A.S.A. 1947, § 19-5306.

14-59-107. Fixed asset records.

(a) The governing body shall adopt a policy defining fixed assets. At a minimum, the policy shall set forth the dollar amount and useful life necessary to qualify as a fixed asset.

(b) (1) All municipalities shall establish by major category and maintain, as a minimum, a listing of all fixed assets owned by the municipality.

(2) The listing shall be totaled by category with a total for all categories.

(3) The categories of fixed assets shall include the major types, such as:

(A) Land;

(B) Buildings;

(C) Motor vehicles, by department;

(D) Equipment, by department; and

(E) Other assets.

(c) The listing shall contain as a minimum:

(1) Property item number, if used by the municipality;

(2) Brief description;

(3) Serial number, if available;

(4) Date of acquisition; and

(5) Cost of property.

HISTORY: Acts 1973, No. 159, § 7; A.S.A. 1947, § 19-5307; Acts 2001, No. 1062, § 2; 2011, No. 621, § 3.

14-59-108. Reconciliation of bank accounts.

(a) (1) On a monthly basis, all municipalities shall reconcile their cash receipts and disbursements journals to the amount on deposit in banks.

(2) The reconciliation under subdivision (a)(1) of this section shall be approved by a municipal official or employee, other than the person preparing the reconciliation, as designated by the chief executive officer of the municipality.

(b) The reconciliations should take the following form:

City of

Date

Amount Per Bank Statement

Dated \$.00

Add: Deposits in transit (Receipts recorded in Cash Receipts Journal not shown on this bank statement).

DATE RECEIPTS NO. AMOUNT

\$.00

.00

.00

.00

Deduct: Outstanding Checks (Checks issued and dated prior to date of bank statement per Cash Disbursements Journal not having yet cleared the bank).

CHECK NO. PAYEE AMOUNT

\$.00

.00

.00

.00

RECONCILED BALANCE

\$.00

This reconciled balance shall agree to either the cash balance as shown on the municipality's check stubs running bank balance or the municipality's general ledger cash balance, whichever system the municipality employs.

HISTORY: Acts 1973, No. 159, § 12; A.S.A. 1947, § 19-5312; Acts 2011, No. 621, § 4.

14-59-109. Prenumbered receipts.

(a) All funds received are to be formally receipted at the time of collection or the earliest opportunity by the use of prenumbered receipts or mechanical receipting devices.

(b) (1) In the use of prenumbered receipts, the following minimum standards shall be met:

(A) If manual receipts are used, receipts are to be prenumbered by the printer and a printer's certificate obtained and retained for audit purposes. The certificate shall state the date printing was done, the numerical sequence of receipts printed, and the name of the printer;

(B) The prenumbered receipts shall contain the following information for each item receipted:

- (i) Date;
- (ii) Amount of receipt;
- (iii) Name of person or company from whom money was received;
- (iv) Purpose of payment;
- (v) Fund to which receipt is to be credited; and
- (vi) Identification of employee receiving money.

(2) If manual receipts are used, the original receipt should be given to the party making payment. One (1) duplicate copy of the receipt shall be maintained in numerical order in the receipt book and made available to the auditors during the course of annual audit. Additional copies of the receipt are optional with the municipality and may be used for any purposes they deem fit.

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

HISTORY: Acts 1973, No. 159, § 4; A.S.A. 1947, § 19-5304; Acts 2011, No. 621, § 5.

14-59-110. Cash receipts journals.

(a) (1) Municipalities shall establish a cash receipts journal or an electronic receipts listing that shall indicate:

- (A) The receipt number;
- (B) The date of the receipt;
- (C) The payor;
- (D) The amount of the receipt; and
- (E) Classification or general ledger account.

(2) The classification of the receipts shall include the major sources of revenue, such as:

- (A) State revenues;
- (B) Property taxes;
- (C) Sales taxes;
- (D) Fines, forfeitures, and costs;
- (E) Franchise fees;
- (F) Transfers in; and

(G) Other.

(b) (1) All items of receipts shall be posted to and properly classified in the cash receipts journal or electronic receipts listing.

(2) (A) The journal shall be properly balanced and totaled monthly and on a year-to-date basis.

(B) The journal shall be reconciled monthly to total bank deposits as shown on the municipalities' bank statements.

(3) The electronic receipts listing shall be posted to the general ledger at least monthly. The general ledger shall be reconciled monthly to total bank deposits as shown on the municipalities' bank statements.

HISTORY: Acts 1973, No. 159, § 10; A.S.A. 1947, § 19-5310; Acts 2001, No. 1062, § 3; 2011, No. 621, § 6.

14-59-111. Cash disbursements journals.

(a) (1) Municipalities shall establish a cash disbursements journal or electronic check register that shall indicate the date, payee, check number or transaction number, amount of each check written or transaction, and classification or general ledger account.

(2) The classifications of expenditures shall include the major type of expenditures by department, such as:

(A) Personal services;

(B) Supplies;

(C) Other services and charges;

(D) Capital outlay;

(E) Debt service; and

(F) Transfers out.

(b) (1) The cash disbursements journal shall be properly balanced and totaled monthly and on a year-to-date basis.

(2) The cash disbursements journal shall be reconciled monthly to total bank disbursements as indicated on the monthly bank statements.

(3) The electronic check register shall be posted to the general ledger at least monthly. The general ledger shall be reconciled monthly to total bank disbursements as indicated on the monthly bank statements.

HISTORY: Acts 1973, No. 159, § 11; A.S.A. 1947, § 19-5311; Acts 2001, No. 1062, § 4; 2011, No. 621, § 7.

14-59-112, 14-59-113. [Repealed.]

14-59-114. Maintenance and destruction of accounting records.

(a) Accounting records can basically be divided into the following three (3) groups:

(1) (A) Support Documents. Support documents consist primarily of the following items:

- (i)** Cancelled checks;
- (ii)** Invoices;
- (iii)** Bank statements;
- (iv)** Receipts;
- (v)** Deposit slips;
- (vi)** Bank reconciliations;
- (vii)** Check book register or listing;
- (viii)** Receipts listing;
- (ix)** Monthly financial reports;
- (x)** Payroll records;
- (xi)** Budget documents; and
- (xii)** Bids, quotes, and related documentation.

(B) These records shall be maintained for a period of at least four (4) years and in no event shall be disposed of before being audited for the period in question.

(2) (A) Semipermanent Records. Semipermanent records consist of:

- (i)** Fixed assets and equipment detail records;
- (ii)** Investment and certificate of deposit records;
- (iii)** Journals, ledgers, and subsidiary ledgers; and
- (iv)** Annual financial reports.

(B) (i) These records shall be maintained for a period of not less than seven (7) years and in no event shall be disposed of before being audited for the period in question.

(ii) For investment and certificate of deposit records, the seven (7) years of required maintenance begins on the date of maturity.

(3) (A) Permanent Records. Permanent records consist of:

- (i)** City or town council minutes;
- (ii)** Ordinances;
- (iii)** Resolutions;
- (iv)** Employee retirement documents; and
- (v)** Annual financial audits.

(B) These records shall be maintained permanently.

(b) When documents are destroyed, the municipality shall document the destruction by the following procedure:

(1) (A) An affidavit is to be prepared stating which documents are being destroyed and to which period of time they apply, indicating the method of destruction;

(B) This affidavit is to be signed by the municipal employee performing the destruction and one (1) council member.

(2) (A) In addition, the approval of the council for destruction of documents shall be obtained, and an appropriate note of the approval indicated in the council minutes along with the destruction affidavit;

(B) This council approval shall be obtained before the destruction.

HISTORY: Acts 1973, No. 159, § 15; 1979, No. 616, § 2; A.S.A. 1947, § 19-5315; Acts 2011, No. 621, § 8.

14-59-115. Duties of municipal treasurer.

(a) Each municipal treasurer of this state or the designated representative that has been approved by the governing body shall submit a monthly financial report to the council or board of directors.

(b) (1) Municipal treasurers shall maintain the accounting records prescribed in this chapter.

(2) (A) If the treasurer does not comply with the provisions of this chapter or requests that specific duties be assigned to another employee or contracting entity, the governing body of a municipality may assign specific duties outlined in this chapter to another employee, or it may contract for such services to be performed by a private, qualified person or entity.

(B) The governing body of a municipality may not assign duties relating to the collecting or

disbursing of funds to anyone other than an employee of the municipality.

HISTORY: Acts 1973, No. 159, § 13; A.S.A. 1947, § 19-5313; Acts 2001, No. 1062, § 5; 2011, No. 621, § 9.

SEE ACT 582 OF 2015 – EFFECTIVE JULY 21, 2015

14-59-116. Annual publication of financial statement.

(a) (1) The governing body of each municipality shall publish annually a financial statement of the municipality, including receipts and expenditures for the period and a statement of the indebtedness and financial condition of the municipality. The financial statement shall be published one (1) time in a newspaper published in the municipality.

(2) This financial statement shall be at least as detailed as the minimum record of accounts as provided in this chapter.

(3) This financial statement shall be published by April 1 of the following year.

(b) In municipalities in which no newspaper is published, the financial statement shall be posted in two (2) of the most public places in the municipality.

HISTORY: Acts 1973, No. 159, §§ 18, 19, as added by 1977, No. 308, § 1; A.S.A. 1947, §§ 19-5316, 19-5317; Acts 2011, No. 621, § 10.

14-59-117. Withholding of turnback for noncompliance.

(a) (1) If the Division of Legislative Audit determines that a municipal treasurer is not substantially complying with this chapter, the division shall report the findings to the Legislative Joint Auditing Committee.

(2) (A) If a public official or a private accountant determines that a municipal treasurer is not substantially complying with this chapter, the official or accountant shall notify the Legislative Joint Auditing Committee of his or her findings.

(B) Upon notification, the Legislative Joint Auditing Committee shall direct the division to confirm that the municipal treasurer is not substantially complying with this chapter.

(C) Upon confirmation, the division shall report the findings to the Legislative Joint Auditing Committee.

(b) (1) Upon notification of noncompliance by the division, the Legislative Joint Auditing Committee shall notify in writing the mayor and the city council or town council that the municipality's accounting records do not substantially comply with this chapter.

(2) The municipality has sixty (60) days after the date of notification to bring the accounting records into substantial compliance with this chapter.

(3) (A) After the sixty (60) days allowed for compliance or upon request by the appropriate municipal officials, the division shall review the records to determine if the municipality substantially complies with this chapter.

(B) The division shall report its findings to the Legislative Joint Auditing Committee.

(c) (1) (A) If the municipality has not achieved substantial compliance within the sixty-day period, the Legislative Joint Auditing Committee may report the noncompliance to the Treasurer of State.

(B) Upon receipt of the notice of noncompliance from the Legislative Joint Auditing Committee, the Treasurer of State shall place fifty percent (50%) of the municipality's turnback in escrow until the Legislative Joint Auditing Committee reports to the Treasurer of State that the municipality has substantially complied with this chapter.

(2) If the municipality has not achieved substantial compliance within the sixty-day period, the governing body of the municipality shall assign specific duties outlined in this chapter to another employee or shall contract for the services to be performed by a qualified person or entity.

(3) (A) The division shall notify the Legislative Joint Auditing Committee when the municipality has substantially complied with this chapter.

(B) (i) The Legislative Joint Auditing Committee shall notify the Treasurer of State that the municipality has substantially complied with this chapter.

(ii) Upon notice of compliance from the Legislative Joint Auditing Committee, the Treasurer of State shall remit all turnback due to the municipality.

(d) (1) If the division has not received a request for a review of the records from the municipality before the end of the one-hundred-twenty-day period after the first date of notification of noncompliance, the Legislative Joint Auditing Committee may notify the municipality and the Treasurer of State of the continued noncompliance.

(2) Upon notice by the Legislative Joint Auditing Committee, the Treasurer of State shall withhold all turnback until such time that the accounting records have been reviewed and determined by the division to be in substantial compliance with this chapter.

(e) (1) If the division has not received a request for a review of the records from the municipality before the end of six (6) months after the initial notification of noncompliance, the Legislative Joint Auditing Committee may notify the municipality and the Treasurer of State of the continued noncompliance.

(2) Upon notice of noncompliance for six (6) months, the municipality forfeits all escrowed funds, and the Treasurer of State shall redistribute all escrowed turnback funds applicable to the municipality among all other municipalities receiving turnback.

(3) The municipality shall not be eligible to receive any additional turnback from the state until the Legislative Joint Auditing Committee notifies the Treasurer of State that the municipality has substantially complied with this chapter.

HISTORY: Acts 2001, No. 1062, § 6; 2009, No. 288, § 1.

14-59-118. Penalty.

(a) Any municipal treasurer who refuses or neglects to maintain the books and records provided in this chapter shall be deemed guilty of malfeasance.

(b) Upon conviction in circuit court, the treasurer shall be fined in any sum not less than one hundred dollars (\$100) nor more than one thousand dollars (\$1,000) and shall be removed from office.

HISTORY: Acts 2001, No. 1062, § 7.

MUNICIPAL ETHICS LAWS

14-42-107. Interest in offices or contracts prohibited.

(a) (1) No alderman, member of any council, or elected official of a municipal corporation, during the term for which he or she has been elected or one (1) year thereafter, shall be appointed to any municipal office that was created or the emoluments of which have been increased during the time for which he or she has been elected except to fill a vacancy in the office of mayor, alderman, clerk, clerk-treasurer, recorder, or recorder-treasurer.

(2) No alderman or council member shall be appointed to any municipal office, except in cases provided for in §§ 14-37-101 et seq. -- 14-61-101 et seq., during the time for which he or she may have been elected.

(b) (1) No alderman, council member, official, or municipal employee shall be interested, directly or indirectly, in the profits of any contract for furnishing supplies, equipment, or services to the municipality unless the governing body of the city has enacted an ordinance specifically permitting aldermen, council members, officials, or municipal employees to conduct business with the city and prescribing the extent of this authority.

(2) The prohibition prescribed in this subsection shall not apply to contracts for furnishing supplies, equipment, or services to be performed for a municipality by a corporation in which no alderman, council member, official, or municipal employee holds any executive or managerial office or by a corporation in which a controlling interest is held by stockholders who are not aldermen or council members.

HISTORY: Acts 1875, No. 1, § 86, p. 1; C. & M. Dig., § 7520; Pope's Dig., § 9580; Acts 1963, No. 182, § 1; 1981, No. 485, § 1; A.S.A. 1947, § 19-909; Acts 2003, No. 1299, § 1; 2009, No. 403, § 1.

14-42-108. Prohibited actions by municipal officials or employees -- Penalty.

(a) (1) It shall be unlawful for any official or employee of any municipal corporation of this state to receive or accept any water, gas, electric current, or other article or service from the municipal corporation, or any public utility operating therein, without paying for it at the same rate and in the same manner that the general public in the municipal corporation pays therefor.

(2) (A) This section shall not affect rights to free or other special services given to certain municipal officials and employees under the terms of franchises in effect with public utilities in this state.

(B) This section shall not apply to any city official or employee of any municipal corporation of this state as to free streetcar transportation.

(b) (1) It shall be unlawful for any city official or employee of any municipal corporation in this state to furnish or give to any person, concerns, or corporations any property belonging to the municipal corporation, or service from any public utility owned or operated by the municipal corporation, unless payment is made therefor to the municipal corporation at the usual and regular rates, and in the usual manner, except as provided in subsection (a) of this section.

(2) The waterworks commission of cities of the first class shall be authorized to make donations of money from the revenue of municipal waterworks systems to the local United Way campaign or other citywide nonsectarian, incorporated charitable organizations.

(c) (1) Any person violating the provisions of this section shall be deemed guilty of a misdemeanor and upon conviction shall be fined in any sum not less than ten dollars (\$10.00) nor more than two hundred fifty dollars (\$250).

(2) Conviction shall ipso facto remove the official or employee from the municipal office or position held by him and shall render him ineligible to thereafter hold any office or position under, or in connection with, the municipal corporation.

HISTORY: Acts 1919, No. 230, §§ 1-3; C. & M. Dig., §§ 7522-7524; Pope's Dig., §§ 9582-9584; Acts 1941, No. 288, § 1; A.S.A. 1947, §§ 19-916 -- 19-918.

CHECK IMAGING LAWS

19-2-501. Purpose.

The State of Arkansas and its political subdivisions have the responsibility to properly account for all financial transactions. In order to help fulfill this responsibility, the State of Arkansas and other public entities are required to maintain books and records of transactions. The State of Arkansas and its political subdivisions recognize that through the use of computers and electronic data, banking and the flow of information are continuing to change. With this change, it is important that the State of Arkansas and its political subdivisions continue to receive evidentiary information concerning financial transactions. The purpose of this subchapter is to permit public entities to accept photographic copies or digital images of financial transactions and to require financial institutions to furnish the needed documentation in a readable, meaningful, permanent format.

HISTORY: Acts 1999, No. 648, § 1.

19-2-502. Definitions.

As used in this subchapter, "public entity" means state agencies, including all constitutional offices and agencies, boards, and commissions, state institutions of higher education, municipalities, counties, school districts, education service cooperatives, improvement districts, and other public officials or public offices. Public entities shall maintain records of all transactions with financial institutions.

HISTORY: Acts 1999, No. 648, § 2; 2007, No. 617, § 39.

19-2-503. Eligibility to accept public funds.

In order for a financial institution to be eligible to be a depository of public funds, the financial institution must furnish the public entity documentation, as required in this subchapter, of transactions with or through that institution.

HISTORY: Acts 1999, No. 648, § 3.

19-2-504. Transaction summaries.

On a monthly basis, financial institutions shall furnish public entities with statements summarizing all transactions of the public entity. Unless the public entity and the financial institution have a written agreement to receive digital images or copies in compliance with the provisions of this subchapter, the financial institutions shall return all original canceled checks to the public entity along with the transaction summary or statement.

HISTORY: Acts 1999, No. 648, § 4.

19-2-505. Approval by the Division of Legislative Audit.

Any financial institution desiring to provide public entities with images of canceled checks on paper or by digital media as provided in this subchapter shall provide a sample of imaged documents or the digital media to the Division of Legislative Audit for review. Upon receipt, the Division of Legislative Audit shall immediately review and notify the financial institution whether or not the imaged documents or digital media are in compliance with this subchapter.

HISTORY: Acts 1999, No. 648, § 5.

19-2-506. Digital images or copies of documentation.

(a) Agreement. After a financial institution has received written notification from the Division of Legislative Audit that the submitted samples of its imaged documents or digital media comply with the provisions of this subchapter and upon agreement with the public entity, the financial institution may provide public entities canceled check images in the media type and quality approved by the Division of Legislative Audit.

(b) Complete image. The canceled check copies or the digital images of financial transactions provided to the public entity by the financial institutions must be legible and show both the front and back images of the canceled checks.

(c) Digital images. (1) If a financial institution provides the canceled check images on digital media, the images shall be provided on a read-only CD-ROM or other agreed upon digital media that would provide a permanent and tamper-proof record.

(2) If particular software is needed to view or search the digital images, the financial institution shall provide such software to the public entity and, upon request, to the Division of Legislative Audit. When using the appropriate software, the canceled check images must be clear and readable.

(3) Before delivery of the CD-ROM or other digital media to the public entity, the financial institution shall perform random verification of the legibility of the contents of the data. The financial institution shall submit a letter or other method approved by the Division of Legislative Audit acknowledging verification of the contents, along with the CD-ROM or other digital media, to the public entity.

(4) The financial institution may also provide a duplicate copy of the check images on digital media, conforming to the specifications provided in this subchapter, to the Division of Legislative Audit on a monthly basis.

(d) Paper images. If a financial institution provides the canceled check images on paper, the images must be of such clarity and size that the details may be read without the aid of a magnifying device. The financial institution must be able to, and, at the request of the Division of Legislative Audit, must provide duplicate copies of any checks and statements delivered to a public entity with the same clarity and size as the imaged documents previously delivered.

(e) Authentication of paper images. (1) If the financial institution provides canceled check images on paper, the financial institution shall implement one (1) of the following procedures to provide verification of the authenticity of the records retained by the public entity:

(A) A duplicate copy of the check images on paper and statements mailed to the Division of Legislative Audit on a monthly basis;

(B) The use of an identifying mark unique to the financial institution on the paper images of checks sent to the public entity;

(C) The delivery of a duplicate copy of the check images on digital media, conforming to the digital imaging specifications set forth in this subchapter, to the Division of Legislative Audit on a monthly basis; or

(D) Any other authenticating method approved by the Division of Legislative Audit.

(2) The financial institution is authorized to elect which of the foregoing procedures it shall implement to provide authentication of paper images relating to the accounts of each public entity. Upon reasonable notice to the Division of Legislative Audit and the public entity, the financial institution may elect to implement one (1) of the other authentication procedures or elect to provide images on digital media as set forth in this subchapter.

HISTORY: Acts 1999, No. 648, § 6.

19-2-507. Request of records by Legislative Auditor.

(a) Upon request by the Legislative Auditor, a financial institution shall provide a copy of a public entity's financial information directly to the Division of Legislative Audit staff without delay or approval from the public entity.

(b) The financial institutions may provide the digital transaction statements and digital canceled check images to the Division of Legislative Audit in a media format allowed under the provisions of this subchapter for public entities or other media mutually agreed upon by the financial institution and the Division of Legislative Audit.

(c) No bank shall be liable for making available to the Division of Legislative Audit staff any of the information required under the provisions of this subchapter.

(d) Any cost associated with providing this information to the Division of Legislative Audit shall be borne by the public entity being audited or investigated.

HISTORY: Acts 1999, No. 648, § 7.

19-2-508. [Repealed.]

19-2-509. Effect on other laws.

The provisions of this subchapter do not change, amend, or repeal any laws or regulations regarding a financial institution's normal obligations and responsibilities to maintain customer financial records.

HISTORY: Acts 1999, No. 648, § 9.

PURCHASING LAWS

14-58-303. Purchases and contracts generally.

(a) In a city of the first class, city of the second class, or incorporated town, the mayor or the mayor's duly authorized representative shall have exclusive power and responsibility to make purchases of all supplies, apparatus, equipment, materials, and other things requisite for public purposes in and for the city and to make all necessary contracts for work or labor to be done or material or other necessary things to be furnished for the benefit of the city, or in carrying out any work or undertaking of a public nature in the city.

(b) (1) (A) Except as provided under § 14-58-104, the municipal governing body of any city of the first class shall provide by ordinance the procedure for making all purchases which do not exceed the sum of twenty thousand dollars (\$20,000).

(B) Except as provided under § 14-58-104, the municipal governing body of any city of the second class or incorporated town may provide by ordinance the procedure for making all purchases.

(2) (A) (i) Except as provided under § 14-58-104, in a city of the first class where the amount of expenditure for any purpose or contract exceeds the sum of twenty thousand dollars (\$20,000), the mayor or the mayor's authorized representative shall invite competitive bidding on the purpose or contract by legal advertisement in any local newspaper.

(ii) Bids received pursuant to the advertisement shall be opened and read on the date set for receiving the bids in the presence of the mayor or the mayor's authorized representative.

(iii) The mayor or the mayor's authorized representative shall have exclusive power to award the bid to the lowest responsible bidder, but may reject any and all bids received.

(B) The governing body by ordinance may waive the requirements of competitive bidding in exceptional situations where this procedure is deemed not feasible or practical or as provided under § 14-58-104.

(c) (1) In a city of the first class, a city of the second class, or an incorporated town, the governing body by ordinance shall have the option to make purchases by participation in a reverse Internet auction, except that purchases and contracts for construction projects and materials shall be undertaken pursuant to subsections (a) and (b) of this section and § 22-9-203.

(2) The ordinance shall include, but is not limited to, the following procedures:

(A) Bidders shall be provided instructions and individually secured passwords for access to the reverse Internet auction by either the city or the town, or the reverse Internet auction vendor;

(B) The bidding process shall be timed, and the time shall be part of the reverse Internet auction specifications;

- (C) The reverse Internet auction shall be held at a specific date and time;
 - (D) The reverse Internet auction and bidding process shall be interactive, with each bidder able to make multiple bids during the allotted time;
 - (E) Each bidder shall be continually signaled his or her relative position in the bidding process;
 - (F) Bidders shall remain anonymous and shall not have access to other bidders or bids; and
 - (G) The governing body shall have access to real-time data, including all bids and bid amounts.
- (3) The governing body may create by an additional ordinance reverse Internet auction specifications for the anticipated purchase of a specific item or purchase.
- (4) (A) The governing body is authorized to pay a reasonable fee to the reverse Internet auction vendor.
- (B) The fee may be included as part of the bids received during the reverse Internet auction and paid by the winning bidder or paid separately by the governing body.
- (5) The governing body retains the right to:
- (A) Refuse all bids made during the reverse Internet auction; and
 - (B) Begin the reverse Internet auction process anew if the governing body determines it is in the best interest of the city or town.
- (d) For purposes of this section:
- (1) "Reverse Internet auction" means an Internet-based process in which bidders:
 - (A) Are given specifications for items and services being sought for purchase by a municipality; and
 - (B) Bid against one another in order to lower the price of the item or service to the lowest possible level; and
 - (2) "Reverse Internet auction vendor" means an Internet-based entity that hosts a reverse Internet auction.

HISTORY: Acts 1959, No. 28, § 5; 1979, No. 154, § 1; 1985, No. 745, § 3; A.S.A. 1947, § 19-4425; Acts 1995, No. 812, § 1; 2001, No. 508, § 1; 2005, No. 1435, § 2; 2005, No. 1957, § 1; 2009, No. 756, § 24.

14-58-305. Payment of claims.

- (a) In a city of the first class, the mayor or his duly authorized representative may approve for payment out of funds previously appropriated for that purpose, or disapprove, any bills, debts, or liabilities asserted as claims against the city.

(b) The municipal governing body shall, by ordinance, establish in that connection a maximum amount, and the payment or disapproval of such bills, debts, or liabilities exceeding that amount shall require the confirmation of the governing body.

HISTORY: Acts 1959, No. 28, § 6; A.S.A. 1947, § 19-4426.

14-58-104. Specific purchases and contracts.

(a) The municipal governing body of a city of the first class, city of the second class, or an incorporated town may purchase the following commodities without soliciting bids:

(1) Motor fuels, oil, asphalt, asphalt oil, and natural gas; and

(2) New motor vehicles from a motor vehicle dealer licensed under the Arkansas Motor Vehicle Commission Act, § 23-112-101 et seq., if the motor vehicle is purchased for an amount not to exceed the fleet price awarded by the Office of State Procurement and in effect at the time the municipal governing body of a city of the first class, city of the second class, or an incorporated town submits the purchase order for the same make and model motor vehicle.

(b) The municipal governing body of a city of the first class, city of the second class, or an incorporated town may renew or extend the term of an existing contract without soliciting bids.

HISTORY: Acts 2009, No. 756, § 23.

Arkansas Constitution, Article 12 § 5.

Political subdivisions not to become stockholders in or lend credit to private corporations.

No county, city, town or other municipal corporation, shall become a stockholder in any company, association, or corporation; or obtain or appropriate money for, or loan its credit to, any corporation, association, institution or individual.

SALE OF ASSETS LAW

14-58-306. Disposal of municipal supplies, etc.

(a) In a city of the first class, city of the second class, or incorporated town, the mayor or his or her authorized representative may sell or exchange any municipal supplies, materials, or equipment with a value of twenty thousand dollars (\$20,000) or less, unless the municipal governing body shall, by ordinance, establish a lesser amount.

(b) No item or lot of supplies, material, or equipment that is to be disposed of as one (1) unit shall be sold without competitive bidding if the amount exceeds twenty thousand dollars (\$20,000) or the maximum provided by ordinance, unless the mayor shall certify in writing to the governing body that, in his or her opinion, the fair market value of the item or lot is less than the amount established by ordinance as indicated.

(c) (1) If an item of personal property belonging to a municipality becomes obsolete or is no longer used by a municipality, it may be:

(A) Sold at public or Internet auction;

(B) Sent to the Marketing and Redistribution Section of the Office of State Procurement of the Department of Finance and Administration; or

(C) Transferred to another governmental entity within the state.

(2) If an item is not disposed of under subdivision (c)(1) of this section, the item may be disposed of in the landfill used by the municipality if the mayor or his or her authorized representative certifies in writing and the governing body of the municipality approves that it has:

(A) Been rendered worthless by damage or prolonged use; or

(B) (i) Only residual value; and

(ii) Been through public auction and not sold.

(d) (1) A record shall be maintained of all items disposed of and reported to the governing body.

(2) The municipal fixed asset listing shall be amended to reflect all disposal of property made under this section.

HISTORY: Acts 1959, No. 28, § 7; A.S.A. 1947, § 19-4427; Acts 2007, No. 661, § 1; 2011, No. 622, § 2.

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)
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)
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 (ACOOP) provides a methodology, hardware, software, training, and user assistance for the development, maintenance, and testing of disaster recovery plans for Arkansas agencies, boards, commissions, school districts, counties, and cities. These plans are intended to ensure that essential services continue to be provided after any disruptive event.

For more information, 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

**CITY/TOWN OF SAMPLE, ARKANSAS
FIXED ASSET LISTING
YEAR ENDING 12/31/2013**

Appendix B

<u>Description</u>	<u>Acquisition Date</u>	<u>Property No.</u>	<u>Serial No.</u>	<u>Amount</u>
<u>Land</u>				
Lot 5, Section C	7/2/71			\$ 5,000
<u>Buildings</u>				
City Hall	7/2/71			\$ 54,257
Fire Station	10/24/81			26,482
TOTAL BUILDINGS				<u>\$ 80,739</u>
<u>Motor Vehicles</u>				
<u>General</u>				
1991 Chevy Truck	7/6/05		BR549	\$ 10,502
<u>Fire</u>				
1984 Pumper	12/14/07		V187K816G987	35,864
1972 Fire Truck	8/18/97		V1357M751R321	9,762
				<u>45,626</u>
TOTAL MOTOR VEHICLES				<u>\$ 56,128</u>
<u>Equipment</u>				
<u>General</u>				
Dell Computer	9/14/08		CW12589KL654	\$ 2,500
Power Washer	12/19/10		WKR325	2,764
				<u>\$ 5,264</u>
<u>Fire</u>				
Jaws of Life	4/1/12		682RDL937	\$ 2,534
TOTAL EQUIPMENT				<u>\$ 7,798</u>
TOTAL FIXED ASSETS				<u><u>\$ 149,665</u></u>

Note: A list of deletions and additions must be maintained in order to reconcile beginning balance to ending balance. Beginning balance of the current year (or ending balance of the previous year) plus additions less deletions should equal ending balance of the current year.

**CITY/TOWN OF SAMPLE, ARKANSAS
GENERAL FUND
CASH RECEIPTS JOURNAL
YEAR ENDING 12/31/2013**

Appendix C

<u>Date</u>	<u>Receipt Number</u>	<u>Received from</u>	<u>Total</u>	<u>State Aid</u>	<u>Federal Aid</u>	<u>Property Taxes</u>	<u>Sales Taxes</u>	<u>Franchise Taxes</u>	<u>Fines, Forfeitures and Costs</u>	<u>Local Permits and Fees</u>	<u>Other</u>
1/2/13	1001	State of Arkansas	\$ 3,500.00	\$ 3,500.00							
1/3/13	1002	County	2,432.15			\$ 2,432.15					
1/4/13	1003	District Court	1,436.78						\$ 1,436.78		
1/8/13	1004	State of Arkansas	3,427.64				\$ 3,427.64				
1/9/13	1005	Entergy	485.98					\$ 485.98			
1/10/13	1006	John Doe	75.00							\$ 75.00	
1/17/13	1007	US Dept of Justice	10,000.00		\$ 10,000.00						
1/18/13	1008	Centerpoint/Arkla	376.25					376.25			
1/18/13	1009	Jan Doe	15.00								\$ 15.00
1/18/13	1010	District Court	1,567.38						1,567.38		
		Monthly Totals	<u>23,316.18</u>	<u>3,500.00</u>	<u>10,000.00</u>	<u>2,432.15</u>	<u>3,427.64</u>	<u>862.23</u>	<u>3,004.16</u>	<u>75.00</u>	<u>15.00</u>
		Year-to-date Totals	<u>\$ 23,316.18</u>	<u>\$ 3,500.00</u>	<u>\$ 10,000.00</u>	<u>\$ 2,432.15</u>	<u>\$ 3,427.64</u>	<u>\$ 862.23</u>	<u>\$ 3,004.16</u>	<u>\$ 75.00</u>	<u>\$ 15.00</u>

**CITY/TOWN OF SAMPLE, ARKANSAS
GENERAL FUND
CASH DISBURSEMENTS JOURNAL
YEAR ENDING 12/31/2013**

Date	Check Number	Payee	Total	Mayor's Office					Police Department					
				Personal Services	Supplies	Other Services & Charges	Capital Outlay	Debt Service	Personal Services	Supplies	Other Services & Charges	Capital Outlay	Debt Service	
1/2/13	2001	AT&T	\$ 381.25			\$ 257					\$ 124			
1/3/13	2002	Regions Bank	651.49											\$ 651
1/4/13	2003	Bill's Police Supply	125.32							\$ 125				
1/8/13	2004	Smith Chevrolet	25,432.97									\$ 25,433		
1/9/13	2005	Payroll Account	3,736.23	\$ 1,368					\$ 2,368.58					
1/10/13	2006	Farmer's & Merchants Bank	323.85											323.85
1/17/13	2007	Entergy	221.15			100.58					120.57			
1/18/13	2008	Wal-Mart	26.35		\$ 26									
1/24/13	2009	Payroll Account	3,860.33	1,367.65					2,492.68					
1/30/13	2010	Centerpoint/Arkla	437.63			153.28					284.35			
		Monthly Totals	35,196.57	2,735.30	26.35	510.75	-	-	4,861.26	125.32	529.28	25,432.97	975.34	
		Year-to-date Totals	\$ 35,196.57	\$ 2,735.30	\$ 26.35	\$ 510.75	\$ -	\$ -	\$ 4,861.26	\$ 125.32	\$ 529.28	\$ 25,432.97	\$ 975.34	

Note: Arkansas Code Ann. 14-59-111 states that classifications of expenditures shall include the major type of expenditures (Personal Services, Supplies, etc.) by department (Mayor, Clerk, Treasurer, Police, Fire, etc.). Only 2 departments are shown above for illustrative purposes.

MUNICIPAL DEPARTMENT CLASSIFICATIONS

Appendix E

General Government

Mayor's office	0100
City Clerk's office	0101
City Treasurer's office	0102
City Council	0103
City Attorney	0104
Planning Department	0105
Code Enforcement	0106
Computer Services	0107
Economic Development	0108
Advertising and Promotion	0109
Tourism	0110

Highways and Streets

Street Department	0200
-------------------	------

Law Enforcement

Police Department	0301
District/City Court	0302
Animal Control	0303
Dispatch	0304
Police Pension	0305
Judge and Clerk Retirement	0306
Drug Control	0307

Public Safety

Fire Department	0401
911	0402
Fire Pension	0403

Sanitation

Sanitation Department	0501
Landfill	0502
Recycling	0503

Health

Ambulance service	0601
Mosquito control	0602

Recreation and Culture

Parks and recreation	0701
Library	0702

Social Services

Senior Citizen's Center	0801
Cemetery	0802

Airport

Municipal Airport	0901
-------------------	------

1 State of Arkansas
2 90th General Assembly
3 Regular Session, 2015

A Bill

HOUSE BILL 1445

4
5 By: Representatives K. Ferguson, Blake

For An Act To Be Entitled

8 AN ACT TO AMEND THE LAW CONCERNING THE DUTIES OF A
9 MUNICIPAL TREASURER; AND FOR OTHER PURPOSES.

Subtitle

12 TO AMEND THE LAW CONCERNING THE DUTIES OF
13 A MUNICIPAL TREASURER.

10
11
14 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:

16
17 SECTION 1. Arkansas Code § 14-59-115(b)(2), concerning the duties of a
18 municipal treasurer, is amended to read as follows:

19 (2)(A)(i) If the municipal treasurer does not comply with ~~the~~
20 ~~provisions of~~ this chapter or requests that specific duties be assigned to
21 another employee or contracting entity, the governing body of a municipality
22 may assign specific duties outlined in this chapter to another employee, or
23 it may contract for ~~such~~ the services to be performed by a private, qualified
24 person or entity.

25
26 (ii)(a)(1) Before the governing body of a
27 municipality assigns or contracts with a person or entity for the disbursing
28 of funds, the governing body of a municipality shall establish by ordinance a
29 method that provides for internal accounting controls and documentation for
30 audit and accounting purposes.

31
32 (2) The municipal treasurer shall
33 approve the disbursement of funds before the private, qualified person or
34 entity disburses the funds.

35 (b) The governing body of a municipality shall
36 ensure that the person or entity is adequately insured and bonded and



1 conforms to best practices and standards in the industry.

2 (B)(i) The governing body of a municipality may not assign
3 duties relating to the collecting ~~or disbursing~~ of funds to anyone other than
4 an employee of the municipality.

5 (ii) The governing body of a municipality may assign
6 or contract with a private, qualified person or entity for the duties
7 relating to the disbursing of funds for payroll, bonded debt, or construction
8 projects funded with bond proceeds.

9
10
11 **APPROVED: 03/20/2015**
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36