

PREPARING FOR A LEGISLATIVE AUDIT

DIVISION OF LEGISLATIVE AUDIT



MAY 8, 2019

TABLE OF CONTENTS

	Page
Information about Legislative Audit.....	1
Records Necessary for an Audit.....	7
Budgeting Laws.....	10
Publishing Requirements Law.....	11
Segregation of Duties.....	12
Municipal Accounting Law.....	14
Municipal Ethics Law.....	26
Check Imaging Law.....	27
Purchasing Laws Generally.....	31
Purchase and Sale of Real and Personal Property.....	35
 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

Roger Norman, JD, CPA, CFE, CFF

Legislative Auditor

roger.norman@arklegaudit.gov

Marti Steel, CPA

Deputy Legislative Auditor

marti.steel@arklegaudit.gov

Tim Jones, CPA, CFF

Audit Manager

tim.jones@arklegaudit.gov

Field Audit Supervisors by District:

District 1:

Lance Woodworth, CPA

Field Audit Supervisor (Harrison)

(501) 683-8600 Ext. 1054

lance.woodworth@arklegaudit.gov

District 2:

Christy McCurry, CPA
Field Audit Supervisor (Waldron)
(501) 683-8600 Ext. 4421
christy.mccurry@arklegaudit.gov

District 3:

John Elser, CPA, CFE
Field Audit Supervisor (Ozark)
(501) 683-8600 Ext. 1050
john.elser@arklegaudit.gov

District 4:

Jimmy Garrett, CPA, CFF
Field Audit Supervisor (Little Rock)
(501) 683-8600 Ext. 1030
jimmy.garrett@arklegaudit.gov

District 5:

Duane Bowden, CPA
Field Audit Supervisor (Nashville)
(501) 683-8600 Ext. 4603
duane.bowden@arklegaudit.gov

District 6:

Theresa Outlaw, CPA, CFE
Field Audit Supervisor (Monticello)
(501) 683-8600 Ext. 4632
theresa.outlaw@arklegaudit.gov

District 7:

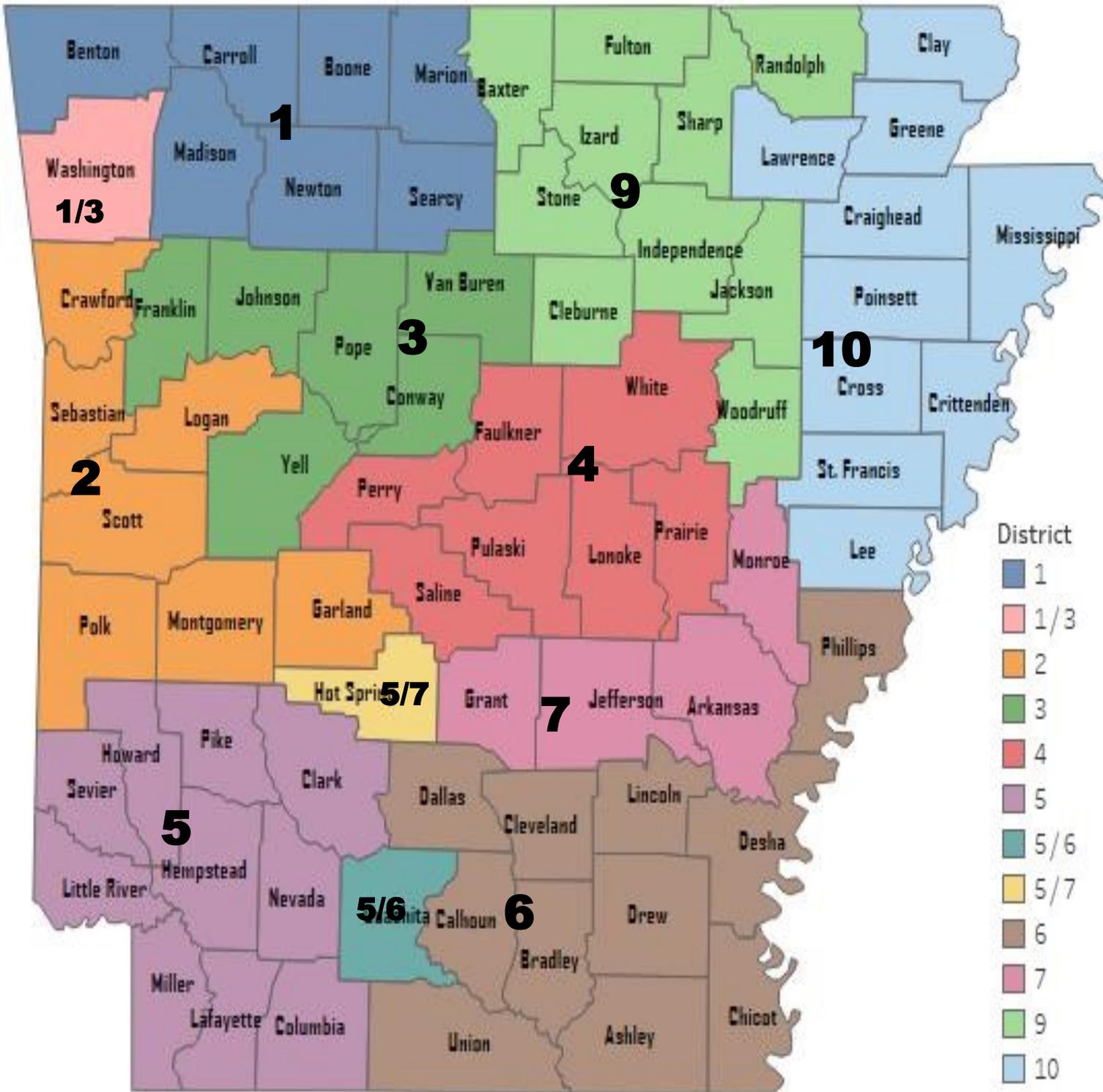
Joe Archer, CPA
Field Audit Supervisor (Sheridan)
(501) 683-8600 Ext. 4602
joe.archer@arklegaudit.gov

District 9:

Jessica Brown, CPA
Field Audit Supervisor (Batesville)
(501) 683-8600 Ext. 4503
jessica.brown@arklegaudit.gov

District 10:

Jeff McMillin, CPA, CFF
Field Audit Supervisor (Jonesboro)
(501) 683-8600 Ext. 4518
jeff.mcmillin@arklegaudit.gov



Supervisors:

- 1 – Lance Woodworth
- 2 – Christy McCurry
- 3 – John Elser
- 4 – Tim Thompson (ed), Jimmy Garrett
- 5 – Beth Gray (ed), Duane Bowden
- 6 – Paul McEachern (ed), Theresa Outlaw
- 7 – Joe Archer
- 9 – Jessica Brown
- 10 – Shannon Norris (ed), Jeff McMillin

LEGISLATIVE JOINT AUDITING COMMITTEE

The Legislative Joint Auditing Committee is responsible for the independent auditing of entities and political subdivisions of the State to furnish the General Assembly with information vital to the discharge of its constitutional duties. When the General Assembly is not in session, the full Committee meets on the second Friday of each month, with the three Standing Committees meeting on the preceding Thursday. For the purpose of reviewing audit reports, members of the Committee are assigned to the Standing Committee on State Agencies, the Standing Committee on Educational Institutions, and the Standing Committee on Counties and Municipalities.

The Legislative Joint Auditing Committee is made up of 44 members as follows:

- 16 Members selected by the Senate
- 20 Members selected by the House of Representatives
- President Tempore of the Senate, ex-officio
- Speaker of the House of Representatives, ex-officio
- Immediate past Co-Chairs of the Committee, ex-officio
- Co-Chairs and Co-Vice Chairs of the Legislative Council, ex-officio

2019-20 Co-Chairs – Senator Jason Rapert and Representative Richard Womack

2019-20 Co-Vice Chairs – Senator Eddie Cheatham and Representative DeAnn Vaught

ARKANSAS LEGISLATIVE AUDIT

The mission of Arkansas Legislative Audit is to serve the General Assembly, the Legislative Joint Auditing Committee, and the citizens of the State of Arkansas by promoting sound financial management and accountability of public resources entrusted to various governmental entities. To assist the Legislature in oversight of state and local government, Arkansas Legislative Audit is responsible for over 1,000 engagements, including audits, financial and compliance reports, and special reports. Arkansas Legislative Audit continually strives to promote an atmosphere of mutual trust, honesty, and integrity among its staff members, various governmental entities, and the people it is privileged to serve.

Arkansas Legislative Audit currently has 263 professional staff and 12 support staff. As of January 1, 2019 professional staff had achieved the following designations:

- 171 Certified Public Accountants (CPA)
- 51 Certified Fraud Examiners (CFE)
- 11 Certified in Financial Forensics (CFF)
- 10 Certified Information Systems Auditors (CISA)
- 3 Attorneys (JD)

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

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

Court reports

Ticket log

Court dockets

Time payment records

Monthly settlements

Completed ticket books

Records relating to the collection of hot checks

Printer's certificates for ticket 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

PERS records

Other miscellaneous records

Council minutes up to the present date

Pension Board minutes up to the present date

Six-month financial statements and proofs of publications

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 of budget.

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

Employee (1)	PAYROLL		DEPARTMENT	
	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 written policies and procedures to ensure that the electronic funds payment system provides for internal accounting controls and documentation for audit and accounting purposes; and

(C) Each electronic funds payment system established under this subsection shall comply with the information systems best practices 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; 2019, No. 138, § 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			\$.00
Dated			
Add:	Deposits in transit (Receipts recorded in Cash Receipts Journal not shown on this bank statement).		
<u>DATE</u>	<u>RECEIPTS NO.</u>	<u>AMOUNT</u>	
		\$.00	
		.00	
		<u>.00</u>	.00
Deduct:	Outstanding Checks (Checks issued and dated prior to date of bank statement per Cash Disbursements Journal not having yet cleared the bank).		
<u>CHECK NO.</u>	<u>PAYEE</u>	<u>AMOUNT</u>	
		\$.00	
		.00	
		<u>.00</u>	<u>.00</u>
RECONCILED BALANCE			<u>\$.00</u>

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)(i) If the municipal treasurer does not comply with 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 the services to be performed by a private, qualified person or entity.

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

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

(b) The governing body of a municipality shall ensure that the person or entity is adequately insured and bonded and conforms to best practices and standards in the industry.

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

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

HISTORY: Acts 1973, No. 159, § 13; A.S.A. 1947, § 19-5313; Acts 2001, No. 1062, § 5; 2011, No. 621, § 9; 2015, No. 582, § 1.

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 Arkansas Legislative Audit determines that a municipal treasurer is not substantially complying with this chapter, Arkansas Legislative Audit 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 Arkansas Legislative Audit to confirm that the municipal treasurer is not substantially complying with this chapter.

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

(b)(1) Upon notification of noncompliance by Arkansas Legislative Audit, 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, Arkansas Legislative Audit shall review the records to determine if the municipality substantially complies with this chapter.

(B) Arkansas Legislative Audit 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) Arkansas Legislative Audit 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 Arkansas Legislative Audit 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 Arkansas Legislative Audit to be in substantial compliance with this chapter.

(e)(1) If Arkansas Legislative Audit 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.

14-59-119 Debit card and credit card payments.

(a) A municipality may accept a legal payment and any associated costs through a debit card or credit card in accordance with applicable state and federal law.

(b)(1) A municipality may enter into a contract with a credit card or debit card company and pay any fee normally charged by the card or debit card company for allowing the municipality to accept the credit card or debit card as payment as authorized under subsection (a) of this section.

(2) When a payment is made through a credit card or debit card, the municipality shall assess a transaction fee equal to the amount charged to the municipality by the credit card or debit card company.

(3) A municipality shall not assess a transaction fee for payments made through a credit card or debit card if the governing body of the municipality determines that the transaction fee is included in the amount charged for the service or product for which a credit card or debit card payment is made.

HISTORY: Acts 2019, Nos. 195, § 1; 773, § 1.

MUNICIPAL ETHICS LAW

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

(a)(1) A council member or elected official of a municipal corporation, during the term for which he or she has been elected or one (1) year thereafter, shall not 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, council member, clerk, clerk-treasurer, recorder, or recorder-treasurer.

(2) A council member shall not be appointed to any municipal office, except in cases provided for in this subtitle, during the time for which he or she may have been elected.

(b)(1) A council member, official, or municipal employee shall not 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 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 does not apply to contracts for furnishing supplies, equipment, or services to be performed for a municipality by a corporation in which no 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 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; 2017, No. 879, § 11.

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. Definition.

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 Arkansas Legislative Audit.

(a) A financial institution desiring to provide public entities with images of canceled checks as provided in this subchapter shall provide a sample of imaged documents in one (1) or more of the following formats to Arkansas Legislative Audit for review.

- (1)** Stored on a CD-ROM or similar tangible digital media;
- (2)** Accessible through the internet; or
- (3)** On paper.

(b) Upon receipt of imaged documents submitted under subsection (a) of this section, Arkansas Legislative Audit shall immediately review and notify the financial institution whether or not the imaged documents are in compliance with this subchapter.

HISTORY: Acts 1999, No. 648, § 5; 2019 No. 255, § 1.

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

(a) After a financial institution has received written notification from Arkansas Legislative Audit that the submitted samples of its imaged documents under § 19-2-505 comply with this subchapter and upon agreement with the public entity, the financial institution may provide the public entity canceled check images in the format and quality approved by Arkansas Legislative Audit.

(b) The canceled check images of financial transactions provided to the public entity by the financial institution under this subchapter shall be legible and show both the front and back images of the canceled checks.

(c)(1) If a financial institution provides canceled check images on tangible digital media under this subchapter, 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)(A) If particular software is needed to view or search the digital images provided under this subchapter, the financial institution shall provide the software to the public entity and, upon request, to Arkansas Legislative Audit.

(B) Software provided under subdivision (c)(2)(A) of this section shall make canceled check images clear and readable.

(3) Before delivery of a CD-ROM or other tangible digital media to a public entity, a financial institution shall perform random verification of the legibility of the contents of the data.

(d)(1) If a financial institution provides canceled check images to a public entity through internet access to online banking documents under this subchapter, the financial institution may provide Arkansas Legislative Audit read-only internet access to the public entity's online banking documents.

(2) Read-only internet access granted under subdivision (d)(1) of this section shall permit viewing and copying of each public entity's bank statements, canceled check images,

deposit slips, and other financial transaction documentation made available to the public entity.

(3)(A) If particular software is needed to view or search images made available under this subsection, the financial institution shall provide the necessary software to the public entity and, upon request, to Arkansas Legislative Audit.

(B) Software provided under subdivision (d)(3)(A) of this section shall make canceled check images clear and readable.

(4) An online banking document made available to a public entity under this subsection shall be available for read-only internet access for at least five (5) years after the document is made available to the public entity online.

(e) If a financial institution provides canceled check images on paper under this subchapter, the images shall be of such clarity and size that the details may be read without the aid of a magnifying device.

(f)(1) If a financial institution provides canceled check images under this subchapter, 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 Arkansas 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 stored on tangible digital media, conforming to the digital imaging specifications stated in this subchapter, to Arkansas Legislative Audit on a monthly basis;

(D) The provision to Arkansas Legislative Audit of read-only internet access to the public entity's online banking documents in accordance with the requirements of this subchapter; or

(E) Any other authenticating method approved by Arkansas Legislative Audit.

(2) A financial institution may elect which of the procedures listed in subdivision (f)(1) of this section it shall implement to provide authentication of images relating to the accounts of each public entity.

(g) A financial institution shall be able to, and, at the request of Arkansas Legislative Audit, shall provide duplicate copies of any checks and statements delivered to a public entity:

(1) With the same clarity and size as the imaged documents previously delivered; and

(2) In the format requested by Arkansas Legislative Audit if the format is currently available to the financial institution.

HISTORY: Acts 1999, No. 648, § 6; 2019 No. 255, § 1.

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 Arkansas 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 Arkansas 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 Arkansas Legislative Audit.

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

(d) Any cost associated with providing this information to Arkansas 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) Cities of the first class, cities of the second class, and incorporated towns may accept competitive bids in the following forms:

(i) Written; or

(ii) Electronic media.

(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; 2017, No. 170, § 2.

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.

Ark. Const. Art. 12, § 5 (2017)

§ 5. Political subdivisions not to become stockholders in or lend credit to private corporations -- Exceptions.

(a) 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.

(b) However, a county, city, town, or other municipal corporation may obtain or appropriate money for a corporation, association, institution, or individual to:

(1) Finance economic development projects; or

(2) Provide economic development services.

(c) As used in this section:

(1) "Economic development projects" means the land, buildings, furnishings, equipment, facilities, infrastructure, and improvements that are required or suitable for the development, retention, or expansion of:

(A) Manufacturing, production, and industrial facilities;

(B) Research, technology, and development facilities;

(C) Recycling facilities;

(D) Distribution centers;

- (E)** Call centers;
- (F)** Warehouse facilities;
- (G)** Job training facilities; and
- (H)** Regional or national corporate headquarters facilities;

(2) "Economic development services" means:

(A) Planning, marketing, and strategic advice and counsel regarding job recruitment, job development, job retention, and job expansion;

(B) Supervision and operation of industrial parks or other such properties; and

(C) Negotiation of contracts for the sale or lease of industrial parks or other such properties; and

(3) "Infrastructure" means:

(A) Land acquisition;

(B) Site preparation;

(C) Road and highway improvements;

(D) Rail spur, railroad, and railport construction;

(E) Water service;

(F) Wastewater treatment;

(G) Employee training which may include equipment for such purpose; and

(H) Environmental mitigation or reclamation.

(d) The General Assembly, by a three-fourths vote of each house, may amend the provisions of subsections (b) and (c) of this section so long as the amendments are germane to this section and consistent with its policy and purposes. [As amended by Const. Amend. 97.]

PURCHASE AND SALE OF REAL AND PERSONAL PROPERTY

14-54-302. Purchase, lease, and sale authorized.

(a) A municipality may:

(1) Sell, convey, lease, rent, let or dispose of any real estate or personal property owned or controlled by the municipality, including real estate or personal property that is held by the municipality for public or governmental purposes;

(2) Buy any real estate or personal property; and

(3)(A) Donate real estate or personal property, or any part of the real estate or personal property, to the United States Government or any agency of the United States Government, for any one (1) or more of the following purposes, that is, having the real estate or personal property, or both, activated, reactivated, improved, or enlarged by the donee.

(B) The municipality may donate the fee simple title and absolute interest, without any reservations or restrictions, in and to all real estate or personal property, or both, or any part of the real estate or personal property, to the United States Government, if this real estate or personal property was previously conveyed or otherwise transferred by the United States Government to the municipality without cost to the municipality.

(C) All other donation instruments shall contain provisions by which the title to the property donated shall revert to the municipality when the donated property is no longer used by the donee for the purposes for which it was donated.

(b) The execution of all contracts and conveyances and lease contracts shall be performed by the mayor and city clerk or recorder, when authorized by a resolution in writing and approved by a majority vote of the governing body of the municipality present and participating.

(c) The mayor or his or her authorized representative may sell or exchange any municipal personal property with a value of twenty thousand dollars (\$20,000) or less, unless the governing body of the municipality shall by ordinance establish a lesser amount.

(d) Municipal personal property to be disposed of as one (1) unit shall not be sold without competitive bidding if the amount exceeds twenty thousand dollars (\$20,000) or the maximum provided by resolution, unless the mayor certifies in writing to the governing body of the municipality that in his or her opinion the fair market value of the item or lot is less than the amount established by ordinance.

(e)(1) If personal property of the municipality becomes obsolete or is no longer used by a municipality, the personal property 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;

(C) Transferred to another governmental entity within the state; or

(D) Donated under this section.

(2) If an item of personal property is not disposed of under subdivision (e)(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:

(A) The item has been rendered worthless by damage or prolonged use; or

(B) The item has:

(i) Only residual value; and

(ii) Been through public auction and not sold.

(f)(1) A record shall be maintained of all items of personal property disposed of under this section and reported to the governing body of the municipality.

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

HISTORY: Acts 1935, No. 176, § 2; Pope's Dig., § 9539; Acts 1953, No. 13, § 1; 1959, No. 159, § 1; 1977, No. 823, § 1; 1983, No. 183, § 2; A.S.A. 1947, § 19-2310; Acts 2005, No. 436, § 1; 2017, No. 470, § 1; 2019, No. 575, § 1.

APPENDIX A

Arkansas Legislative Audit

Information Systems Best Practices



TABLE OF CONTENTS

	Page
PURPOSE.....	1
Internal Controls.....	1
Assessing Risk.....	1
Monitoring	1
INTRODUCTION.....	2
Part One: General Controls.....	2
Part Two: Application Controls	2
Part Three: Other Technology	2
BEST PRACTICES – GENERAL CONTROLS	3
IS Management.....	3
Contract/Vendor Management.....	4
Network Security.....	4
Wireless Networking Security	5
Physical Access Security.....	6
Logical Access Security.....	7
Disaster Recovery/Business Continuity	8
BEST PRACTICES – APPLICATION CONTROLS	9
Data Input	9
Data Processing	9
Data Output	10
Application-Level General Controls	11
Application Security Management	11
Application Configuration Management.....	11
Segregation of Duties	12
Application Contingency Planning	12
BEST PRACTICES – OTHER TECHNOLOGY.....	13
Electronic Signatures and Digital Signatures.....	13
Payment Cards (Debit or Credit).....	13
Bring Your Own Device (BYOD).....	13
Electronic Banking.....	14

PURPOSE

Arkansas Legislative Audit (ALA) establishes the following Information System (IS) Best Practices, utilized throughout industry and government, to provide practical information about internal controls and encourage entities to develop, implement, and maintain IS policies and procedures that conform to current best practices. ALA recommends entity management conduct a risk assessment and rely on the results of the assessment to establish which best practices are appropriate for their environment. Since each situation is unique, management should utilize these guidelines as a self-monitoring tool to understand, assess, and mitigate potential information security risks to the entity's operations and assets. These best practices should be used as a resource to improve the design of existing internal controls and to implement new policies and procedures required by changes in risk to assets and operations. These best practices **are not all-inclusive**, nor are they a replacement for locally developed internal control policies and procedures. Optimally, control policies and procedures should be described in a written document and distributed to all employees since the application of these control procedures is every employee's responsibility. Successful internal controls depend on management and staff commitment to the protection of resources.

Internal Controls

It is management's responsibility to ensure that the right controls are in place and that they are performing as intended. Therefore, internal controls are necessary for the effective and efficient operation of all levels of government. Internal controls are policies or procedures put in place to provide reasonable assurance that operations are achieving stated objectives. Properly designed and functioning controls help an entity adjust to ever-changing situations, changing demands, and varying threats and reduce the likelihood that significant errors or fraud will occur and remain undetected.

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

To execute responsibilities effectively, management needs to understand how an integrated internal control framework should work. Standards for Internal Control in the Federal Government "Green Book" (which may be found at <https://www.gao.gov/products/D08784>) may also be adopted by state and local governmental entities.

Assessing Risk

Each governmental entity has its own unique set of circumstances and risks that affect the design and implementation of internal controls. Before determining which controls should be implemented, entities should conduct a risk assessment to identify, analyze, and respond to risk potential, fraud, or errors occurring and remaining undetected.

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

Monitoring

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

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

INTRODUCTION

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

Part One: General Controls

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

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

Part Two: Application Controls

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

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

Part Three: Other Technology

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

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

BEST PRACTICES – GENERAL CONTROLS

IS Management

- 1-1: IS management must ensure adequate internal controls are in place to achieve the organization's established goals and objectives.**
- 1-1.1: Develop an IS Department organizational chart, and update it as the environment changes.
 - 1-1.2: Conduct an overall risk assessment of the organization's goals, functions, and reputation to identify, monitor, and manage risks associated with the use of information technology. Gain an understanding of current practices in addressing these risks and mitigating negative impacts.
 - 1-1.3: Develop and maintain a formally-approved IS Operational Policy and Procedure Manual. The manual can be one document or several documents but should be reviewed and updated as the operating environment changes.
 - 1-1.4: Ensure that duties of software developers and IS operators are distinctly segregated and clearly documented.
 - 1-1.5: Develop policies and procedures addressing non-business use of entity equipment, facilities, and Internet services.
 - 1-1.6: Obtain proper replacement insurance for the production hardware/equipment.
 - 1-1.7: Develop and document database and network backup processes to include data and record retention periods, how often data are backed up, and how copies of backups will be maintained.
 - 1-1.8: Assign and communicate network backup responsibilities to designated staff.
 - 1-1.9: Establish access to an environmentally safe, secure off-site location to retain network backups.
 - 1-1.10: Establish and formally document frequency of backups, ensuring that minimum industry standards (i.e., daily, weekly, monthly, annually) are met. Backups should occur daily for critical processes or at longer intervals based on the significance of the information and rate of changes.
 - 1-1.11: Establish and formally document the method of backup:
 - a. Full Back up: All files and software.
 - b. Incremental Backup: Files that have changed since the previous backup.
 - c. Differential Backup: All the data that have changed since the last full backup.
 - d. Mirror Backup: Straight copy of the selected folders and files at a given instant in time.
 - 1-1.12: Ensure that the selected backup process and retention policy are in compliance with laws and regulations. Retention policy may include retaining periodic snapshots of all data backups in the event data become corrupted and contaminate the backup.
 - 1-1.13: Routinely copy operating system software, application software, hardware configurations, and production information to backup media based on frequencies set by management. This applies to all systems (e.g., local area network [LAN] or wide area network [WAN] servers, client/server database servers, special-purpose computers, etc.).
 - 1-1.14: Frequently test data backups to ensure data are restored and recoverable. Also, ensure backup settings are in compliance with entity policies.
 - 1-1.15: Ensure administrator/super user accounts are limited and properly approved.
 - 1-1.16: Regularly evaluate network availability and provide ongoing improvements to services and security as needed.

- 1-1.17: Establish and maintain a formal cybersecurity awareness program that ensures end users are aware of current cyber security threats the importance of protecting assets and the related risks.
- 1-1.18: Make employees aware of social engineering threats, which are attacks carried out by persuading authorized users or administrators to reveal confidential information to people they don't know over the phone or through emails from unknown parties. Employees should be trained to never open or download suspicious attachments.
- 1-1.19: Periodically host cybersecurity training for employees. Training may consist of table top discussions on cybersecurity or security policy review. Conduct relevant discussion and training on emerging cybersecurity threats, trending social engineering methods, and limiting the types of sensitive information collected, transported and stored. Discuss viruses, malware, and ransomware and the hazards of downloading email attachments, accessing malicious web sites, downloading files from the Internet, or simply clicking links embedded in emails that may appear reasonably valid.

Contract/Vendor Management

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

- 1-2.1: Conduct a risk assessment to identify risks associated with outsourcing IT services. Based on the results of the risk assessment, determine the appropriate course of action to respond to the identified risk.
- 1-2.2: Review all contract(s) prior to approval to ensure that business processes and any applicable legal requirements are adequately addressed and documented.
- 1-2.3: Involve end-users in the project.
- 1-2.4: Establish a Service Level Agreement for the maintenance and support of the contract, carefully defining specific performance expectations for each party.
- 1-2.5: Test the vendor's business processes for fitness and adequacy to gain assurance that network and application security controls are properly understood and established within the entity.
- 1-2.6: Confirm that the vendor is a going concern. Ensure that provisions are made to hold application source code in escrow.
- 1-2.7: Limit vendor access to entity resources, and document monitoring and evaluation of access reasons and results.
- 1-2.8: Vendors of cloud computing services or other types of hosted solutions should comply with ALA IS Best Practices and the State of Arkansas information security standards through service level agreements and contracts.
- 1-2.9: Prior to transferring data or application services to a cloud computing environment, it is vital to understand applicable laws, regulations, duties, and responsibilities imposed on both management and the vendor (e.g., data retention, data protection, jurisdictional issue, disclosures).

Network Security

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

- 1-3.1: Establish a security policy for the network that is clearly documented and formally approved. Ensure that policies describe potential security risks (identified in section 1-1.2) and are clearly communicated to users. Provide for monitoring of emerging security threats to ensure policies are kept current.
- 1-3.2: Ensure that network devices (e.g., firewalls, routers, etc.) are appropriately placed and configured to adequately protect both internal and external access to devices, applications, and services.

- 1-3.3: Limit physical and logical access to network devices (e.g., firewalls, routers, servers, etc.), and ensure that changes to these devices are properly managed. Establish policies for proper tracking, authorization, testing, and approval of changes.
- 1-3.4: Obtain anti-virus, anti-malware, and advanced persistent threats software and provide for their continued use. Ensure programs are set for automatic updates, and scan devices on an established schedule. Also, scan any media that is inserted into hardware (e.g., USB and external hard drives). Ensure that the network security policy covers use of external devices (e.g., USB drives, Smart Devices, etc.).
- 1-3.5: Establish a routine schedule for the performance and review of network vulnerability scanning, including documentation of critical risks identified and addressed.
- 1-3.6: Conduct a risk assessment to identify risks associated with allowing remote access to entity resources. Gain an understanding of current practices for addressing these risks and mitigating negative impacts.
- 1-3.7: Develop remote access authentication policies and procedures and encryption protocols (considering the risks identified above). Consider the use of virtual private networking (VPN) technology. Include procedures for usage restrictions, configuration/connection requirements, implementation guidance for each type of remote access allowed, and monitoring and handling of questionable activity.
- 1-3.8: Establish encryption methods for sensitive data transmitted externally and across the network, including procedures for keeping protocols current.
- 1-3.9: Ensure that all IT administration duties outsourced to a vendor are evaluated for risks associated with vendor access to your network and that vendor access is restricted only to files and applications needed to perform its duties. The contract with the vendor should provide that the vendor agrees to perform services in compliance with the entity's security policies and legal requirements.
- 1-3.10: Ensure operating systems are set to automatic updates. Turning off or rebooting computers regularly supports the installation of updates and refreshes system resources. Updates and patches for server operating systems are critical and should be reviewed and updated on a regular schedule.

Wireless Networking Security

- 1-4: Wireless security provides a secure network connection to prevent harm to the network and inappropriate access to resources.**
- 1-4.1: Conduct a risk assessment to identify risks associated with the use of wireless networking. Gain an understanding of current practices for addressing these risks and mitigating negative impacts.
- 1-4.2: Establish security policies and procedures that ensure wireless usage restrictions, configuration, connection and password requirements, and implementation guidance for wireless access are authorized and protected. Address the use of wireless technology to ensure compliance with IEEE 802.11i Security Standard. Document policies to include the risks (identified above) associated with this technology, and ensure that policies are clearly communicated to users.
- 1-4.3: Ensure that the Administrator credentials and Service Set Identifier (SSID) are changed from the default value and a naming convention that excludes all identifiable information about the entity and the technology in use. The SSID name should be communicated to entity employees.
- 1-4.4: Establish routine application of security patches for wireless access devices, ensuring that upgrades are applied as released.
- 1-4.5: Maintain an inventory of authorized access points (APs) and periodically conduct site inspections to determine that no unauthorized APs are in use.
- 1-4.6: Establish physical access controls over wireless devices to prevent unauthorized access, such that wireless devices are secured with locking mechanisms or kept in a restricted area where access is granted to authorized personnel only.

- 1-4.7: Review perimeter (external) security established in section 1-3.2, and ensure that the risks identified for wireless networking (see section 1-4.1) are adequately addressed in the placement and configuration of network devices.
- 1-4.8: 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 and access that is no longer necessary is terminated timely
- 1-4.9: Ensure that entity-approved guest access allows users access to only the Internet, requires guest users to agree to terms of use, and states that user activity on the wireless network is monitored.

Physical Access Security

- 1-5: Physical access security controls are implemented to protect system resources and the facilities used to support their operation.**
- 1-5.1: Develop a Physical Access Security Policy based on criticality of network devices and their physical placement. The policy should include access key/keycard management; authorization procedures for visitors, new employees, contractors, etc.; and provisions for cessation of access for terminated employees, consultants, security professionals, etc.
- 1-5.2: Ensure that the server room is adequately segregated from user areas and located in a discreet area inaccessible to outsiders and restricted to authorized personnel.
- 1-5.3: Ensure that data processing areas are properly segregated from public access and restricted to authorized personnel. Any devices that contain data should be physically secured in a locked room, cage, or other secure area.
- 1-5.4: Implement the following physical security controls:
 - a. Entrance and exit controls.
 - b. Visitor escorting.
 - c. Vendor escorting.
 - d. Logging of entry and exit dates and times.
 - e. Surveillance cameras.
- 1-5.5: Implement the following environmental controls, where possible:
 - a. Fire suppression system.
 - b. Smoke detector.
 - c. Temperature/Humidity detector.
 - d. Uninterruptible power supply (UPS).
 - e. Emergency power generator.
 - f. Raised floor.
 - g. Water detection.
- 1-5.6: Conduct a key/keycard inventory to identify those with physical access to facilities and to determine that terminated employee access has been properly removed. If unauthorized access exists, rekey doors, and change security codes to establish proper authentication. Develop specific procedures to ensure that terminated employee access is immediately disabled and to control issuance/revocation of access keys/keycards.
- 1-5.7: Develop a monitoring system for physical access, ensuring that access violations are detected and that both violations and corrective actions are documented.
- 1-5.8: Ensure that any data storage device, workstations, or other mobile equipment no longer in operation are reformatted/wiped based on current data sanitization methodologies or the hard drive physically destroyed to minimize the risk of exposure. Any paper documents containing personally identifiable information that are no longer in use should be shredded to minimize the risk of exposure.

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

- 1-6.1: Develop and document a Logical Access Security Policy, based on identified risk areas, to protect high-risk system resources. The policy should establish user identification, authentication, and account control mechanisms as well as protect system administration tools and utilities from unauthorized access. Include provisions for monitoring of access security best practices to ensure policies remain current.
- 1-6.2: Establish user security access on the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned duties in accordance with the entity's business process and functions.
- 1-6.3: Establish security administration procedures that ensure proper authorization of changes and additions to user accounts, including periodic review of user access security by resource owners (e.g., elected officials, directors, or their designees) and investigation of questionable authorizations. Access to security administration and other sensitive system resources should be narrowly limited to only users with a documented business purpose; all unnecessary accounts (e.g., system/admin default, guest, terminated users, etc.) should be removed or disabled.
- 1-6.4: Ensure that, at a minimum, the following password parameters for logical security controls are required:
- a. User identification and password are required.
 - b. Users are systematically forced to change passwords on a periodic, recurring basis not more than 90 days.
 - c. Passwords are systematically required to be composed of a mixture of alpha and numeric characters and a minimum of 8 characters, with no repeating characters.
 - d. New users are forced by the system to change their initially assigned password.
 - e. A password history file systematically prevents reuse of at least the last five passwords.
 - f. The user account is locked after three unsuccessful logon attempts and remains locked until reset by an administrator or in a reasonable period of time.
 - g. Computer sessions timeout after a reasonable period of no activity, requiring user authentication to restore session.
 - h. Passwords are not revealed to anyone, including management, help desk personnel, security administrators, family members, or co-workers.
 - i. Management establishes and monitors user Activity Log/Audit Trail.

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

Note: Any deviations from established password best practices are evaluated on a case-by-case basis.

- 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.
- 1-6.6: Other technologies for user identification and authentication, such as biometrics (e.g., finger-print verification, signature verification) and use of hardware tokens (e.g., smart cards) are available and should be considered, if appropriate.
- 1-6.7: Systems using both user ID/password and ID/biometrics should enforce the same password parameters described at 1-6.4. Systems using ID/biometrics with password access disabled achieve the same level of security while eliminating physical credential and password management.

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

Disaster Recovery/Business Continuity

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

- 1-7.1: Document and approve a Disaster Recovery and Business Continuity Plan that, at a minimum, achieves the following:
- a. Ensures that disaster recovery roles and responsibilities are clearly defined.
 - b. Includes detailed technical instructions and procedures for restoring all critical systems (i.e., networking, operating system, and critical applications).
 - c. Identifies the alternate work/office location and the offsite backup storage facility.
 - d. Includes necessary contact information for employees, vendors, etc.
 - e. Includes manual operating procedures and resources to be used until IT operations are restored.
 - f. Includes application-level contingency planning (established in section 2.7).
 - g. Covers all systems and operational areas.
 - h. Been approved by appropriate governance.
- 1-7.2: Ensure that a copy of the Disaster Recovery/Business Continuity Plan is stored at the off-site backup location.
- 1-7.3: Ensure that the Disaster Recovery/Business Continuity Plan is relevant, addresses current risk, and is updated annually or as conditions and risk change.
- 1-7.4: Conduct and document annual testing of the Disaster Recovery/Business Continuity Plan to the fullest extent possible. Document in sufficient detail and evaluate test results, modifying the plan if necessary.

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

BEST PRACTICES – APPLICATION CONTROLS

Data Input

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

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

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

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

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

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

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

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

Data Processing

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

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

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

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

- 2-2.3: Establish input approval, and review policies and procedures. Management should have procedures in place to identify and correct any errors that occur during the data entry process. These procedures should reasonably assure that errors and irregularities are detected, reported, and corrected:
- Ensure that data input is done in a controlled manner (e.g., proper authorization controls exist, both systematic and manual).
 - Ensure that all data inputs have been processed and accounted for.
 - Identify and investigate missing or unaccounted for source documents or data input transactions.
 - Periodically review user error logs to evaluate the extent and status of data errors.
 - Require data exception resolution within a specific time period.
- 2-2.4: Establish procedures to ensure that periodic reconciliations are performed between subsidiary ledgers and the general ledger, to include exception handling.
- 2-2.5: Establish monitoring procedures to include the following:
- 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.

Data Output

- 2-3: Data output controls ensure the integrity and reliability of output information as well as the accuracy and timely distribution of all output produced.**
- 2-3.1: Based on risk assessment, establish necessary controls over data output (both automated and manual).
- 2-3.2: Develop procedures for system output and reporting to ensure the following:
- Consistency of content, format, 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 review should be performed periodically.
- 2-3.4: Establish procedures to ensure that output is in compliance with applicable laws and regulations and that legally required reporting is complete and accurate. Review system-generated outputs/reports to assure the integrity of production data and transaction processing. This review should be performed periodically.

Application-Level General Controls***Application Security Management***

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

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

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

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

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

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

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

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

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

Application Configuration Management

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

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

Segregation of Duties

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

- 2-6.1: Ensure that process owners have identified and documented incompatible activities and transactions based on identified business process and application security risks. Ensure that application security policies address these areas and that users are systematically prevented from executing incompatible transactions.
- 2-6.2: Small governments with less staff and limited resources have a reduced capacity to segregate duties. Therefore, it may not be practical or cost-effective to segregate conflicting duties in these cases, and compensating controls should be designed to reduce the risk of error or fraud not being detected. Confirm that user access to transactions or activities that have segregation of duties conflicts is appropriately controlled.
- a. Access to incompatible activities is assigned only when supported by a business need.
 - b. User access authorizations are frequently reviewed by management for segregation of duties conflicts, considering position and process changes and updating access to current job assignments.
 - c. Users with segregation of duties conflicts are documented, and their activity is monitored via transaction and audit logs.
 - d. Management retains documentation that segregation of duties risk has been mitigated through effective controls and monitoring.
 - e. Develop a segregation of duties grid by using the “roles and responsibilities” or security master report function within software applications wherever possible, and maintain a segregation of duties grid for all key business processes.

Application Contingency Planning

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

- 2-7.1: Determine mission-critical functions performed by the financial applications, documenting associated key data and programs. Identify the impacts of automated process disruption and maximum allowable outage times for each application, and establish recovery time objectives.
- 2-7.2: Set backup retention policy for each application based on recovery time objectives, ensuring that backup intervals retained support necessary restoration periods. Current application programs and data should be copied according to this policy and securely stored at a geographically distant off-site location.
- 2-7.3: Establish manual procedures for continuing operations during outage times for the critical functions identified in section 2-7.1. Incorporate the application-level contingency planning and procedures (including backup policy) into the organization’s Disaster Recovery Plan.
- 2-7.4: Provide for periodic testing of the application contingency planning to include documentation of test results and corrective actions (including resulting changes to the plan) to be incorporated into organization-wide Disaster Recovery Plan testing and planning.

BEST PRACTICES – OTHER TECHNOLOGY

Electronic Signatures and Digital Signatures

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

- 3-1.1: If electronic signatures or digital signatures are used, management must understand the technology and associated risks, develop and implement controls to address risks identified, and comply with applicable laws and regulations.
- 3-1.2: Resources include the following: Electronic Signatures in Global and National Commerce Act (15 USC 7001); Arkansas Electronic Records and Signatures Act (Ark. Code Ann. § 25-31-101); Uniform Electronic Transactions Act or UETA (Ark. Code Ann. § 25-32-101); and Arkansas Department of Information Systems Electronic Signature Standard SS-70-011.
- 3-1.3: Ensure that implementation of the electronic equivalent of a written signature, which can be recognized as having the same legal status as a written signature, provides adequate security. A digitized written signature can easily be copied from one electronic document to another, with no way to determine whether it is legitimate. Electronic signatures, on the other hand, are unique to the message being signed and will not verify if they are copied to another document.
- 3-1.4: A software application that creates a signature on checks and affixes the signature to the check should have an associated access control mechanism. The access control mechanism should only be known by the cash custodian.

Payment Cards (Debit or Credit)

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

- 4-1.1: If payment cards are accepted for payment, management must understand the technology and associated risks; develop and implement controls to address risks identified; and comply with applicable laws, regulations, and industry standards.
- 4-1.2: Develop and maintain written comprehensive policies and procedures that cover the process by which payment cards are accepted and payment card data are processed. Policies and procedures should include but are not limited to:
 - a. Segregation of duties.
 - b. Physical security.
 - c. Storage and transmission of payment card information.
 - d. Disposal of payment card information.
 - e. Employee criminal background checks.
 - f. Technology security policies and procedures.
 - g. Incident response plan.
- 4-1.3: Industry standards include credit card brands' compliance programs and the Payment Card Industry (PCI) Data Security Standards (DSS).

Bring Your Own Device (BYOD)

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

- 5-1.1: If BYOD is allowed, management must understand the technology and associated risks, develop and implement controls to address risks identified, and comply with applicable laws and regulations.
- 5-1.2: Ensure use of the device security features, such as a PIN, password/passphrase, and automatic lock to help protect the device when not in use.
- 5-1.3: Keep the device software up to date. Devices should be set to update automatically.

- 5-1.4: Activate and use encryption services and anti-virus protection if your device features such services. Install and configure tracking and/or wiping services, such as Apple's "Find My iPhone," Android's "Where's My Droid," or Windows' "Find My Phone," if the device has this feature.
- 5-1.5: Remove any entity information stored on your device, including deleting copies of attachments to emails, such as documents, spreadsheets, and data sets, as soon as you have finished using them.
- 5-1.6: Remove all entity information from your device and return it to the manufacturer's settings before you sell, exchange, or dispose of your device.
- 5-1.7: Promptly report to entity management if your device is lost or stolen or its security is compromised.
- 5-1.8: Establish a comprehensive BYOD policy that provides policies, standards, and rules of behavior for the use of personally-owned devices. These policies must be adhered to in order to access organizational resources.

Electronic Banking, Electronic Commerce and other Electronic Transfer of funds

- 6-1: Electronic banking and other electronic funds transfer (EFT) enables bank customers to perform account management and financial transactions over the Internet that directly, or indirectly, affect funds held by the bank. Despite security controls, there is no absolute way to guarantee the safety of online electronic transactions. Entities should research and understand the risk involved before commencing online electronic transactions.**
- 6-1.1: Develop comprehensive written policies and procedures for all electronic transactions (e-transactions), online banking, and EFT activities. Policies and procedures should include statutory and other legal requirements and responsibilities as well as, but not limited to:
 - a. Documentation of proper segregation of functions (i.e., initiator cannot be an approver, etc.).
 - b. Online banking and EFT activities that will be used.
 - c. Person(s) authorized to initiate e-transactions.
 - d. Person who approves e-transactions.
 - e. Person who transmits e-transactions.
 - f. Person who records e-transactions.
 - g. Person who reviews and reconciles e-transactions and how frequently reviews are performed.
 - h. Procedures for prompt removal or changes to access security for local and online access.
 - i. Documentation to support transaction is properly maintained for historical review and audit purposes.
- 6-1.2: Establish a dedicated "hardened" computer with only application/services loaded that are necessary to perform online banking transactions. This computer should not be used for any other purpose. In cases where a dedicated computer is not available, entities must be able to reduce online banking risks to an acceptable level through a combination of other controls.
- 6-1.3: Install on the computer antivirus, anti-spyware, and malware and adware detection software that is current and set to automatically update.
- 6-1.4: Ensure all updates and patches to software, operating systems, and hardware are installed timely.
- 6-1.5: Install firewalls and intrusion detection and prevention systems with continuous monitoring. Any unauthorized and/or suspicious behavior or traffic should be investigated and, if necessary, blocked using access control lists in conjunction with a firewall.
- 6-1.6: Employ multi-factor authentication such as tokens and digital certificates, require unique login ids and complex passwords, and ensure computers and browsers are not allowed to save passwords. Keep passwords confidential.
- 6-1.7: Limit Internet access to only business-related programs. Frequently delete browsing history, temporary Internet files, and cookies. In the event the system is compromised, any information captured will not be stolen by a hacker or malware program.
- 6-1.8: Check that the session is secure (minimum 128-bit SSL encryption) before undertaking any online banking.

- 6-1.9: Monitor and reconcile bank accounts daily (when feasible), review accounts for unauthorized or suspicious activity, and report any suspicious activity immediately.
- 6-1.10: Ensure written agreements with banks and/or other payment solutions are reviewed by legal counsel.
- 6-1.11: Ensure written agreements with banks provide appropriate controls for all electronic or wire transfers.
- 6-1.12: Ensure computer is disconnected from the Internet by unplugging the Ethernet/DSL cable when not in use.
- 6-1.13: Employ dual-authorization of transactions, enforced by bank security where possible (requiring at least two user accounts to submit and approve electronic transactions).
- 6-1.14: Disallow online account management functions (such as adding users or modifying user security). Account changes should be conducted in person, or at least in writing, with the bank.
- 6-1.15: When possible, implement use of out-of-band transaction verification (such as text message or other security message to an approver with the entity). Take advantage of other system alerts including:
 - a. Balance alerts.
 - b. Transfer alerts.
 - c. Password change alerts.
 - d. Login failure alerts.
- 6-1.16: Ensure that blank check stock, card stock, signature stamps, and facsimile signatures are properly safeguarded with inventory control.
- 6-1.17: Use a clearing bank account when paying electronically rather than paying directly from primary account.
- 6-1.18: Establish transaction and daily limits to lower loss potential.
- 6-1.19: Consider the cost benefit of cybersecurity or fraud insurance.
- 6-1.20: Restrict browser(s) to sites necessary for EFT.
- 6-1.21: Ensure that users performing banking transactions use only non-administrative user accounts.
- 6-1.22: Implement use of fraud controls, when possible and feasible, to ensure that the bank only processes authorized transactions it has been instructed to perform, Features to consider:
 - a. Positive Pay.
 - b. ACH Positive Pay.
 - c. ACH Debit Block and Debit Filters.
 - d. Direct Deposit.
- 6-1.23: Implement use of processing calendar with the bank, if possible, to ensure the bank only processes transactions on pre-established days throughout the year.
- 6-1.24: Comply with all security requirements outlined in the service level agreement with the bank and all other prudent security measures.
- 6-1.25: Allow electronic delivery of statements and account information. Ensure any paper statements or documents containing account information are properly secured or destroyed.
- 6-1.26: Never share any confidential information, tax IDs, Social Security numbers, or account numbers via email.

**CITY/TOWN OF SAMPLE, ARKANSAS
FIXED ASSET LISTING
YEAR ENDING 12/31/2019**

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		WKRP325	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 12/31/2019**

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>
1/2/19	1001	State of Arkansas	\$ 3,500.00	\$ 3,500.00							
1/3/19	1002	County	2,432.15			\$ 2,432.15					
1/4/19	1003	District Court	1,436.78						\$ 1,436.78		
1/8/19	1004	State of Arkansas	3,427.64				\$ 3,427.64				
1/9/19	1005	Entergy	485.98					\$ 485.98			
1/10/19	1006	John Doe	75.00							\$ 75.00	
1/17/19	1007	US Dept of Justice	10,000.00		\$ 10,000.00						
1/18/19	1008	Centerpoint/Arkla	376.25					376.25			
1/18/19	1009	Jan Doe	15.00								\$ 15.00
1/18/19	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 12/31/2019**

Appendix D

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
1/2/19	2001	AT&T	\$ 381.25			\$ 257					\$ 124		
1/3/19	2002	Regions Bank	651.49										\$ 651
1/4/19	2003	Bill's Police Supply	125.32						\$ 125				
1/8/19	2004	Smith Chevrolet	25,432.97									\$ 25,433	
1/9/19	2005	Payroll Account	3,736.23	\$ 1,368					\$2,368.58				
1/10/19	2006	Farmer's & Merchants Bank	323.85										323.85
1/17/19	2007	Entergy	221.15			100.58					120.57		
1/18/19	2008	Wal-Mart	26.35		\$ 26								
1/24/19	2009	Payroll Account	3,860.33	1,367.65					2,492.68				
1/30/19	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	<u>\$35,196.57</u>	<u>\$2,735.30</u>	<u>\$ 26.35</u>	<u>\$ 510.75</u>	<u>\$ -</u>	<u>\$ -</u>	<u>\$4,861.26</u>	<u>\$125.32</u>	<u>\$ 529.28</u>	<u>\$25,432.97</u>	<u>\$975.34</u>

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.

EXAMPLE MUNICIPAL FUND CODES

Appendix E

GENERAL	1000
STREET	2000
<u>SPECIAL REVENUE FUNDS</u>	
LOCAL POLICE AND FIRE RETIREMENT	3001
FIRE EQUIPMENT AND TRAINING - ACT 833	3002
<u>CAPITAL PROJECTS FUNDS</u>	
CITY HALL CONSTRUCTION	4001
<u>DEBT SERVICE FUNDS</u>	
SALES TAX BOND	5001
<u>AGENCY FUNDS</u>	
POLICE BOND AND FINE	6001
DISTRICT COURT	6002
<u>ENTERPRISE FUNDS</u>	
LANDFILL	7001
<u>TRUST FUNDS</u>	
NONUNIFORM	8001
POLICE	8002
FIRE	8003

MUNICIPAL DEPARTMENT CLASSIFICATIONS

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
-------------------	------

EXAMPLE CHART OF ACCOUNTS

ASSETS	1000
Cash	1010
Investments	1020
Accounts receivable	1030
Interfund receivables	1040
LIABILITIES	2000
Accounts payable	2010
Interfund payable	2020
Settlements pending	2030
FUND BALANCE	3000
Nonspendable	3100
Restricted	3200
Committed	3300
Assigned	3400
Unassigned	3500
REVENUES	4000
State aid	4100
Federal aid	4200
Property taxes	4300
Franchise fees	4400
Sales taxes	4500
Fines, forfeitures, and costs	4600
Interest	4700
Local permits and fees	4800
Sanitation fees	4900
Gas and oil company reimbursements	4910
Other	4950
EXPENDITURES	
Personal services	5000
Supplies	6000
Other services and charges	7000
Capital outlay	8000
Debt service	9000
OTHER FINANCING SOURCES (USES)	0000
Transfers in	0100
Contribution from water department	0110
Transfers out	0150
Contribution to water department	0200

EXAMPLE MUNICIPAL EXPENDITURE CODES CHART

PERSONAL SERVICES - Amounts paid to both permanent and temporary government employees, including personnel substituting for those in permanent positions. This category includes gross salary for personal services rendered while on the payroll of the government and amounts paid by the government on behalf of employees; these amounts are not included in the gross salary, but are in addition to that amount. Such payments are fringe benefits payments and, although not paid directly to employees, are a part of the cost of personal services.

5001	Salaries, Full-Time
5002	Salaries, Part-Time
5003	Extra Help
5004	Contract Labor
5005	Overtime and Other Premium Compensation
5006	Social Security Matching
5007	Retirement Matching
5008	Noncontributory Retirement
5009	Health Insurance Matching
5010	Workmen's Compensation
5011	Unemployment Compensation
5012	Other Fringe Benefits
5013	Car Allowance
5014	Cobraserv
5015	Uniform Allowance
5016	Life Insurance

SUPPLIES - Amounts paid for items that are consumed or deteriorated through use or that lose their identity through fabrication or incorporation into different or more complex units or substances.

SUPPLIES

6001	General Supplies
6002	Small Equipment
6003	Janitorial Supplies
6004	Clothing and Uniforms
6005	Fuels, Oils, and Lubricants
6006	Tires and Tubes

REPAIR AND MAINTENANCE SUPPLIES

6020	Building Materials and Supplies
6021	Paints and Metals
6022	Plumbing and Electrical
6023	Parts and Repairs
6024	Maintenance and Service Contracts
6025	Asphalt
6026	Culvert and Pipe
6027	Gravel, Dirt, and Sand
6028	Lumber and Pilings
6029	Small Tools
6030	Concrete
6031	Bridges and Steel

EXAMPLE MUNICIPAL EXPENDITURE CODES CHART

OTHER SERVICES AND CHARGES

PROFESSIONAL SERVICES - Services that by their nature can be performed only by persons or firms with specialized skills and knowledge. Although a product may or may not result from the transaction, the primary reason for the purchase is the service provided.

7001	Accounting and Auditing
7002	Management Consulting
7003	Computer Services
7004	Engineering and Architectural
7005	Special Legal
7006	Other Professional Services
COMMUNICATIONS	
7020	Telephone and Fax - Landline
7021	Postage
7022	Cell Phones and Pagers
7023	Internet Connection
TRANSPORTATION	
7030	Travel
7031	Common Carrier
ADVERTISING AND PUBLICATIONS	
7040	Advertising and Publications
INSURANCE (OTHER THAN PERSONAL SERVICES)	
7050	Official and Employee Bond
7051	Boilers and Machinery Insurance
7052	Fire and Extended Coverage
7053	Fleet Liability
7054	Other Sundry Insurance
UTILITIES	
7060	Utilities - Electricity
7061	Utilities - Gas
7062	Utilities - Water
7063	Utilities - Water Disposal
RENTALS AND LEASES (NOT LEASE PURCHASE)	
7070	Rent - Land and Buildings
7071	Rent - Machinery and Equipment
7072	Lease - Land and Buildings
7073	Lease - Machinery and Equipment
PUBLIC RECORDS	
7080	Public Records
MISCELLANEOUS	
7090	Dues and Memberships
7091	Miscellaneous Law Enforcement
7092	Meals and Lodging
7093	Vending Machines - Food/Drinks
7094	Other Miscellaneous
7095	Training and Education
7096	Computer Software, Support, and Maintenance Agreement

EXAMPLE MUNICIPAL EXPENDITURE CODES CHART

CAPITAL OUTLAY

8001	Land
8002	Buildings
8003	Improvements Other Than Buildings
8004	Machinery and Equipment (Other Than Vehicles)
8005	Vehicles
8006	Construction in Progress

DEBT SERVICE

9001	Bond Principal
9002	Bond Interest
9003	Note Principal
9004	Note Interest
9005	Lease Purchase Principal
9006	Lease Purchase Interest