ARKANSAS MUNICIPAL LEAGUE GREAT CITIES MAKE A GREAT STATE

MUNICIPAL FINANCE AND BUDGETING CERTIFICATION WORKSHOP: BEST PRACTICES

September 12, 2018

8:30 a.m. – 9:00 a.m.	**Registration**	
9:00 a.m.	**Welcome**	Mayor Joe Smith, League President City of North Little Rock
9:00 a.m. – 10:00 a.m.	**Annual Budget – What are the legal requirements and who is in charge?**	Mark Hayes, Executive Director AML
10:00 a.m. – 10:30 a.m.	**Establishing the Budget Process - What is the best way?**	Mark Hayes, Executive Director AML
10:30 a.m. – 11:00 a.m.	**Preparing the Budget – Have you taken all revenue sources into consideration?**	Karen Scott, Finance Director City of North Little Rock
11:00 a.m. – 11:30 a.m.	**Adopting the Budget – How is this best accomplished?**	Mark Hayes, Executive Director AML
11:30 a.m. – 12:00 p.m.	**Financial Controls and Reporting – Are these being done in the correct way?**	Cindy Frizzell, Finance Director AML
12:00 p.m. – 1:00 p.m.	**LUNCH**	
1:00 p.m. – 1:30 p.m.	**Legislative Audit – What are the most common findings and how can you avoid them?**	Joe Archer, Field Audit Supervisor AR Legislative Audit

1:30 p.m. – 2:00 p.m.	**Legislative Audit's Information Systems Best Practices – Are you in compliance?**	David Coles, Field Audit Supervisor AR Legislative Audit
2:00 p.m. – 2:30 p.m.	**ACOOP and IT in a Box – How can they help your city**?	Carol Skill, DIS QA Coordinator AR Dept. of Information Systems Nathan Hansard, Account Executive Sophicity – IT in a Box
2:30 p.m. – 3:00 p.m.	**Transparency and Accountability - Conway's Open Checkbook**	Tyler Winningham, Finance Director City of Conway
3:00 p.m. – 3:30 p.m.	**Q&A Session**	Mark Hayes, Executive Director AML

BUDGET LAW

Mark R. Hayes
Executive Director
Arkansas Municipal League
(501) 978-6102
September, 2018

THE SHALLS…

THY MAYOR SHALL SUBMIT…

- **Ark. Code Ann. § 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.

THINE GOVERNING BODY SHALL PASS…

- **Ark. Code Ann. § 14-58-202. Adoption.**
- Under this subchapter, **the governing body of the municipality shall, on or before February 1 of each year, adopt a budget** by ordinance or resolution for operation of the city or town.

SPEND
ONLY WHAT'S IN THE BUDGET

- **Ark. Code Ann. § 14-58-203. Appropriations; alterations and limitations.**
- **(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.

THE MAYS…

- **Ark. Code Ann. § 14-58-203. Appropriations and changes.**
- **(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**:
- (SEE NEXT SLIDE…ALSO, PURPOSE MEANS PUBLIC PURPOSE!)

THE BE CAREFULS…

- **Ark. Code Ann. § 14-58-203. Appropriations and changes.**
- **(1)** Funds resulting from taxes levied under statutes or ordinances for specific purposes may not be diverted to another purpose;
- (ILLEGAL EXACTIONS!!!)
- **(2)** Appropriated funds may not be diverted to another purpose where any creditor of the municipality would be prejudiced thereby.
- (CONTRACT LAWSUITS!!!)

THE A.G.

- Opinion 2002-268:
- "It is my opinion that municipalities may not formulate their budgets to end on January 31 of each year rather than December 31"
- Citing one of our ***shall*** statutes **Ark. Code Ann. § 14-58-201**
- "…the mayor …***shall submit*** to the governing body of the city or town…a proposed budget for operation of the city or town from ***January 1 to December 31*** of the forthcoming year."

THE A.G. CONTINUED

- Opinion 2002-268:
- ***Question 3 - Is there a conflict between A.C.A. § 14-58-201, which requires a budget period from January 1 to December 31, and A.C.A. § 14-58-202, which allows until February 1 for the annual budget to be adopted?***
- "It is my opinion that rather than conflicting, these two provisions simply **permit a situation in which the city would be required to operate without a permanent budget for a limited time**."

A.G. CONTINUED

- This conclusion, of course, raises the question of how the city is to operate during the time period between December 31 and February 1. During that time period, the city must operate by way of specific city council action for expenditures. Such specific city council action can take the form of **simply adopting the previous year's budget on a temporary basis, or can be applied to individual expenditures.**

A.G. CONTINUED

- In my opinion, the city council's general authority over the city's fiscal affairs, *see* A.C.A. § 14-43-502, and the council's general power of appropriation, *see* A.C.A. § 14-58-203, provide a sufficient basis for its authority to operate the city by way of specific action for expenditures during that limited period (***JANUARY!***). (AND…see next slide)

A.G. CONTINUED

- Although this issue has not been addressed by the Arkansas Supreme Court, at least one court of another jurisdiction that has addressed the issue has adopted this approach. See *Wilson v. Dawson*, 590 So.2d 263 (Ala. 1991) (city council's statutory authority to control city's finances gave it authority to approve expenditures in absence of valid budget).

THE SHALLS CONTINUED

- **14-43-313. City clerks and attorneys generally.**
  - "The city clerks and the city attorneys in cities of the first class ***shall*** …receive **such salary as is prescribed by ordinance** in each of these cities."
- **14-43-316. City clerk, treasurer, or clerk-treasurer in mayor-council cities of fewer than 50,000. (first class only per (a))**
  - **(c)** The city clerk and city treasurer, or city clerk-treasurer…***shall*** receive a salary **as is prescribed by ordinance** in each of these cities.
- **Cities of the second class and incorporated towns…lucky you!**

THE ROLE OF THE MAYOR…

- MAYOR: Report, report, report!
- **"[W]ithin the first 90 days of the year…"** A.C.A. §§14-43-504 and 14-58-302.
- I suggest monthly financial reports.
- What do you do?
- Monthly, weekly…
- The better informed the council is, the better the budget.
- (and don't forget the shalls: submit, submit, submit)

THE ROLE OF THE COUNCIL…

- PASS THE BUDGET! SHALL, SHALL, SHALL!!
- Be well informed: read the financial statements early and often.
- Ask the mayor for specific department needs.
- Look at long term plans and needs.
- Meet and study long before the date of passage.

First Class City "Maximum Amount" Statute: SHALL…

- 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.

- 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.**

- Ark. Code Ann. § 14-58-305. (Home Rule: likely all cities and towns can do this)

Limits on Mayor's Spending Authority

- § 14-55-204 – appropriations require a majority vote of the council.
- § 14-58-203 – the budget is an appropriation.

So if it hasn't been appropriated…

- … ***Then it shouldn't be spent.***
- ***AGAIN: NO APPROPRIATION; NO SPENDING***
- If it got spent anyway, amend the budget before the End of Year.
- If you don't do it by the End of the Year, do it ASAP!

So basically…

- … The budget (or possibly some other form of appropriation) sets the parameters for what the Mayor may spend.

THE ROLE OF THE CLERK/RECORDER/TREASURER

THE ROLE OF THE CLERK/RECORDER/TREASURER

- SUPPORT, RECORD-KEEPING AND CHECKS AND BALANCES!
- The Clerk/Recorder/Treasurer Handbook
- The AML Handbook.
- Others:
- https://static.ark.org/eeuploads/arml/MayorCouncil_Guidebook_2015_WEB.pdf
- https://static.ark.org/eeuploads/arml/Guidebook_City_Managers_2015_WEB.pdf

THE AUDITORS

- **14-58-101. Audit by independent accountant. (every municipality!)**
- **(a)** The **audit or agreed-upon procedures engagement** of every municipality ***shall be made*** by the **Arkansas Legislative Audit or other independent persons** licensed and in good standing to practice accounting by the Arkansas State Board of Public Accountancy, **to be selected by the governing body of the municipality.**

- **14-58-307. Annual audit. (First Class)**
- In cities of the first class, the municipal governing body ***shall*** have the financial affairs of the city **audited annually** by an **independent certified public accountant**, who is not otherwise in the service of the city, **or by the Division of Legislative Audit** of the State of Arkansas.

AUDITORS

A.C.A. § 14-58-101(b):

- Compliance with:
- **(1)** Arkansas Municipal Accounting Law, 14-59-101 et seq.;
- **(2)** Arkansas District Courts Accounting Law, 16-10-201 et seq.;
- **(3)** Improvement contracts, 22-9-202 → 22-9-204;
- **(4)** Budgets, purchases, and payments of claims, etc., 14-58-201 et seq. and 14-58-301 et seq;
- **(5)** Investment of public funds, 19-1-501 et seq.; and
- **(6)** Deposit of public funds, 19-8-101 → 19-8-107.

AUDITORS

- **(c) (2) (A)** The financial statements of municipalities shall be presented on a fund basis with, as a minimum:
- **(i)** The general fund and the street fund presented separately; and
- **(ii)** All other funds included in the audit presented in the aggregate.
- **(B)** The financial statements shall consist of the following:
- **(i)** A balance sheet;
- **(ii)** A statement of revenues (receipts), expenditures (disbursements), and changes in fund equity (balances);
- **(iii)** A comparison of the ***final adopted budget*** to the actual expenditures for the general fund and street fund of the entity; and
- **(iv)** Notes to financial statements.

AUDITORS

A.C.A. § 14-58-101

- **(C)** The report shall include as supplemental information a schedule of ***general fixed assets, including land, buildings, and equipment***.
- **(3)** In the alternative to subdivision (c)(2) of this section, the ***governing body of the municipality may adopt an annual resolution*** **requiring their audit to be performed in accordance with the guidelines and format prescribed by the Governmental Accounting Standards Board**, the American Institute of Certified Public Accountants, and the United States Government Accountability Office, if applicable.

Personal Interest

- (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. Ark. Code Ann. § 14-42-107

ACT 582 OF '15, 14-59-115

- Authorizes electronic distribution of funds by private person/entity (payroll)
- Requires ordinance dictating a method accounting control, documentation etc.
- Requires city to ensure the private person/entity is insured, bonded and uses best practices
- Treasurer must still approve disbursement before funds are dispersed

Uniformed Employees-Police

- Law enforcement officers in cities and towns with fewer than five (5) law enforcement officers, including the chief or marshal, are exempt from the overtime provisions.
- Volunteers are not considered "employees" for this purpose however. No distinction is made between part-time and full-time employees.
- You must be sure your officers receive a minimum wage for all hours worked in a work period.
- 29 U.S.C. §213(b)(20); 29 C.F.R. §§ 553.200, 553.211.

Uniformed Employees- Fire

- Same as police, see above.
- "Employee in fire protection activities" means an employee: including a firefighter, paramedic, emergency medical technician, rescue worker, ambulance personnel, or hazardous materials worker, who--
  - (1) is trained in fire suppression, has the legal authority and responsibility to engage in fire suppression, and is employed by a fire department of a municipality, county, fire district, or State; and
  - (2) is engaged in the prevention, control, and extinguishment of fires or response to emergency situations where life, property, or the environment is at risk.
  - 29 U.S.C.A. § 203(y)

Uniformed Officers' Workweek

- The FLSA provides a partial overtime exemption for uniformed employees who work a "work period" established by the city of no fewer than:
  - seven days and no more than twenty-eight days.
  - The city can establish separate work periods for the police department and the fire department.
  - If the city fails to establish a work period, 207(k) does not apply and a fire or police employee working over forty hours will accrue overtime compensation.
    - See handout for chart.
    - 29 C.F.R. § 553.230.

Final Thoughts

- The city as employer has the option of paying overtime or of giving comp time off.
  - The employee must understand that the city has a policy of compensatory time off.
- Compensatory time is accrued at 1 ½ hours for each hour worked.
  - Police and fire employees can accrue a maximum of 480 hours of comp time or 320 hours worked.
- After an employee has accrued maximum compensatory time, the employee must be paid in cash for overtime worked.
- 29 C.F.R. § 552.230

Final Thoughts Part Deux

- There is no FLSA limit on the number of hours per day worked (other than child labor). 29 C.F.R. § 778.102.
- A work week under the FLSA is defined as seven consecutive 24-hour periods (although this may be altered for police and firefighters as discussed above). Note that this may not be the same as the city's "pay period."
- Only hours worked count in calculating overtime. Pay for holidays, vacations, sick time, jury duty, etc., do not count as hours worked.
- 29 C.F.R. § 778.102.

Questions/Comments?

Mark R. Hayes

Executive Director

Arkansas Municipal League

(501) 978-6102

September, 2018

Establishing the Budget Process

Mark Hayes

Executive Director, ARML

mhayes@arml.org

When to Start the Budget Process?

- As early as possible.
- Remember that the first deadline is **December 1** for submitting the budget.
- Which means that the mayor must have already prepared the budget by November.
- This takes time, and should not be rushed at the last minute.

When to Start the Budget Process?

- As a baseline, consider a "6 month rule"
- Every six months you should either be starting the budget process, or submitting the budget.
- Submit the budget in December, start the budget process in June/July.
- At the very latest, begin the budget process in August/September, because no matter what you need to take into account a plethora of consideration, and turn that information into a budget.

Understanding the Budget Process

- Budgets serve a different purpose in a government than they do in a business
- In a business, they are a plan to shoot for; often they can be a aggressive plan that you may or may not be likely to achieve;
- In a Municipality, the expenditure side of the budget is called "appropriations," and it is the legal authority for the City to provide services.

Understanding the Budget Process

- The budget appropriation is not a forecast of the amount the Municipality expects to spend; it is the **maximum amount** that the city is allowed to spend.
- Just because a department is under budget, but asking for more revenue does not mean anything other than they followed the law, but need a larger budget to provide high level of services to your municipality.
- Which leads into the next topic:

Communication is Key

- This includes municipal employees, businesses, citizens, council members, the mayor, administration, and more.
- These groups are all going to bring a differing perspective that you as city officials should consider.
- Remember, just because you disagree with them doesn't mean they aren't providing meaningful information for the budget process.

Communication - Input

- Mayors and Council Members start with the people who know best
- The Department Heads
- Fire, Police, Street, Water, etc.
- These individuals will be able to tell you what is happening on a day-to-day basis.
- Keep in mind, even if they're departments are operating well they may need:
  - New fire equipment, new police equipment, vehicles, additional personnel to keep pace with a growing city.

Communication – Input

- You may want to instruct department heads to gather information throughout the year or leading up to the budget process.
- In the same way you need input from the department heads
  - They will need input from the employees.
- Are the police officers carrying guns without bullets, driving vehicles which have holes in the floors.
- What are our working conditions?

Communication – Outside Input

- Remember, your citizens and businesses will have valuable input as well.
- They will see where our services could use improvement
  - Do we have enough personnel that we're providing necessary services in a timely manner?
  - Are police able to respond to all calls, how about water/sewer?
- Ask you business community if they see any need for improvement of infrastructure which could help?
- Obtaining community input to help in the strategic planning process can be achieved through citizen surveys, community forums or other public participation processes.

Capital Projects and Assets

- Set up a system so that your city reviews its capital assets to determine if the city needs to budget for them this year.
- For example, does our offices need major or minor repairs? Have we outgrown our police department and need to start budgeting for a new building/lease?
- How are the streets and other infrastructure?
- Establishing a process to review our assets not only helps us organize this year, but helps us keep an eye on the future.

Communication – Long term strategy

- Even if we can't accomplish everything our citizens/businesses and employees are bringing to us, it leads into a very important topic.
- What are our long term goals financially for the municipality?
- By developing specific goals and objectives, the budget process logically follows by attaching financial resources to the goals.
- Draft goals can be prepared by the governing body or mayor, and presented through a public participation process. Goals communicate your community visions, desires and promises, and set the tone for the future budgets.

Communication – Long term strategy

- Try to stay focused on providing a great one year budget, with an eye toward three or five year plans for the city.
- Do you want to revitalize the public parks, downtown, improve infrastructure?
- You don't accomplish that all in one budget, you can do it pieces at a time and slowly build up a long term budgeting strategy to accomplish the goals you set.

Future Considerations

- As you set your future strategies and goals, and begin budgeting for the future keep in mind those items which are sure to impact the city.
- Retirement funds/liabilities for city officials. Are you prepared to fund a statutory retirement for a mayor/clerk/recorder/treasurer?
- Do we have debt payments looming? Are we keeping pace with these payments?
- How much should we set aside to offset this future liability?

Communication – City Council

- Councilmembers need to decide how they would like to provide input
- Do you want to put a committee together to help address the council's concerns before the mayor submits the budget?
- Councilmembers are answerable to their constituents who will have opinions that the city needs to hear.

Communication – Recorders, Clerks, and Treasurers

- It should go without saying that your financial officers, and primary city administrators will have a different perspective than all other officials.

- They will see more of the input/output of the budget than the other officials, and should be involved in the process from day 1.

How to get the information?

- For all the non-council positions, departments, employees, citizens, businesses;
- Consider setting up information request;
- For example, each department can submit a yearly budget request. (or something similar).
- Always leave enough time for the mayor to receive the information and digest it into a workable budget.

Misc. Topics

- Try to keep an open mind throughout the process.
- There will always be new and unique budgeting concerns.
- Does the city need to begin setting aside an Information Technology budget?
- What will our city do in case of an emergency?

Benefits of Full Transparency

- The degree to which the budget & budgeting are open to the public is a matter of local discretion.
- Are budget meetings well publicized ahead of time?
- Is the budget document understandable to all the parties involved?
- Is there sufficient detail to justify the revenue & expenditure projections?
- Is the process clear?
- Are there opportunities for citizen input?

Final thoughts?

Mark R. Hayes

Executive Director

Arkansas Municipal League

(501) 978-6102

September, 2018

Preparing the Budget – Have You Taken All Revenue Sources Into Consideration

Arkansas Municipal League Finance & Budgeting Workshop

September 12, 2018

Revenues – The Big Three for North Little Rock

- Local Real & Personal Property Tax Millage – communication with county assessor & collector
  - General Fund
  - Street Fund
  - Police & Fire Pension Funding
  - Library Funding
- State Turnback
  - Annual Estimated Amounts Provided by AML
- Local Sales Tax
  - Lucky enough to have one?
    - Trend data available
    - DF&A Website - https://www.ark.org/dfa/localtaxes/index.php
    - DF&A Revenue Forecasts & Monthly Reports

Other Revenues

- Franchise Fees
- Business License Fees
- Building Permit Fees
- Court Fines & Fees
- User Fees (Parks, Sanitation, Senior Citizens Center)
- Hamburger Tax – Limited Uses
- Grants
- Local Sales Tax – Don’t have one but want to pursue it – League Resources

Other Revenue Considerations

- Missed Opportunities –
  - Franchise Fees (audits)
  - Tower Rental Income (long-term agreements)
  - Rental Income (parks facilities, airports)
  - Code Enforcement
  - Business Licenses
  - Police Expense Refunds (reimbursements for overtime, school resource officers)
  - Excessive Burglar Alarms
  - Fire Alarms
  - Cost Sharing Projects – partnerships with other governments or community organizations
  - Interest Income – maximize in a still challenging interest rate environment
  - Refinance Outstanding Debt – ability to eliminate future rate increases to citizens

Grants

- Advantages
  - Without grant funding, many projects/purchases do not happen
    - Streets – AHTD
    - Personnel – US Dept. of Justice, FEMA
- Disadvantages
  - Many times match is required
  - Many personnel grants do not allow eliminating those positions after grant funding has expired
- FEMA Funds
  - Organized Coordination of Efforts – administrative, fiscal, public safety, public works
  - Diligence

Future Planning

- Budget More Conservatively
  - Do not budget revenues that are not realistic
  - Transparency - better headlines when revenues and expenditures are within budget, rather than outside of budget
- Analysis of Revenues Collected – Are Revenues Covering Program Costs
  - Animal Control
  - Parks
  - Sanitation

Questions??

Karen Scott, Finance Director

City of North Little Rock

kscott@nlr.ar.gov

501-975-8800

Adopting the Budget

Mark R. Hayes

Executive Director

Arkansas Municipal League

(501) 978-6102

September, 2018

A Cautionary Tale

- “A budget tells us what we can’t afford, but it doesn’t keep us from buying it.”

- William Feather

Resolution or Ordinance?

- A city may legally use a resolution or an ordinance to adopt its budget
- However, a resolution is the preferable option.
- Legally speaking there are no differences in how it impacts your budget, but a resolution is easier to adopt and amend.
- We have a sample on the next page which we can provide to you if you do not already have one.

SAMPLE

Resolution for the Adoption of the Municipal Budget[1]

Resolution No. _____

A RESOLUTION PROVIDING FOR THE ADOPTION OF A BUDGET FOR THE CITY (OR TOWN) OF _____, ARKANSAS, FOR THE TWELVE (12) MONTHS BEGINNING JANUARY 1, 20___ AND ENDING DECEMBER 31, 20____, APPRORPIATING MONEY FOR EACH ITEM OF EXPENDITURE THEREIN PROVIDED FOR;[2] AND FOR OTHER PURPOSES.

WHEREAS, the City (or Town) Council has made a comprehensive study and review of the proposed budget submitted by the mayor, and;

WHEREAS, it is the finding and conclusion of the City (or Town) Council that the schedules and exhibits of anticipated revenues and expenditures for the calendar year appear to be as accurate as possible for budgetary purposes.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY (OR TOWN) COUNCIL OF _____, ARKANSAS:

Section 1. This resolution shall be known as the budget resolution for the City (or Town) of _____, Arkansas, for the twelve (12) month period beginning January 1, 20___ and ending December 31, 20 ___. The attached budget, incorporated herein as if set out word for word and figure for figure, reflects estimated revenues and expenditures as set forth on the succeeding pages.

Section 2. The respective funds for each item of expenditure proposed in the budget for 20___ are hereby approved and adopted for the operation of the City (or Town) of _____, Arkansas, by the City (or Town) Council on this date and constitute an appropriation of funds which are lawfully applicable to the items contained within the budget. This budget may be altered or revised by action of this governing body and

---

[1] NOTE: If this resolution is used as presented it must include the budget document. The resolution should be at the beginning of the budget document.

[2] Because the Arkansas Municipal League ("AML") cannot anticipate when every city (or town) will pass its budget, as an option the following emergency clause is included in this footnote. This Language should be added to the resolution if an emergency is to be declared:

A. After footnote 2 add: DECLARING AN EMERGENCY

B. After Section 4 add: Section 5. WHEREAS, the efficient operation of municipal government requires that a budget be planned and adopted by the governing body, and that without a budget the city (or town) may not pay its bills, debts or liabilities; now, therefore, an emergency is hereby declared to exist and this resolution being necessary for the preservation of the public peace, health and safety shall take effect and be in force from and after its passage and approval.

The Complete Process

- Pre-submission information gathering – Summer through December 1
- Mayor's budget submission deadline – December 1st.
- Council approves the next year's budget – December or at the latest Early Jan.
- Revision and amending the budget – Periodically or year end.

Initial Budget Draft

- Once the mayor has a draft budget prior to Dec. 1st
- Give consideration to getting this information out to the department heads and council as soon as practicable.
- This will give time for feedback which can help shape the budget
- Several weeks for the council is recommended so that the council can start deciding on how they will to comment, or amend the budget based off their own concerns.

Drafting the Initial Budget Revenues

- Keep track of all your revenue on the budget. (Talk with your treasurer/financial officers to make sure you aren't missing anything).
- This includes all available revenues to for the coming fiscal year.
- A municipalities revenues typically include non-restricted funds (General Funds), restricted funds (Specific sales tax, street funds, etc.), and other possible funding sources as allocated and approved by the council.
- The services provided by city are based on the available revenues from all sources as approved in its annual budget, which is a result of the annual budget process.

Drafting the Initial Budget Expenses

- The expenses of the budget process is determined based on the available revenues and approved allocation of these revenues to pay for projected purchases and approved services.
- Available funds are allocated to finance the services provided by the city, as well as its approved capital projects, for the coming fiscal year.
- Remember the previous topics, try to create the budget for this year but with an eye to next year

Emergency Funds

- As part of a forward thinking municipality, the municipality might set up a "rainy day" fund.
- Emergencies happen and the city can begin establishing an emergency fund for these unforeseeable concerns.
- Remember, you're not only worried about the city for this year, but you're concerned about the next five years, the next decade and beyond.

Discussing the Budget

- Budgeting is political
- Budgets control spending
- Budgeting creates conflict
- Budgeting reflects organizational culture
- Budgeting involves balancing values

Discussing the Budget

- You're going to disagree on how best to create the budget.
- Some people will value certain projects/expenditures over others.
- Some will simply value crafting as fiscal a budget as possible.
- You will disagree, but you shouldn't fight over it.
- Deadlocked councils who fight on every item, slow down the city and damage the public image of our municipality.

Discussing the Budget

- If you feel like you've lost on the budget process it isn't a good idea to oppose everything the city does in retaliation.
- Begin working on convincing the other members of why we should change, you have a full year to show everyone why you're right, not why they're wrong.
- This is the tough advice to give and receive, but ultimately the majority of the council will decide the budget.

Amending the Budget

- Your budget is likely to change throughout the year as you notice different results from your predictions.
- If the council is approached "before" the over-expenditure occurs, the board has a chance to make the following choices:
  - Increase the budget
  - OR Control/reduce expenditures

Amending the Budget

- How often do you want to review the budget throughout the year?
- Yearly? This means a large amendment at the end of the year to "fix" the budget
- Quarterly?
- Monthly?

Final Considerations

- Your city must make one final budget consideration:
  - Line item v. General budgets
- Line items give ultimate control to the council, but will require many more meetings and repeated amendments throughout the year to maintain they system.
- General budgets will put more discretion in the mayor's hands, but will require less meetings and oversight by the council.

Final Considerations

- A large topic when considering line item v. general budgets is how do you want to set salaries?
- Do you want the council dictating each employee's salaries, or do you want to provide your departments with a general operating budget that they can work with?
- There's no right answer but you need to keep in mind the pros and cons of each system.

Final Considerations

- Remember that salaries are the most likely to change year to year.
- It is easier to keep your good employees than it is to find new ones.
- I promise turnover can be more costly than a raise depending upon how skilled your current employees are.
- Keep this in mind as you're adopting a budget, you may want to offer a double check of projected salaries.

Other Resources

- ARML Publications – FAQs, Accounting Handbook, and Other Timely Topics
- https://www.arml.org/services/publications/publications-for-free

- Pay particular attention to budgets, debt, accounting, and bidding.

Final thoughts?

Mark R. Hayes

Executive Director

Arkansas Municipal League

(501) 978-6102

September, 2018

Arkansas Legislative Audit

Information Systems Best Practices

January 2018

TABLE OF CONTENTS

PURPOSE

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

Internal Controls

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

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

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

Assessing Risk

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

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

Monitoring

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

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

INTRODUCTION

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

Part One: General Controls

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

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

Part Two: Application Controls

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

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

Part Three: Other Technology

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

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

BEST PRACTICES – GENERAL CONTROLS

IS Management

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contract/Vendor Management

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

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

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

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

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

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

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

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

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

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

Network Security

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

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

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

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

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

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

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

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

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

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

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

Wireless Networking Security

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

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

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

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

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

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

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

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

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

Physical Access Security

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

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

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

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

1-5.4: Implement the following physical security controls:

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

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

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

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

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

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

Logical Access Security

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

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

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

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

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

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

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

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

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

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

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

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

Disaster Recovery/Business Continuity

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

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

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

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

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

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

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

BEST PRACTICES – APPLICATION CONTROLS

Data Input

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

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

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

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

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

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

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

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

Data Processing

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

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

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

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

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

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

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

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

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

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

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

Data Output

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

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

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

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

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

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

Application-Level General Controls

Application Security Management

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

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

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

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

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

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

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

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

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

Application Configuration Management

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

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

Segregation of Duties

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

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

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

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

Application Contingency Planning

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

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

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

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

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

BEST PRACTICES – OTHER TECHNOLOGY

Electronic Signatures and Digital Signatures

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

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

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

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

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

Payment Cards (Debit or Credit)

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

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

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

Bring Your Own Device (BYOD)

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

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

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

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

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

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

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

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

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

Electronic Banking

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ACOOP: Arkansas Continuity of Operations Program

CAROL M. SKILL

DEPARTMENT OF INFORMATION SYSTEMS
DIS

HTTPS://ACOOP.ARKANSAS.GOV

Arkansas Department of information Systems

When Do I Need ACOOP?

Arkansas Department of information Systems

Why is ACOOP Important?

In the event of a Disaster:

- What Do you do First?
- Who needs to be contacted?
  - How do we Inform Employees of what to do?
- Where will the Employees go?
- Where is your Data Stored (Backups)?
- How are you Going to Restore your Data?
- What is your Essential Functions?
- What “Teams” Do we have?
  - What “tasks” do each team need to complete to function?
- What supplies, equipment, etc. do we need?
  - How many?

Arkansas Department of information Systems

What We Do

- Arkansas Continuity of Operations Program ACOOP
  - All Hazards
  - Response, Continuity, Recovery
  - Required for State Agencies
  - Available to all State and County

Arkansas Department of information Systems

Arkansas Dept. of Legislative Audit

- Serve the General Assembly Legislative Joint Auditing Committee and Arkansas Citizens
- Promote sound financial management and accountability of public resources
- Completes financial audits, reviews and special reports
- Conducted in an independent and unbiased manner

http://www.arklegaudit.gov/

Arkansas Department of information Systems

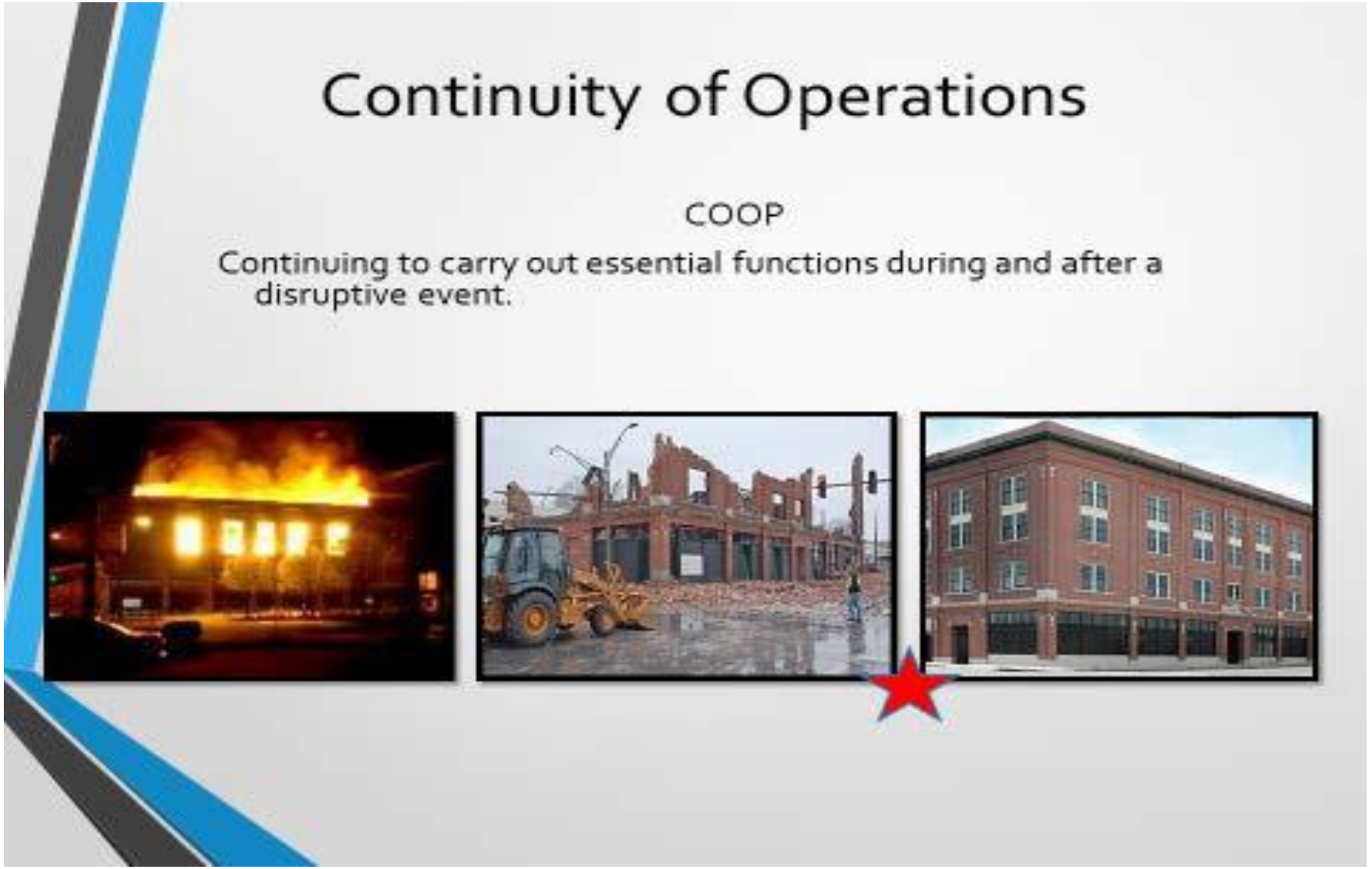
What Does ACOOP DO?

ACOOP Provides

- Software
- Consulting
- Training
- Testing
- Resource
- Data Backups

Arkansas Department of information Systems

What is Continuity of Operations?



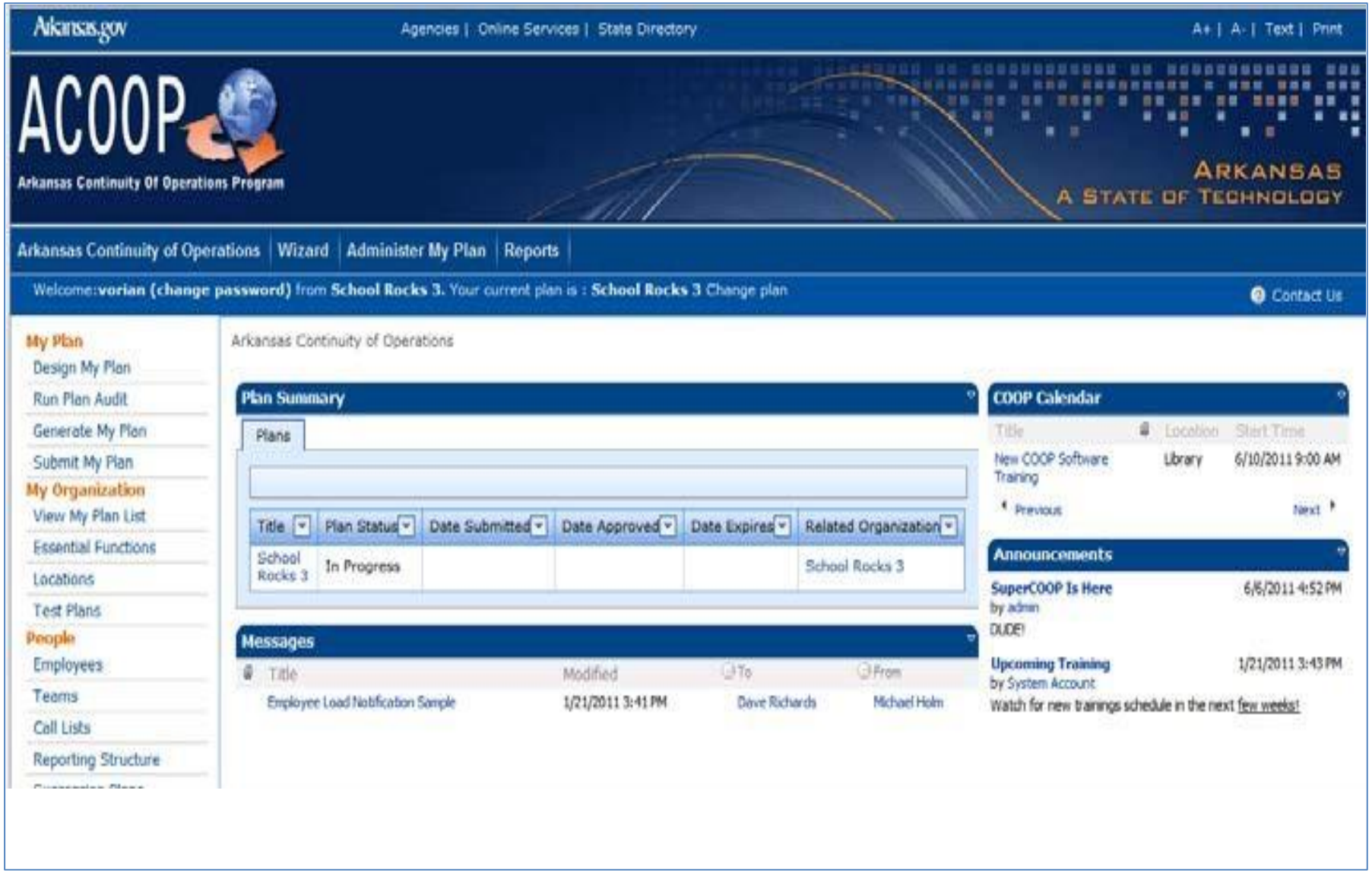
Arkansas Department of information Systems

ACOOP: General Plan Information

- URL:
  - https://acoop.arkansas.gov
- Individual Login and Plan
- Data Stored by Department of Information Systems (DIS)
- When Plan is Completed:
  - Anyone should be able to review the plan and know exactly what tasks need to be completed in order to have your organization functional.

Arkansas Department of information Systems

What Does ACOOP Look Like?



Arkansas Department of information Systems

What Information is Required?

Arkansas Department of information Systems

What Are Essential Functions?

Arkansas Department of information Systems

What Needs to be Included in "Teams and Tasks?"

Arkansas Department of information Systems

Call Lists, Reporting Structure & Order of Succession

Arkansas Department of information Systems

What Are Vital Records?

Arkansas Department of information Systems

Resources Needed

Arkansas Department of information Systems

Plan For Several Different Disasters

Arkansas Department of information Systems

What Other Documents Are Required?

Arkansas Department of information Systems

Contact Information

Carol M. Skill

501-682-5381

Carol.Skill@Arkansas.gov

ACOOP Help Desk

DIS.ACOOP@Arkansas.gov

General Help

501-682-4357 (682-HELP)

Arkansas Department of information Systems

IT in a Box

A *complete* IT solution for city governments.

Cybersecurity and Computer Maintenance

IT in a Box guards against cyberattacks by keeping your computers patched, protected, and healthy. Includes always-on monitoring and alerting for issues, enterprise-class antivirus protection, automated computer maintenance, and ongoing software patching to keep you secure.

24x7 Helpdesk

IT in a Box's U.S. based helpdesk provides cities both remote and onsite support. You will talk to senior IT engineers with many years of experience supporting municipal staff and applications. Available 24x7x365, our helpdesk supports your municipal staff in the office, working from home, and on the road.

Data Backup and Disaster Recovery

Onsite data backup for quick recovery after events like a server failure. Unlimited offsite data backup for worst-case scenario recovery after a major incident like a natural disaster. Real-time monitoring to quickly address data backup issues and quarterly testing to verify your disaster recovery.

Records / Document Management and Email

Software and policies to protect your city records, documents, and email. Reliably archive, retain, access, and delete information according to your record retention schedules—and we even help you process Open Records Requests. Also includes Microsoft Office Professional Plus and city email with 50GB of mailbox storage for each user.

Video Archiving

No more buying additional expensive storage for video. We provide unlimited offsite video storage to meet state record retention policies. As your squad car and body camera video continue to grow at a rapid pace, your storage costs do not change.

Who guarantees IT services based on your expectations?

WE DO!

Our GUARANTEE

- **Love I.T.** If we don't meet your expectations, then cancel the service!
- **Flat monthly fee.** No hourly charges. Predictable!
- **No upfront project fees.** Onboarding, equipment, and setup included!
- **Flexible.** Increase or decrease your number of users any time!
- **Proven.** Tailored for cities!

Policy and Compliance

We help you adopt best practices and policies that address information security risks and assist with Legislative Audit compliance. By making sure your staff is knowledgeable and prepared, we help your city comply with the law and lessen your risk of falling victim to the latest external and internal threats.

Website

We provide you a modern website with a custom design that will reflect your community well online. To save you time, submit your website updates to us and we will post them for you.

Vendor Management and Procurement

No more frustrating calls with vendors. We've got it! Issues with your software or hardware vendor? Call us for support. Need a new computer? Call us and we'll procure it.

Dave Mims | 770.670.6940 x110
davemims@sophicity.com
www.sophicity.com

Powered by Sophicity

Chris Hartley | 501.978.6106
chartley@arml.org
www.arml.org