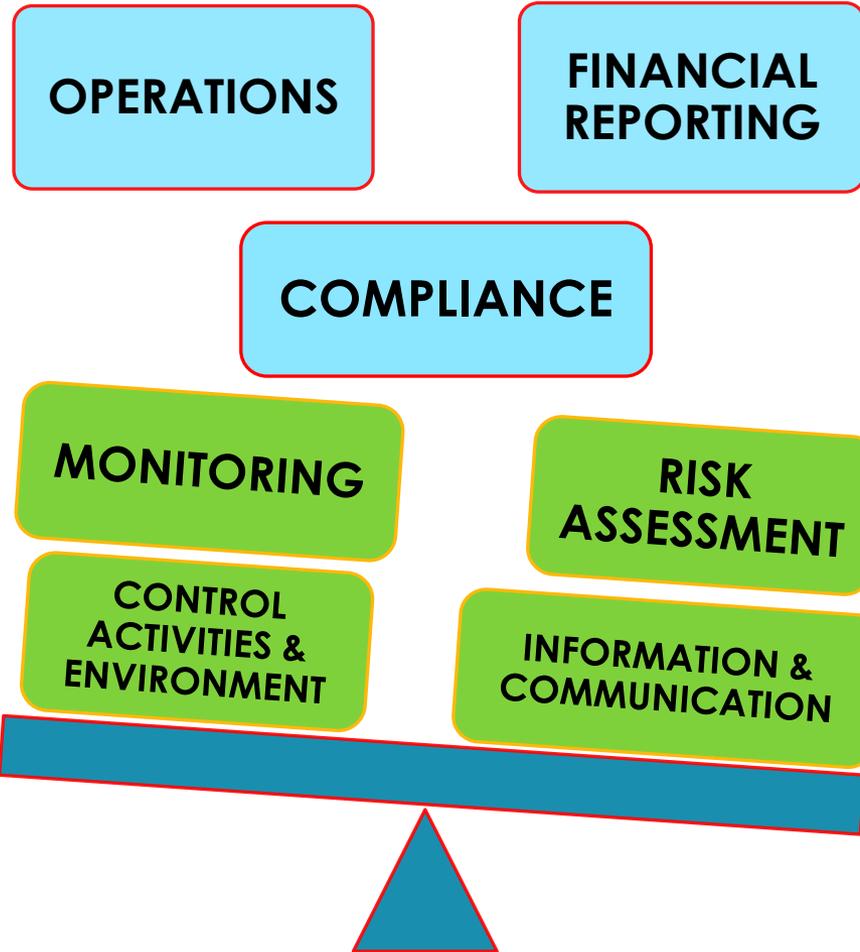


2013 SAD Training

Internal Controls

INTERNAL CONTROLS





COMPLIANCE

**Montana Code
Annotated (MCA's)**

**Generally Accepted
Accounting Principles
(GAAP)**

**3rd Party Restrictions;
* bond requirements**

Federal laws

Required per MOM policy

- Per MOM 302. VIII.
- State agencies are responsible for implementing internal control procedures to ensure all transactions necessary for compliance with generally accepted accounting principles (GAAP) are recorded in SABHRS before fiscal year-end.
- Agencies should develop appropriate internal control procedures based upon their business processes.

I/C Procedures ...

- Promote compliance with policies / regulations
- Promote data integrity/security
- Promote security over physical assets
- May prevent or detect fraud

Should be designed to...

- Detail accountability
- Maximize efficiency
- Minimize fraud risk
- Safeguard sensitive information/areas

Internal Controls Involve ...

- Documentation
- Testing
- Review/Monitoring
- More Documentation

Maintenance never ends....

- Maintaining of internal controls never ends
 - New employees
 - New processes/regulations/systems
- Not a single process
- Not just a financial process
- Lack/failure of internal controls can have financial impact

Other benefits of I/C's

- Creation of internal control processes
 - Looks closely at processes, controls, and result of operations
- Examination may lead to the creation of efficiencies within your operation
 - Do you have redundant steps?
 - Did control work as expected?
 - Where there unexpected outcomes?
 - What improvements can be made?

I/C Provides Reasonable Assurance of

- Financial reporting is reliable
- Effectiveness and efficiency of operations
- Compliance with applicable laws and regulations

Steps that can used to start

- Identify potential areas of risk
- Understand inputs/outputs/requirements
- Diagram process/expectations
- Talk with individuals throughout the process
- Look at other processes that may be similar
- Learn from best practices
- No one size meets all
- Always document

Common I/C Procedures

- Separation of duties
- Rotation of duties
- Checks and balances/comparisons
- Data/security validation
- Limit access to what is needed (buildings, systems, data)
- Rules on approval (who/how)
- Documentation required

Most important element ...

- Management's Support
- "Tone at the Top"
- Relevant at every level

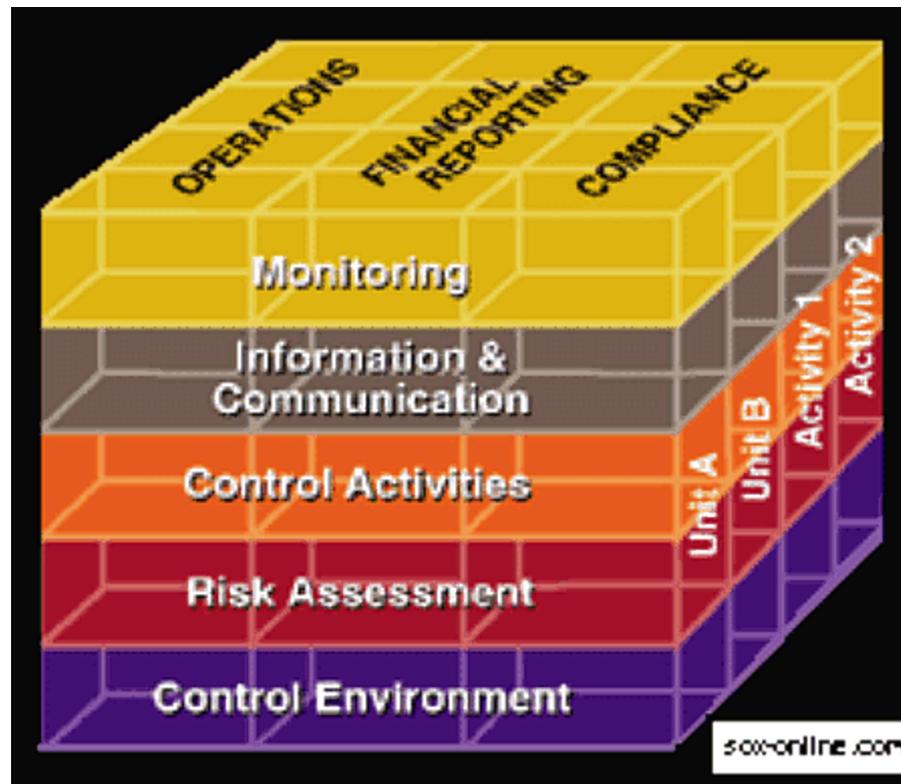
MOM 302 Requirements

- List of personnel authorized approve SABHRS documents
- Receiving report/invoice signed for good recd
- Separation of duties associated with invoices (whenever possible)
- Invoices should be approved. Goods/services under invoice need to have been provided.
- Steps taken to ensure duplicate payment not made.

MOM 302 Requirements (cont)

- Monthly supervisory review of SABHRS reports
 - Research negative encumbrances
 - Entries posted under business unit approved/appropriate
 - Timely correction of unusual/clearing balances
- FYE checklist
 - Unusual balances
 - Clearing account balances that remain

The Original COSO Cube



COSO's Vision ...

- “To be a recognized thought leader in the global marketplace on the development of guidance in the areas of risk and control which enable good organizational governance and reduction of fraud.
- www.coso.org/aboutus.htm

COSO Interrelated Resources

- Provides guidance on 3 interrelated subjects:
 - Enterprise Risk Management
 - Internal Control (update in works)
 - Fraud Deterrence

Control Environment

- Integrity and Ethical Values
- Commitment to Competence
- Management's Philosophy and Operating Style/Structure
- Assignment of Authority and Responsibility
- Human Resource Policies and Procedures
- Audit Committee

Risk Assessment

- Company-wide Objectives
- Process-level Objectives
- Risk Identification and Analysis (potential for fraud)
- Managing Change/impact on I/C

Control Activities

- Activities to mitigate risks
- Activities over technology to support objectives
- Establishment of policies/procedures

Information & Communication

- Quality and relevant information generated and used
- Internally communicates objectives and responsibilities for I/C
- External communication

Monitoring

- On-going Monitoring
- Communication of I/C deficiencies



ACCOUNTING

Cash receipts

Accounts payable

Accounts receivable

Cash reconciliations

Bank deposits

Journal vouchers

Bank Deposits

- WHO:
 - ✓ RECEIVES AND RECEIPTS PAYMENTS
 - ✓ ENTERS INTO THE ACCOUNTING SYSTEM
 - ✓ CREATES THE BANK DEPOSIT, AND MAKES THE BANK DEPOSIT
- WHAT: DESCRIBE THE PROCEDURE FOR;
 - ✓ RECEIVING PAYMENTS
 - ✓ ENTERING PAYMENTS INTO THE ACCOUNTING SYSTEM
 - ✓ PREPARING BANK DEPOSIT
 - ✓ MAKING BANK DEPOSITS

Bank Deposits (cont)

- WHEN:

- ✓ A RECEIPT NEEDS TO BE ISSUED.
- ✓ PAYMENTS SHOULD BE ENTERED INTO THE ACCOUNTING SYSTEM
- ✓ BANK DEPOSIT IS CREATED
- ✓ BANK DEPOSIT SHOULD BE MADE.



OPERATING

Office security

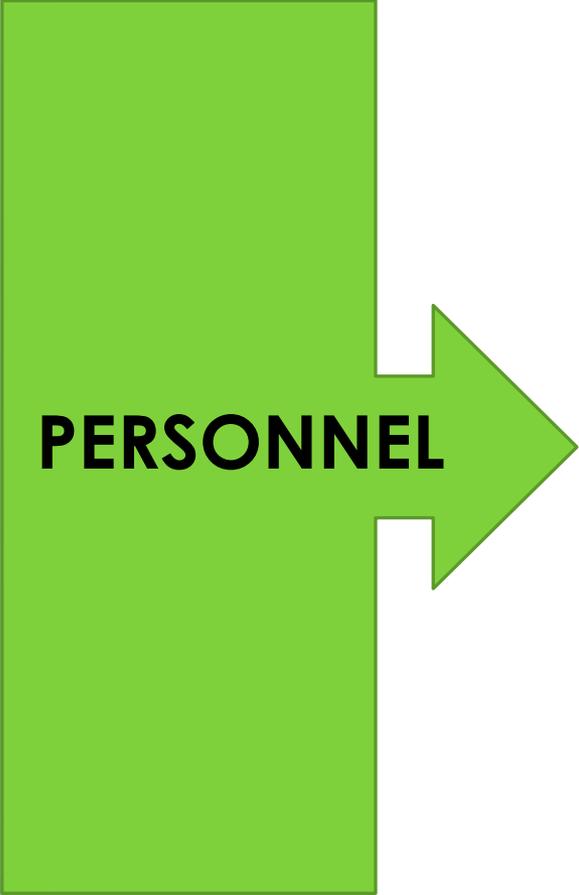
Capital asset
management

Investment policy

Fraud reporting

Business travel
reimbursements

Purchasing policies



PERSONNEL

Standard of conduct

Labor
policies/overtime

Harassment-free
workplace

Wage &
performance review

Benefits

Leave of absence



**CYBER/DATA
SECURITY**

Internet usage at work

Email/Social media

Facilities & physical
hardware

Portable devices

3rd party vendors

Cloud

2-6-504(4), MCA

All state agencies and third parties to whom personal information is disclosed by a state agency shall develop and maintain:

- a) an information security policy designed to safeguard personal information, and**
- b) Breach notification procedures that provide reasonable notice to individuals**



**INFORMATION
SECURITY
POLICY**

RMTD has guidelines concerning possible incidents

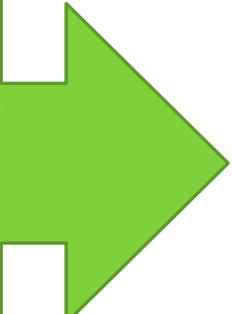
WHEN AN
"INCIDENT"
BECOMES
A "DATA
BREACH"

2-6-501(1), MCA

unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by a **state agency** or by a third party on behalf of a state agency and **causes or is reasonably believed to cause loss or injury** to a person.

Risk of Harm reporting threshold: What "materially compromises the security, confidentiality, or integrity of personal information" is open to interpretation.

**GENERAL
CATAGORIES
OF
PERSONAL
INFORMATION**



**Protected Health Information (“PHI”)
– individually identifiable information
related to treatment, health
condition, or payment for health
care services.**

**Personally Identifiable Information
 (“PII”) – Information capable of
uniquely identifying an individual;
*Name plus one non-public
identifier;
Social Security #, Tax ID #,
Drivers License#, Date of Birth,
Financial Account information**

Under MT Law PII is

- Under Montana law, “personal information” means the first name or first initial and last name of an individual in combination with any one or more of the following data elements when the name and the data elements are not encrypted:

Under MT Law PII is (cont)

- Social security number or tax identification number; or
- Driver's license number, state identification number, or similar identification number issued by any state, district, or territory; or
- An account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to a person's financial account.
- Personal information does not include public information lawfully made available from federal, state, local, or tribal govt records.

Need Cyber/Data I/C's

- All agencies have sensitive or non-public information
 - Systems, on forms, in files
- Does your agency have procedures as to access and storage of non-public information?
- Does your agency know what it should do if information within your agency may have been exposed or is exposed?

Need Data Storage Policies

- Agencies need to evaluate where and how data is stored
 - Do you have PII on hard drives?
 - Do you have PII on mobile devices?
 - If so, are the devices secured ?
 - Is the information encrypted?

RMTD Cyber/Data Security Insurance

- If your agency experiences a data / information security incident involving the unauthorized disclosure of private, non-public information
- **Please contact RMTD for additional information ASAP at 406-444-2421**
- State of Montana does have a cyber security insurance policy
- Numerous prevention tools/hints are also available on their website

Data Breaches are Expensive

- State of South Carolina DOR data breach exposed:
 - Approx 4 million taxpayers SSN
 - Approx 3.3 bank accounts numbers
 - Approx 700,000 businesses exposed
 - SC DOR has had to get a \$20.1 million loan to cover costs associated with exposure and may need another loan

Encryption

Limits in storage capacity of portable devices

Data loss prevention and protection software

Proper security of facilities security & hardware

Proper deletion of information hardware sold/destroyed

**RISK
MITIGATION**



Mgmt's Responsibility for I/C...

- Document Internal Controls
 - Maintenance/Review/Test/Update
- Educate your staff on a regular basis
- Take every opportunity to bring up the value or need for internal controls.

Internal Controls & Audits

Auditor responsibility;

- To plan & perform audit to obtain reasonable assurance about whether the financial statements are free of **material misstatement**, whether caused by error or fraud.
- To express an opinion on the financial statements
- To communicate in writing deficiencies on internal control and compliance

Internal Controls & Audits

Statement of Auditing Standard (SAS) 115 – Communicating Internal Control Related Matters Identified in An Audit

- Material Weakness;

a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Internal Controls & Audits

Statement of Auditing Standard (SAS)

115 – continued

- Significant Deficiency

a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Internal Controls & Audits

Other examples of Internal Control deficiencies:

- Absent or inadequate segregation of duties
- Absent or inadequate controls over safeguarding of assets
- Inadequate design of controls over the preparation of financial statements
- Employees or management who lack the knowledge to fulfill assigned functions

Auditor's ARE NOT responsible for ...

- Creating your internal control structure / procedures
- Reviewing/monitoring your internal control structure
- Finding incidents of fraud / misappropriation

Fraud, Waste or Abuse Hotline

- To report fraud, waste, and abuse in state government
 - 1-800-222-4446
 - 444-4446
- http://leg.mt.gov/css/audit/Fraud%20Hotline/fraud_hotline.asp
- Required per Section 5-13-311, MCA

Agency Theft/Suspected Theft

- MCA 5-13-309(3)
- The head of each state agency shall immediately notify both the attorney general and the legislative auditor in writing upon the discovery of any theft, actual or suspected, involving state money or property that under that agency's control or for which the agency is responsible.

Code of Ethics

- Montana Constitution, Article XIII, Section 4
- MCA Title 2 Chapter 2
- A public officer, legislator or public employee may not:
 - Disclose or use confidential information acquired in the course of official duties
 - Accept a gift of substantial value
 - \$50 or more for an individual
 - Receive salaries from 2 sep positions that overlap unless exceptions are met

Code of Ethics (cont.)

- A public officer or public employee may not:
 - Use public time, facilities, equipment, supplies, personnel, or funds for employee's private business purposes

MCA Title 17 – State Finance

- Chapter 1 – General Administration
- Chapter 2 – Accounting
- Chapter 3 – Federal Revenues /
Endowments
- Chapter 5 – Deposits/Investments
- Chapter 7 – Budgeting/Appropriations
- Chapter 8 – Disbursements/Expenditure

Other Resources

- MOM 399 – Internal Control Guidebook
- Cyber/Data Security RMTD
 - <http://rmtd.mt.gov/insurance/cyberdatainformationsecurityprotection.mcpix>
- State Code of Ethics On-line Presentation
 - http://pdc.mt.gov/content/docs/Code_of_Ethics
- ITSD Encryption Policy
 - <http://mt.gov/search.mcpix?q=encryptoin&via=homepage&cx=013380590290877010950%3A3ubczas3i44&cof=FORID%3A11&ie=UTF-8&q.x=0&q.y=0>

In Summary - Internal Controls

- Are required
- Need support of management
- Applicable to all areas within agency, not just central accounting offices
- Need to be documented/reviewed regularly
- Opportunity to improve operations, compliance and reporting