WASHINGTON STATE UNIVERSITY

# Audits and Internal Controls

**Presented by:**
Tami Bidle, Financial Reporting Manager, Business Services/Controller
Heather Lopez, Chief Audit Executive, Internal Audit

August 22, 2017 1

## Agenda

- Internal Control
- Who is Responsible
- Audits and Audit Process
- Components of Internal Control
- Resources

## WSU's Strategic Plan: Vision, Mission and Values

Washington State University's mission statement includes seven values critical to achieving our goals:

- Quality and excellence
- Integrity, trust and respect
- Research, innovation and creativity
- Land-grant ideals
- Diversity and global citizenship
- Freedom of expression
- Stewardship and accountability

3

***How can we, as an institution and as individuals, uphold the University's values and achieve our mission?***

***…through a strong system of internal controls***

4

## Internal Control

'Internal control is a process, effected by those charged with governance, management, and other employees, designed to provide reasonable assurance regarding the achievement of the entity's objectives relating to operations, reporting, and compliance.

… the state's internal control objectives are defined as the need for each agency to:

- Safeguard its assets.
- Check the accuracy and reliability of its accounting data.
- Promote operational efficiency.
- Encourage adherence to policies for accounting and financial controls.'

WA OFM SAAM Chapter 20 (20.15.10)

5

## Why is internal control important?

Good controls enable better management of institutional risk and provide for better preparation and ability to respond to the unknown.

Good controls provide assurance of compliance with laws, regulations and policies.

Good controls also seek to eliminate waste, fraud and abuse and help an entity avoid damage to its reputation and other consequences.

6

## Internal Control in WA State

WA OFM SAAM Chapter 20, Internal Control

20.10.40 Source of these policies

'These policies are based on and incorporate information from *Standards for Internal Control in the Federal Government* (Green Book) and *COSO Internal Control – Integrated Framework* (2013)'.

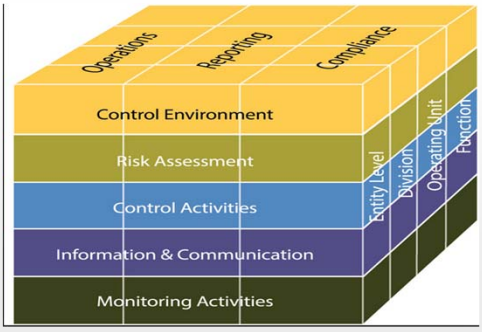
Effective date of changes, July 1, 2017

## What is COSO?

Committee of Sponsoring Organizations of the Treadway Commission

Under COSO, an organization's internal control system is deemed effective only if all five components (along with relevant principles) are both present and functioning.

It is not enough to design and implement a system of control. There must be processes to ensure continued assessment of risks and evaluation of controls working effectively and efficiently and modified as needed to ensure risk is mitigated sufficient to meet objectives.




9

Control Environment: The set of standards, processes, and structures that provide the foundation for carrying out internal control across the agency (SAAM 20.20.10).

Risk Assessment: A dynamic and iterative process for identifying risks to achieving agency objectives, analyzing the risks, and using that information to decide how to respond to risks (SAAM 20.22.10).

Control Activities: Policies, procedures, techniques and mechanisms that help ensure that risks are mitigated (SAAM 20.24.10).

Information and Communication: Necessary… to support the achievement of objectives. Communication is the continual, iterative process of obtaining and sharing necessary information (SAAM 20.26.10).

Monitoring: Process of evaluating the quality of internal control performance over time and promptly addressing internal control deficiencies (SAAM 20.28.10).

10

## Who is responsible for internal controls?

11

- Though leadership is ultimately responsible, everyone in an entity has some responsibility for the organization's internal controls.
- All personnel should be responsible to effect internal controls and to communicate problems in operations, deviations from established standards and violations of policy or law.

***Internal Controls are Everyone's Business!***

12

## Management's Role

- Management has responsibility to:
  - Assess risks to the organization of not meeting its objectives
  - Identify and develop appropriate controls to mitigate/manage identified risks
  - Implement controls and monitor them to ensure they are working as designed and are adequate

13

## Audit's Role

- Auditors test to ensure the controls and processes management has established and implemented are adequate to:
  - Ensure compliance with applicable rules
  - Safeguard resources
  - Properly present and report activity (reliable reporting)
  - Provide for effectiveness and efficiency in operations

14

## Auditors and Types of Audit

- Internal vs. External
- State vs. Federal
- Program Review
- Statutory/Mandated
  - Accountability
  - Performance
  - Bond Covenants/Contractual
  - Single Audit
- Financial

## Audits

- Audits have an objective to evaluate a process, system, unit, operation, program, etc. and tests are performed to ensure the internal controls implemented by management are working as designed.
- Audits yield memos or reports that provide results of tests and evaluations with recommendations for improvement.
- [Internal] Audits are performed according to schedule of audits in annual audit plan – developed as a result of annual risk assessment.

## General Audit Process

- Preliminary assessment of risks – scoping
- Planning procedures – data analysis, research of audit subject, interviews
- Entrance meeting with management
- Fieldwork – test of controls, test of transactions, interviews and walkthroughs, observation
- Closing – summarize issues noted, develop draft memo/report
- Reporting

## Focus on Design and Effectiveness of Internal Controls

- Auditors evaluate the controls management has put in place to mitigate the risk of objectives not being met. If no controls implemented or controls as designed are inadequate – recommendations are made for improvements.
- Auditors are evaluating the internal control system – review all components and how they are working together.

"Desperate people do desperate things. Loyal employees have bills to pay and families to feed. In a good economy, they would never think of committing fraud against their employers."

*2009 Report on Occupational Fraud, ACFE*

Occupational Fraud: "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."

*2016 Report to the Nation on Occupational Fraud and Abuse, ACFE*

19

## Contributing Factors for Fraud/Embezzlement

A strong system of internal control is the greatest fraud deterrent.

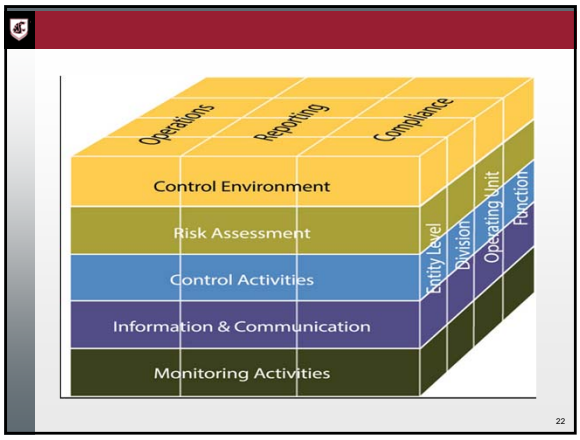
**Fraud Triangle**

- Opportunity: Poor internal controls, lack of oversight, Lack of segregation of duties, lack of clear direction on roles/authorities, poor employee morale due to management, work conditions, work load, other factors
- Pressure: Employees have additional outside pressure (economy bad everywhere, personal financial pressure, etc.)
- Rationalization: Employees under pressure to do more with less (affects attitude, competence and effectiveness)

20

## Investigations

- Investigations are unplanned, have a specific focus and ask: Who, what, when, how and why.
- Answering how: evaluate controls and gaps in controls.
- Investigations yield memos or reports that provide results of test to answer the question and usually recommendations to correct the concern.




## Control Environment

The Control Environment lays the foundation for the internal control system and provides the basis for carrying out internal controls across the organization. If poorly designed, executed or managed other internal controls can crumble.

A strong control environment includes:
- Commitment to integrity
- Exercised oversight accountability
- Enforced accountability
- Established structure, authority and responsibility
- Demonstrated commitment to competence

23

## Tone at the Top

- Ethics, Culture and Work Environment
- Conditions that impact control environment:
  - Leaders engaging in bad behavior – poor examples
  - Offenses not addressed, no consequences
  - Not providing or encouraging a means for employees to report wrongdoing
  - Rumor mill as source of "credible" information with no actions to directly address

## What you can do

- Ensure all employees, including managers and leaders, are aware of standards of conduct and ethics.
  - Provide training or means to get to training on a regular basis to reinforce as a norm.
  - Provide regular notices/reminders about ethics and standards and reporting avenues.
- Include compliance with standards of conduct as part of employee evaluations.
- Enforce consequences – do not turn a blind eye to bad behavior.

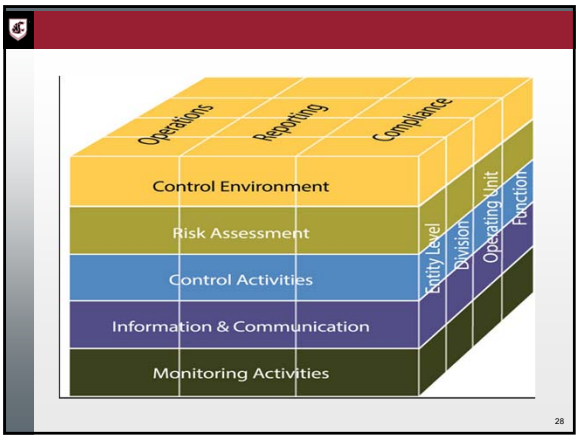
## Structure, Roles and Authority

- Ensure organization charts are current and include reporting lines.
- Position descriptions/duties/responsibilities need to be current and clear.
- Authorizations and delegations should be clearly defined.
- Significant processes should be in writing.

## People are Our Greatest Asset

…and can be our greatest risk.

- Demonstrate commitment to attracting and retaining competent employees.
- Ensure PDs accurately reflect expectations for position before posting.
- Ensure recruitment process and hiring personnel/committees understand desired skill sets and are trained to properly evaluate.
- Do reference checks – always!
- Provide opportunities for employees to gain continuing professional education to stay current and relevant in their field.

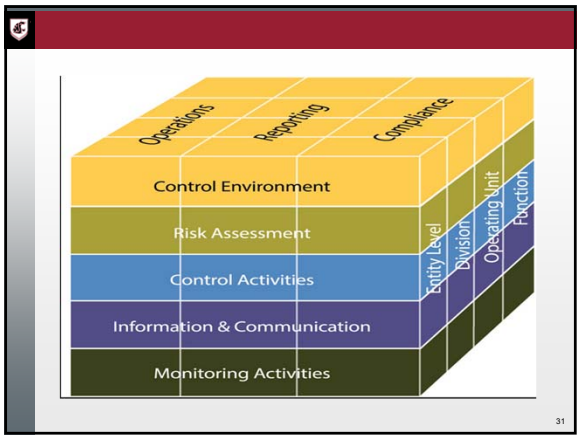



## Risk Assessment

- Identify and analyze risks to the achievement of objectives and use as a basis for determining how the risks should be managed.
- Risk responses:
  - Acceptance – no action take to respond
  - Avoidance – action taken to stop the process causing risk
  - Reduction – action taken to reduce likelihood or magnitude of risk
  - Sharing – transfer or share risks across agency or with external parties (such as insuring against losses)

## Responding to Changes

- Risk assessment and risk identification process considers changes in:
  - The external environment
  - The business model
  - Leadership
- Changing conditions may prompt new risks or changes to existing risks, management should analyze and respond to identified changes that could significantly impact its system of internal control in order to maintain its effectiveness.




## Control Activities

- Control activities are implemented through policies and procedures that should be reassessed periodically and refreshed as necessary
- Performed at all levels of the agency, at various stages within business process and over the technology environment.
  - Preventive controls = designed to deter the occurrence of an undesirable event by implementing procedures to avoid them
  - Detective controls = identify undesirable events that do occur and alter management about what has happened

## Segregation of Duties

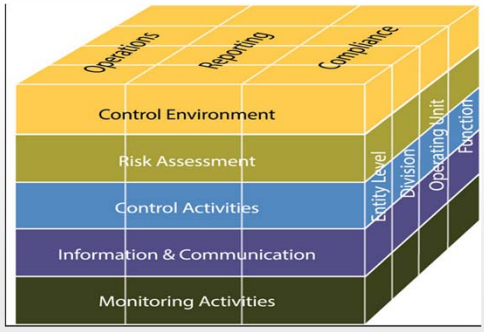
- No one person should hold responsibility for full string of a business process: record keeping, authorization, asset custody and reconciliation
- Where not practical, alternate control activities should be utilized
- Problems with lack of separation:
  - Errors may not be detected since an independent review of transactions may not be occurring
  - Inappropriate or unauthorized transactions are permitted to occur if one individual controls a major portion of the process

## Technology

- WA State OCIO policies should be considered
- Information systems and related control activities
  - Information system designed to obtain, store and process data – steps should be taken to safeguard that data
  - Define responsibilities, assigned to key roles and delegate authority
  - Restrict technology access rights

## Other Key Control Activities

- Authorizations, approvals and verifications
  - Develop written procedures outlining delegation guidelines
  - Never sign a blank form
  - Secure access to electronic signatures
  - No rubber stamping
- Monitoring, reconciliation
  - Means of detecting losses, errors or irregularity
  - Helps understand effectiveness of internal controls

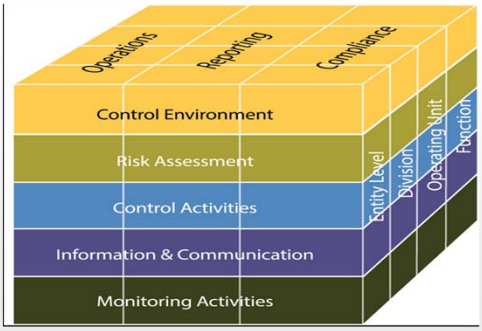



36

## Information and Communication

Management uses relevant and quality information from both internal and external sources to support the functioning of internal control.

- Relevant, useful data from reliable sources
- Data processed into information
- Communicated internally to employees to understand and carryout their responsibilities
- Communicated externally – controlled, relevant and timely




38

## Monitoring

Evaluating the quality of internal control performance over time.

*Can be ongoing or periodic, but looking at performance as a whole to evaluate if working as designed and still aligned with objectives.*

Baselines should be established, as should processes to evaluate results and communicate deficiencies.

| Internal Control Component | Related Principles (17) |
|---|---|
| Control Environment | Commitment to integrity<br>Exercise oversight responsibility<br>Establish structure, authority and responsibility<br>Demonstrate commitment to competence<br>Enforce accountability |
| Risk Assessment | Specifies suitable objectives<br>Identifies and analyzes risk<br>Assesses fraud risk<br>Identifies and analyzes significant change |
| Control Activities | Selects and develops control activities<br>Selects and develops general controls over technology<br>Deploys through policies and procedures |
| Information/Communication | Uses relevant information<br>Communicates – internal<br>Communicates – external |
| Monitoring | Conducts ongoing and/or separate evaluations<br>Evaluates and communicates deficiencies |

## Considerations for Key Business Processes

Purchasing cards

- Understand and comply with policy
- Safeguard cards when not in use
- Use temporary delegation form and checkout logs
- Review timely – follow up on variances
- Don't forget reconciliation to Balances

## Considerations for Key Business Processes

Payroll

- Management should ensure adequate separation of duties – the following should not be one person without appropriate oversight and approval:
  - Appoint personnel
  - Schedule hours
  - Approve hours worked
  - Post hours
  - Approve payroll reports

## Considerations for Key Business Processes

More on Payroll

- Time records are pay-affecting documents
- Never pre-approve or pre-sign
- Should be signed/certified by employee and supervisor after the fact
- Should reflect actual hours worked
- After certification, approved time records should not be returned to employee

## Considerations for Key Business Processes

Receipting and Cash Management

- Cash and checks should be deposited timely.
- Deposits should be intact and in proper composition.
- Funds should be properly safeguarded (before deposit and in transit).
- Numerical receipts should be used in order.
- If using other than official University receipt forms, contact University Receivables for review.
- Checks should be immediately restrictively endorsed.

## Considerations for Key Business Processes

Security of Data, Facilities

- Physical security *(lock doors, desk drawers, etc.)* and restrict access to keys.
- Computer security *(for desktops, shared, LAN servers)* - don't forget to protect portable devices.
- Establish backup and recovery / disaster recovery.
- Periodically review accessibility to programs – limit to those needed.
- Periodically change passwords and do not release.
- Restrict access to confidential data.

## Considerations for Key Business Processes

Physical Assets

- Equipment listings should be kept current.
- Equipment should be properly tagged.
- Equipment taken off premises should be logged.
- Equipment transfers should be approved.
- Maintenance contacts should be reviewed.

## Considerations for Key Business Processes

Reconciliation

- Reconciliation is a detective control.
- Departmental budgets should be reviewed monthly, timely and discrepancies investigated.
- Check budget statements to make sure transactions are:
  - Posted to the correct account
  - Listed as the correct amount
  - Expenditures are appropriate for account
  - Expenditures/receipts not posting that should
- Follow up on errors needing correction.

## Records Maintenance

- Be familiar with your unit's record retention schedule.
- Do not dispose of records
  - Before permitted per retention, or
  - If after retention period, records are under review of audit or public records request
- Records to be disposed should be shredded or disposed of appropriately.

48

## Be Familiar with Authoritative Governing Bodies and Their Policies

- Federal http://uscode.house.gov/
- State
  - RCW http://apps.leg.wa.gov/rcw/
  - WAC http://apps.leg.wa.gov/wac/
  - OFM http://www.ofm.wa.gov/
  - SAAM http://www.ofm.wa.gov/policy/default.asp
- Financial / Regulatory
  - NACUBO http://www.nacubo.org/
  - WSU Procedures, Records & Forms http://www.wsu.edu/~forms/links.html

49

## Resources

- SAAM Chapter 20 Internal Control – http://www.ofm.wa.gov/policy/20.htm
- WSU Internal Audit – 5-5336, ia.central@wsu.edu
- COSO Framework (2013) – www.coso.org
- SAO (Whistleblower program, Audits, Investigations) – http://www.sao.wa.gov

50