Office of Internal Audit

Budget Partners Presentation

June 2022

Agenda

- Office of Internal Audit and our Services
- Internal Controls
- Risk Management
- Fraud in Higher Education
- Ways to Report
- Top 20 University Risks

Office of Internal Audit

- Leah Ladley, Chief Auditor
  - CPA, CIA, CFE, CRMA
- Katie Bumgardner, Associate IT Auditor
  - CIA in process
- Brandi Fleck, Internal Auditor I
- Michelle Greene, Internal Auditor I

What we do

ASSURANCE:
- **Audits**
  - Positive assurance – things are good here
  - Or, recommendations for improvement
- **Risk-based**

Objectives → Risks → Controls

- **Controls:**
  - Are they designed correctly? If yes, then test; If no, make recommendation.
  - Are they working as intended? (evaluated through testing)
- **Two types of controls:**
  - Preventive
  - Detective
- Directive also considered as a control type

CONSULTING:
- You (the client) determine the scope of the project
    - Examples:
        - We find that we are unable to complete our current reconciliations of visitors to campus with deposits made for those charges due to short staffing. What else can we do?
        - We aren't sure our duties are segregated properly. Can you help?

TRAININGS:
- Sessions such as this
- Trainings for specific topics (research compliance, etc.)
- Other sessions

INVESTIGATIONS:
- EthicsPoint (hotline)
- Referrals
- Walk-ins, emails, other

What are Internal Controls?

Internal controls are the mechanisms that allow us to minimize risk and protect UO resources.

Internal controls allow the university to achieve goals, carry out management directives, reduce unpleasant surprises, enhance the reliability of information, promote effectiveness and efficiency of operations, safeguard assets, and com with rules and regulations.

Preventive controls – proactive in nature, intended to prevent loss, errors, or omissions

Detective controls – provide evidence after the fact of a loss or error and pl critical role in ensuring that preventive controls are working as intended

3rd type – directive control – policy, procedure, checklist, etc.

Common Internal Controls

- **Preventive:**
  - Authorization and approval
  - Continuity of operations
    - Business continuity plan
    - Disaster recovery plan
  - Safeguarding assets

- **Directive:**
  - Documentation
  - Policies, standards, and procedures

- **Detective:**
  - Management oversight
  - Monitoring
  - Reconciliation

- **Preventive and Detective:**
  - Segregation of duties*

*have at least two sets of eyes looking at transactions

Internal Controls

Top 10:

1. Control environment – leadership and tone at the top, middle, and everywhere
2. Approval, authority, and responsibilities
3. Reconciliation and reviews (monitoring)
4. [Segregation of Duties](#)
5. Protection of data and assets
6. Policies, procedures, and regulations
7. [Code of Ethics](#)
8. Values, integrity, and ethical practices
9. Documentation and records retention
10. Confidential hotline for reporting concerns

Segregation of Duties

Provides checks and balances in transactions

No individual employee should handle more than one of these functions:

Custody of assets	Record keeping
Authorization	Reconciliation

Examples of Segregation of Duties

- The person who approves purchases should not reconcile monthly financial reports
- The person who maintains accounting records or reconciles financial reports should not have custody of checks
- The person who opens mail and received payments should not make the deposit

Maintaining proper segregation is challenging when there is a small number of employees.

When challenged by staffing constraints:
- Place greater emphasis on monitoring by someone not involved in the process
- Require all employees to take vacation time and have someone else perform their duties while they are out
- Use transaction and activity reports to identify outlier transactions or unexpected trends
- Finding a way to reconcile monies received to monies expected is a strong step to take

Standards from the UO Code of Ethics

- ▶ Honesty and integrity

- ▶ Respect

- ▶ Stewardship and compliance

- ▶ Accountability and responsibility

Ethics

- Oregon Government Ethics Law (ORS Chapter 244):
  - Prohibits use of public office or position for financial gain
  - Requires public disclosure of financial conflicts of interest
  - Limits gifts that an official may receive per calendar year

Introduction to Risk Management

Risk Management → ← Internal Controls

- When a risk is identified, management may implement controls that will mitigate the risk, transfer the risk, or may even accept the risk.

- Identify the risk: recognize and be able to describe the risk

- Assess impact and likelihood: what is the potential severity and what is the likelihood of occurrence?

- Determine the risk treatment: avoid the risk (by process), mitigate the risk (with internal controls), or accept the risk {transfer the risk = insurance}

- Determine the risk owner: who is accountable for the control and the risk?

Example of Risk Management Process: Cash

- Risk: inappropriate safeguarding of cash resulting in loss

- Risk and probability – without internal controls, cash could be stolen, which would result in a loss to the University, and the probability of occurrence could be high

- Determining the risk treatment –
  - Avoiding the risk would mean not accepting cash (could negatively impact customer service)
  - Accepting the risk may not be acceptable either due to the high probability of loss
  - Implementing proper internal controls would be the best choice of risk treatment

- Risk Owner –
  - Normally, the person that has the overall responsibility of determining the risk treatment

Why we care about effective internal controls: FRAUD
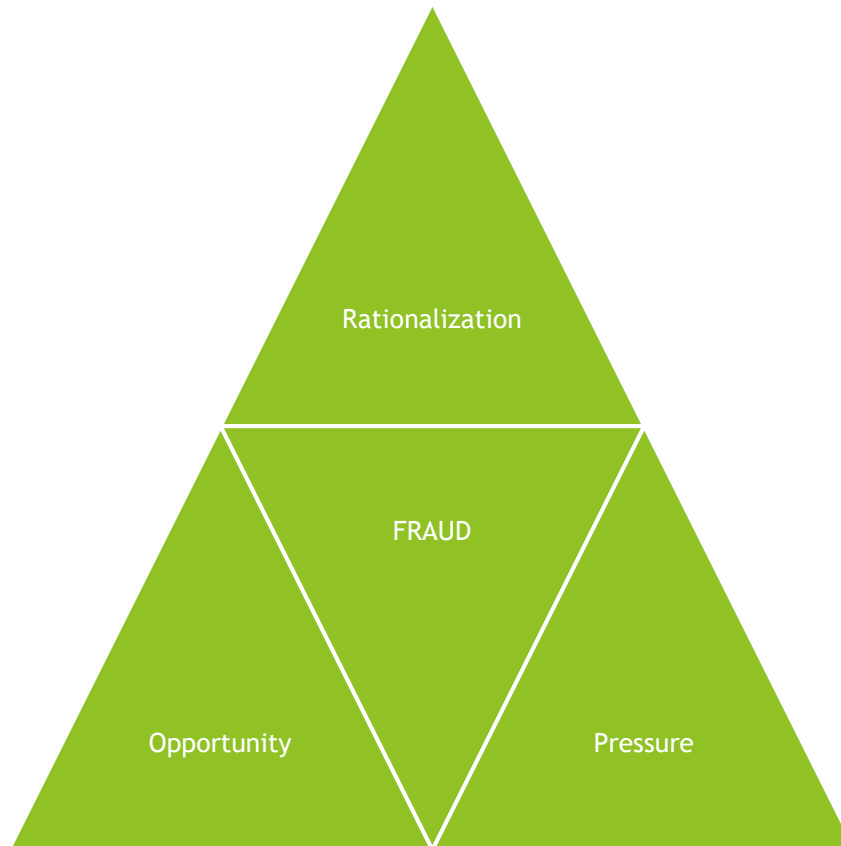
Donald Cressey's Fraud Triangle

Behavioral Red Flags Exhibited by Fraudsters

85% of all fraudsters displayed at least one of these red flags while committing their crime.

- Living beyond their means
- Financial difficulties
- Unusually close association with vendor or customer
- Control issues – unwillingness to share duties
- Irritability, suspiciousness, or defensiveness
- "Wheeler-dealer" attitude

Fraud in Higher Education

ADMISSIONS FRAUD	ACADEMIC FRAUD	CONFLICTS OF INTEREST
Paying someone to take a college entrance exam for a prospective student	Having someone else complete a student's assignments	Using one's position as a UO employee to solicit gifts or anything of value
Paying a university employee to approve a college application	Cheating to get a passing grade/changing or falsifying a grade	Awarding contracts to family members or for one's own interest
Changing a student's score or application information for admission purposes	Awarding a degree, scholarship, or internship that was not earned	Performing duties for another job during UO work hour

Fraud in Higher Education

FINANCIAL FRAUD

Taking or redirecting university funds for personal gain

Using university dollars for personal expenses or in any way that is not appropriate

GRANT FRAUD

Deceiving the sponsor or university about grant spending

Using grant funds for personal expenses or in any way inconsistent with the award

OTHER ASSET FRAUD

Using university equipment, property, or resources for unapproved purposes

Taking university equipment, property, or resources for personal use or failing to return equipment to the university

Ways to Report:

Do NOT attempt to investigate on your own! Report to others.

- Supervisor / Department Head / Unit Leadership

- Office of Internal Audit (call, phone, email)

- UO Hotline: **855-388-2710**

Top University Risks

Information Security

Risk: Scammers could obtain UO data and use it for harm to the university, employees, and students.

Control: Data protection is very important and information security policies and procedures can help protect your unit and the university (access controls, proper off-boarding, data segregation, and appropriate back-up/restoration procedures).

https://infosec.uoregon.edu/policies-procedures-and-standards

Unit Reconciliations and Segregation of Duties

Risk: Without timely reconciliations and segregation of duties, the risk of fraud or undetected error increases.

Control: Reconciliations completed in a timely manner and reviewed by someone other than the person completing; unit approver reviews supporting documentation for expenses and revenue; two sets of eyes on every transaction is the ultimate goal!

Conflict of Interest/Commitment and Outside Employment

Risk: Conflicts can compromise integrity and may result in fraud.

Control: Transparency and disclosure are key!

Management plans are developed to protect the individual and the university.

Compliance Training

Document delivery of training

Risk: When employees do not participate in training, they may not be aware of their compliance responsibilities, which may lead to instances of non-compliance.

Control: Annual and new hire compliance training is critical with specially developed training by and for the unit when compliance risk is elevated.

Business Continuity Plans and Disaster Recovery

Risk: Disruption of services provided by the unit, loss of information/data, confusion and frustration during time of a disruption or disaster.

Control: Development of a business continuity plan and the routine backup and safe storage of key data.

Business Continuity Plans are not just for Information Services/Technology!

Cash/Check Handling

Risk: Without proper cash handling procedures there is an increased possibility of loss or theft.

Control: The unit complies with UO cash handling procedures.

https://ba.uoregon.edu/content/cash-handling-and-departmental-deposits

Contracts

Risk: When unauthorized personnel sign contracts on behalf of the University, UO may be obligated for unallowable, questionable, or excessive costs.

Control: Engage the UO process!

Contracts and Grants in Research

Risk: Noncompliance could result in loss of federal funding, fines, penalties, and even sanctions against individuals.

Control: Principle investigators and all faculty and staff should be appropriately trained and comply with federal Uniform Guidance controls, including unallowable costs, effort certification, cost sharing, and export controls.

Fraud

Risk: The risk of fraud impacts employee morale and could costs the university precious funds, legal fees, and reputational damage.

Control: Ethical behavior, segregation of duties, and reporting your concern.

https://internalaudit.uoregon.edu/reportfraud

Emergency Management: Security, Health, and Safety

Risk: Not following safety protocols could result in injuries, accidents, and even fatalities.

Control: Awareness of what to do in an event and how to prevent accidents and crimes from occurring.

Business Expense Reimbursements

Risk: Noncompliance with policies regarding reimbursements for business expenses could increase fraud risk and reputational damage.

Control: Follow published guidelines, document business purpose and attendees, provide receipts where required, and follow expenditure limits.

Ethics and Tone at the Top

Risk: A lack of ethics and poor tone at the top can negatively impact employee morale and performance.

Control: Policies and procedures, published core values, ethical treatment of others, and consistency in behavior.

Remember – you are the tone at the top for someone!

Events on Campus

Risk: Noncompliance with event policies may lead to numerous issues for the university and its visitors.

Control: Education is key! Policies and procedures and even laws and regulations govern campus events, including the use of facilities, fees, catering, alcoholic beverages, security, training and background checks for those working with minors.

Gifts and Endowments

Risk: Noncompliance with endowment policies and gift acceptance procedures could result in future endowments not being approved by the Board, possible legal actions, negative public relations, loss of support, and donor dissatisfaction.

Control: Policies for the acceptance of gifts and endowments and appropriate use of funds per donor's wishes.

Human Resources

Risk: Noncompliance with UO HR policies could negatively impact employee morale and productivity and create other issues.

Control: Engage UO HR partners when hiring and follow the guidance provided to you.

Privacy

FERPA is a federal law designed to protect privacy of student education records.

HIPAA is a federal law requiring the protection of confidential medical information.

Risk: Inappropriate disclosures may result in harm to people, loss of federal funding, lawsuits, criminal charges, fines, and penalties.

Control: Appropriate systems/applications and training for persons who handle sensitive data.

Property

Risk: Without effective controls for the safeguarding of property, there is an increase risk of loss, theft, or damage.

Control: Property includes both tagged assets and non-tagged assets, such as computer monitors. Property should be properly safeguarded, periodically inventoried, and managed in accordance with policies.

Research Safety
(Animals, Humans, Labs)

Risk: Noncompliance with federal and state policies regarding lab safety and hazardous waste could result in injury and death, fines, penalties, and loss of research funding.

Control: Campus-wide safety and environmental programs are here to promote safety and compliance.

Purchasing Cards

Risk: Error or fraud, asset misappropriation.

Control: Maintaining documentation such as receipts and business purpose for purchase, separation of duties between cardholder and supervisor, reconciliation and review.

Travel

Risk: Error or fraud, asset misappropriation.

Control: All travel paid by UO should have a business purpose for the benefit of UO and should be performed in conformance with UO travel policies. Authorization should occur before travel dates and expense statements should be carefully reviewed for errors and overstatements.

Questions I Frequently Get:

1. How do I know what needs to have a policy?
2. Can you review my segregation of duties?
3. How did I get chosen for an audit?

Contact Information:
Leah Ladley, Chief Auditor
lladley@uoregon.edu
541-346-3200