Good Internal Control Practices and Fraud Prevention Tips

Jayne Blackburn, CPA
Audit Manager, UW Internal Audit

Laura Schrag
Senior Auditor, UW Internal Audit

November 2017

Table of Contents

Introduction

Course Objectives

- What are internal controls?
  - Gain an understanding of concepts.
- Why are internal controls necessary?
  - Establish importance and basic elements.
- Who is responsible for internal controls?
  - Explain roles and responsibilities in implementing internal controls.
- How do I implement internal controls in my department?
  - Provide guidelines for evaluating and enhancing internal controls in your unit.
- Implement procedures that can prevent fraud.
- Create an awareness of fraud symptoms (red flags).
- Gain an understanding of the University's fraud investigation process.

What are internal controls?

A Broad Definition of Internal Controls

A process effected by an entity's governing board, management, faculty, and staff, designed to provide reasonable assurance regarding the achievement of the following objectives:

- **Operations**
  - Effectiveness and efficiency of operations
- **Reporting**
  - Reliability of financial/non-financial reporting
- **Compliance**
  - Compliance with applicable federal/state/local laws and regulations

The definition of internal controls emphasizes the following:

- A *process* consisting of ongoing tasks and activities. It is a means to an end, not an end in itself.
- *Effected by people*. It is not merely about policy manuals, systems, and forms, but about people at every level of an organization that impact internal control.
- Able to provide *reasonable assurance*, not absolute assurance, to an entity's governing board and senior management.
- Geared to the *achievement of objectives* in one or more separate, but overlapping, categories.
- *Adaptable* to the entity structure.

Five Components of Internal Control

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Control Environment

- Foundation for all other components of internal control
- Sets the tone of an organization
- Provides discipline and structure
- Commitment to/model integrity and ethical values
- Leadership sets ethical tone (by example)
- Teach employees that the right thing matters
- Set expectations of appropriate behavior
- Address acts of misconduct and other wrongdoing
- Be clear on consequences of bad behavior (consistency)
- Commitment to competence
  - Hire the right staff (background/reference checks)
  - Invest in employee education
- Practice management accountability. Delegate or “empower” but…
  - Be clear on limits of authority
  - Be clear on responsibility and accountability

Risk Assessment

- Identify/analyze relevant internal and external risks to achievement of objectives
- Basis for determining how risks should be managed
- Risks include operational, strategic, regulatory, financial, reputational
- Identify/deal with risks associated with change
- Includes consideration of fraud

Control Activities

- Policies and procedures that help ensure that necessary actions are taken to address risks/achieve objectives
- Occur throughout the organization, at all levels, in all functions
- Include a range of activities such as reviews, approvals, authorizations, verifications, reconciliations, segregation of duties, security of assets

Objectives, Risks, Control Activities

- What you want to accomplish—Objectives
- What can get in the way/stop you from accomplishing objectives—Risks
- How do you decrease risks—Control Activities

Information and Communication

- Pertinent information identified, captured, and communicated in a form and time frame that enables people to carry out their internal control responsibilities
- All personnel must receive a clear message that control responsibility is taken seriously, understand their own role in the internal control, and how their activities relate to the activities of others
- Effective communication flows to external parties, and internally up, down, and across all levels

Monitoring

- Processes used to assess the quality of internal control performance over time
- Accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two

Internal Controls Can…

- Help achieve performance and profitability targets
- Help ensure reliable financial reporting
- Help ensure compliance with laws and regulations
- Help avoid damage to reputation
- Provide information on the entity's progress, or lack of it, towards achieving goals

Internal Controls Limitations

- Cannot guarantee that all risks are mitigated, and all objectives will be met
- Limitations exist in all internal control systems
- Human decision making/judgment can be faulty resulting in control failures/errors
- Controls can be circumvented and overridden

Characteristics of Effective Control

- Management expectations are communicated to all employees
- Procedures are performed by the right person
- Employees understand why controls are important—No rubber-stamping!
- Control activities are performed consistently
- Control activities are performed in a timely manner
- Errors/irregularities are identified and corrected
- Employees are held accountable for actions

Trust is not a control.

Why are internal controls necessary?

Reasons Why Internal Controls Are Necessary

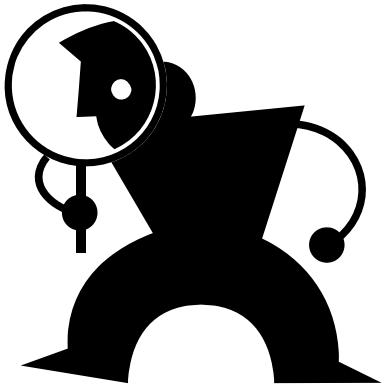
Obvious Reasons… Systems- or Finance-Related

Safeguard assets/funds	As a public institution, the University is responsible for protecting government assets against loss or misuse. It has this same responsibility to donors.
Prevent, detect, and correct errors and irregularities (fraud)	Controls are designed primarily to prevent errors and improper conduct. However, controls should also be designed to detect and correct.
Avoid cost of investigations and other related costs	If fraud is prevented, the University will spend less time and money investigating, litigating, and correcting.
Promote efficiency and cost effectiveness	Citizens and donors entrust resources to the University for specific purposes. It is not enough to simply safeguard assets; money must be used efficiently and effectively to achieve its intended purpose.
Provide reliable financial/ statistical reports	Decisions are as good as the information they are based on. Therefore, it is essential that we provide decision-makers with reliable data. The University has the responsibility to report on its stewardship of various resources. Reliable data is essential when reporting to sponsors and donors.
Ensure compliance with laws and regulations	The University's use of government resources is tightly controlled and limited by legal and contractual restrictions. Policies and procedures must ensure compliance with applicable laws and regulations.

Subtle Reasons…The Human Factor

Protect employees	Employees should never be put in a position in which their honesty could be questioned. An employee may be trusted not to steal, but it is unreasonable to trust them not to make mistakes, which can be as damaging as fraud. Errors or small-scale frauds can lead to termination of employment, which can produce tragic personal consequences.
Maintain employee morale	Suspicion and distrust created by a discovery of fraud can cast a shadow upon individuals in the department even if they weren't involved in the fraud.
Avoid public embarrassment and loss of public confidence	Frauds that have occurred in the past few years have brought increased media attention and scrutiny. Instances of fraud call into question the public's trust in the University.
Prevent whistleblowers and citizen complaints	Employee concerns not immediately addressed by management lead to complaints.

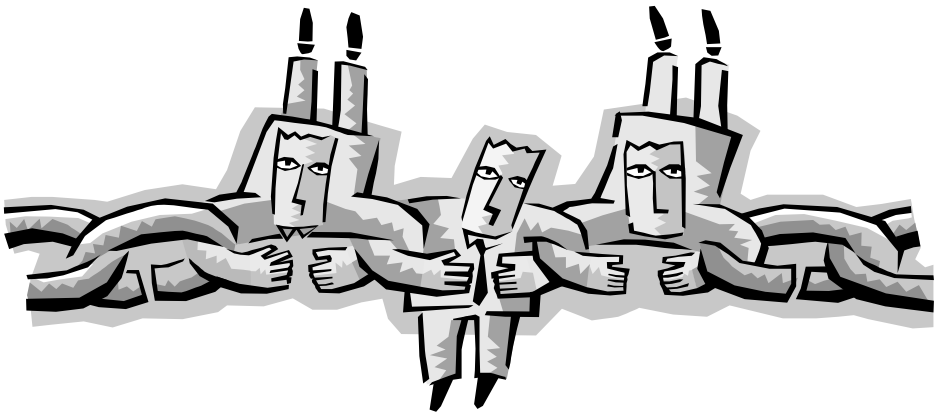
When a department is under scrutiny, internal controls become a focal point during an investigation.



Who is responsible for internal controls?

Roles and Responsibilities

- Everyone in an organization has responsibility for internal control; roles vary in responsibility and level of involvement with each component.
- The governing board has a key role in defining expectations on integrity/ethical values, and internal control responsibilities.
- The CEO is ultimately responsible for the effectiveness of the internal control system.
- Senior management guides the development and implementation of internal control policies and procedures, which are executed by all personnel directly involved at a detailed level.
- Internal auditors evaluate the effectiveness of internal controls, but do not develop/implement/maintain them.



How do I implement internal controls in my department?

Type of Controls

- Detective: Designed to detect errors or irregularities that may have occurred
- Corrective: Designed to correct errors or irregularities that have been detected
- Preventative: Designed to keep errors or irregularities from occurring in the first place
- Manual Controls
- Automated Controls

Control Design and Operating Effectiveness

- To meet objectives and mitigate risks, the controls must be adequately designed, and operate as designed
- One design does not fit all; design depends on objectives, risks, circumstances
- Operating effectiveness also depends on circumstances
- Can have adequate control design, but if not operating as designed, objectives are not met, and risks are not mitigated
- Can have adequate control operating effectiveness, but without adequate design, objectives are not met, and risks are not mitigated

Basic Elements of Internal Control

- Separation of duties
- Authorization
- Documentation
- Reconciliation and review
- Monitoring
- Safeguarding of assets and records
- Information systems security

Separation of Duties: Checks and Balances

No one person should have complete control over all aspects of a financial transaction. Ideally, no single individual should be able to:

- Authorize a transaction,
- Account for the transaction, and
- Have custody of the asset relating to the transaction.

Why?

- Protects employees
- Prevents and detects intentional and unintentional errors
- Discourages sloppy performance of duties

Things to Remember

- The cost of internal controls should never exceed the expected benefit. Sometimes realignment of duty assignment may be all that is necessary to accomplish the objective.
- Separation of duties can be circumvented by collusion.
- Management should take a more active role in overseeing operations when fiscal office staffing prohibits or restricts appropriate separation of duties.
- Mandatory vacation policy, periodic rotation of duties, and analytic reviews are useful tools if appropriate separation of duties is not practical.

Authorization

Transactions should be authorized and executed by persons acting within the scope of their authority.

Why?

- Prevents invalid transactions

Things to Remember

- Individuals should understand the significance of what they are approving, as well as their responsibility and accountability in the approval process.
- Policies and procedures should clearly state which individuals have the authority to approve different types of transactions.
- Authorization should be obtained in advance, if possible, and documented (written or password-secured email).
- Approvers should review supporting information to verify the propriety and validity of transactions, or should have first-hand knowledge of transactions being approved.
- Authority can be delegated, but delegation must be in writing.
- Ensure that inappropriate charges cannot be made to a document after it has been authorized.
- Comply with GIM 2 delegation policy—update delegation when changes occur.
- Ensure receipt of goods or services before approving payment of invoice.

Documentation

Internal control systems and all transactions are to be clearly documented and the documentation should be readily available for examination.

Why?

Systems Documentation:

- Avoids disruption of activities in case of employee turnover.
- Outlines specific authority and responsibility of employees.
- Promotes consistency in how transactions are processed.
- Serves as a reference tool for employees seeking guidance on the handling of less frequently encountered transactions/situations.
- The internal control system (policies, procedures) should be documented and made available to all employees.

Transaction Documentation:

- Ensures accuracy and completeness of transactions.
- Ensures assets are properly controlled.
- Provides evidence of UW business purpose.
- Provides evidence of what really happened.

Things to Remember

- Documentation should be:
  - Prepared at the time the transaction takes place.
  - Recorded in ink.
  - Retained in accordance with the University Records Retention Policy.
- Documentation should include sufficient detail to support the transaction and any amendments.
- Key documents should be sequentially numbered to ensure that all documents can be accounted for.
- Voided/spoiled documents should be retained.

Reconciliation and Review

Reconciliation: The process of comparing accounting data with the underlying items they represent, e.g., reconciling payroll records to MyFD.

Review: An inspection or examination that takes place for the purpose of evaluating something.

Why?

- Ensures accuracy of information
- Proves existence of assets
- Ensures controls are operating properly

Things to Remember

- Reconciliation and review should be done on a timely basis.
- Routinely review “high risk” or unusual transactions, e.g., excessive voids on cash register tapes.
- Source documents should be used in the reconciliation process.
- Investigate and resolve differences. Follow-up!
- Review unusual documentation (e.g., top of cash register tape is cut off, units on invoice do not match the type of merchandise, credit card voucher without description, whiteouts, Rediform receipts, double endorsements).
- The reconciliation process should be documented.

Monitoring

- Is the internal control system effective?
- Ongoing, integrated in the business process
- Managerial and supervisory reviews
- Examples:
  - Actual vs. budget, forecasts
  - Performance reviews of activities/initiatives
  - Review of unexpected results, trends
  - Routine self-assessment (audits)

Safeguarding of Assets and Records

Access to assets and records should be limited to authorized individuals. Accountability for custody and use of resources should be assigned and tracked.

Why?

- Protects assets and records from unauthorized use, loss, or theft
- Avoids the costly and time-consuming redevelopment of records

Things to Remember

- Deposit cash receipts in a timely manner.
- Sensitive items should be kept in a locked storage area at all times when not in use.
- Specific individuals should be assigned responsibility for the custody of specific assets and records.
- Access (i.e. safes, files) should be limited to minimum number of individuals and based on job duties.
- Employees should go through a “check out” procedure when their employment status changes.
- It is best to keep confidential records separate from the rest of the files.
- Consider insuring valuable equipment.

Information Systems Security

Information stored and sent via computer is at risk of disclosure or modification. The confidentiality and sensitivity of the data should be assessed to determine what controls should be in place to protect the information.

Why?

- Secure sensitive and confidential information
- Protect computers and data from theft or damage
- Availability of data

Things to Remember

Data and Records Management (sensitive, confidential, financial, and research data)

- Understand the nature of the data generated and used.
  - Public
  - Restricted
  - Confidential
- Comply with regulations (HIPAA, FERPA).
- Store and manage data in compliance with UW records management and retention policies. (Records Management web page http://f2.washington.edu/fm/recmgt/)
- Protect physical assets (desktops, laptops, servers) from theft or damage.

Access Controls

- Systems must be able to identify and authenticate users.
- Access privileges need to be authorized and documented.
- User access must be based on a unique identifier that is not shared.
- Access must be based on “need to know, need to have.”
- As employee duties change, access to data needs to be reviewed to ensure least privileged.
- Close all accounts and remove all access capabilities related to separated employees.

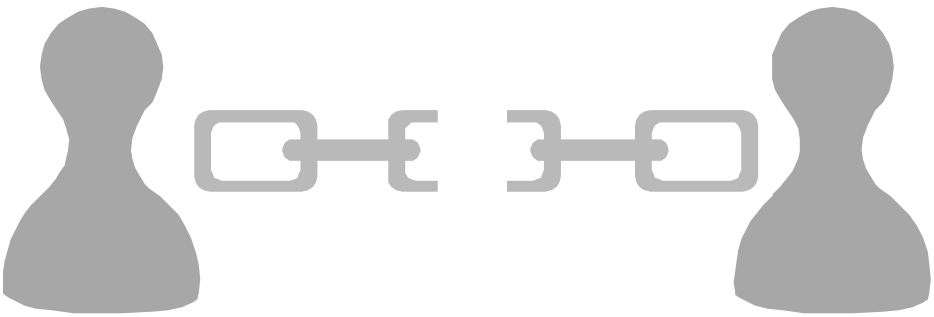
- User data access and modification privileges should support other internal controls:
  - Segregation of duties
  - Protection of assets
  - Transaction authorization

Physical Security

- Critical computers and servers must be housed in protected areas that are away from heavy traffic patterns, and restricted to authorized individuals.
- Computers should be protected from environmental hazards.
- Computer labs must be secured (safeguard asset).
- UW laptops, wireless services, and other mobile computing devices should have check out procedures and identification marks/tags to prevent their theft or compromise.

Common Causes of Internal Control Breakdowns

- Wrong tone at the top
  - Arrogance—"above the rules"
  - Too creative; looks for shortcut
- Lack of communication/collaboration
  - Shortchanged, mistreated, ignored
  - "Not my problem"
- Lack of training, understanding, or experience
- Understaffed
- Collusion
- "Can't afford any more controls"
  - Some risks are unavoidable
  - Weigh cost vs. benefit
- To err is human
  - Errors in actions and judgment



A Guide to Creating Your Own System of Internal Controls

1. Identify the function, activity, or transaction cycle to be reviewed.

2. Document your understanding of the system.

3. Identify the internal control objectives for the system.

4. Determine/brainstorm how errors, frauds, or non-compliance could occur.

5. Determine whether internal control procedures currently in place are adequate to prevent errors, frauds, or non-compliance.

6. If current procedures are inadequate, or if no controls exist, determine which procedures would reduce the risk of errors, frauds, or noncompliance from occurring.

7. Determine the cost of such procedures and compare them to the estimated benefits of implementing the procedures (cost vs. benefit).

8. Make a decision on whether to implement the new procedures.

9. Implement the new procedures.

10. Obtain feedback, analyze and evaluate the effectiveness of the new procedures, and take corrective action, if necessary.

11.

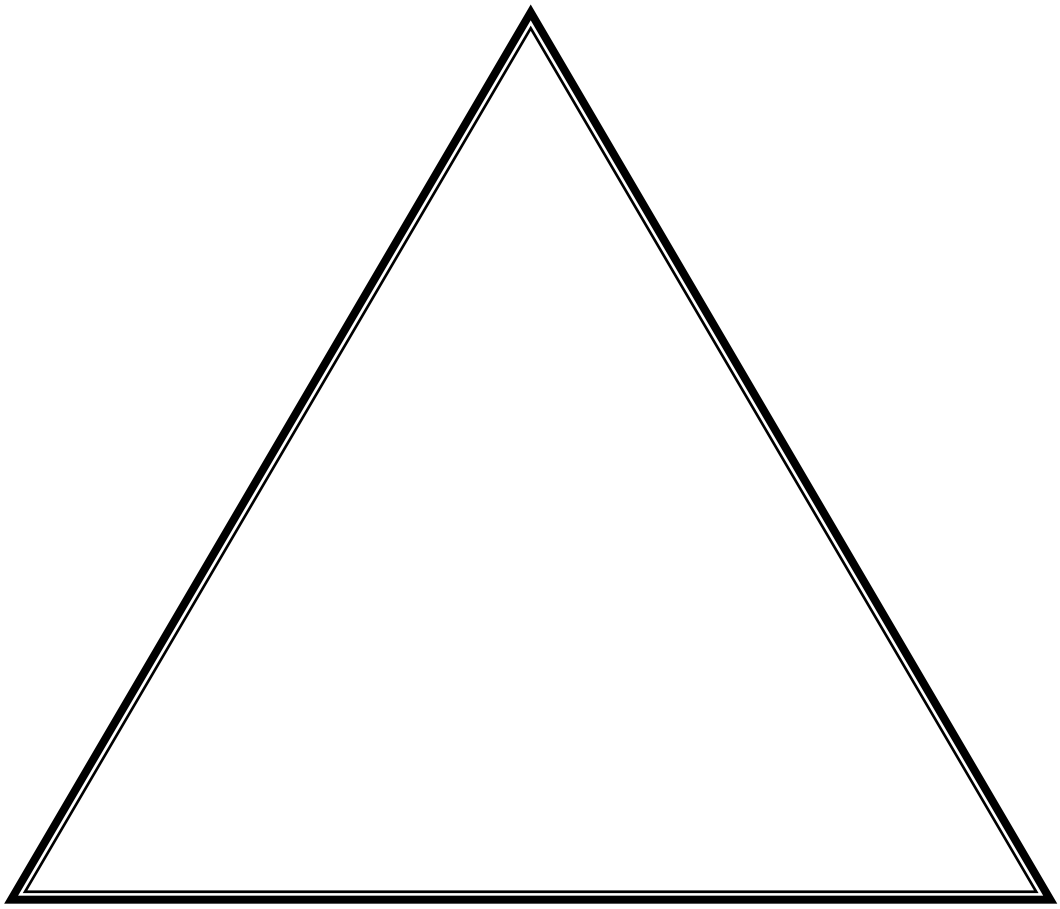
Fraud

What Is Fraud?

- Forgery or alteration of reports, documents, or computer files
- Misappropriation or misuse of University assets (i.e., equipment, supplies, cash)
- Authorizing or receiving compensation for goods not received or services not performed
- Authorizing or receiving compensation for hours not worked.
- Any irregularity in the handling or reporting of money transactions
- Use of University facilities and equipment for private financial gain
- Acceptance of kickbacks or bribes
- Other related illegal acts (i.e., misuse of a U-PASS, email account, or the Internet)

Fraud Triangle

Opportunity



Pressure

Rationalization

Fraud Reporting

Reporting	Notification	Corrective Action
Faculty and Staff Report allegation to management or to Internal Audit. Department managers should not conduct their own investigation. Management should immediately report suspected fraud to Internal Audit.	Internal Audit Notify: 1. State Auditor's Office 2. UW Division of the Attorney General's Office 3. UW Police Department 4. UW Risk Management 5. Appropriate University Human Resources Official	Internal Audit Investigates and concludes on the allegation and issues report. State Auditor's Office Reviews Internal Audit's work, conducts additional audit work if necessary, and issues report. UW Division of State Attorney General Is involved with the legal process and interactions with the State Attorney General's Office. (Recovery action) UW Police Prepares the documents for criminal proceedings and interacts with the King County Prosecutor. (Criminal action) Receivables Collection Office Coordinates the restitution process. (Recovery action) Risk Management Coordinates with insurance company. Appropriate University Human Resources Official Handles the employee/faculty disciplinary actions. (Personnel action) Affected UW Department Protects accounting files. Files police report. Takes corrective action to improve internal controls. (Corrective action)

Types of Fraud

On Book	**Manipulated accounting records**

Off Book	**Bribes, kickbacks, conflict of interest**

Types of Fraud Perpetrators

Active	**Driven by motivation or greed (crook)**

Passive	**Driven by temptation (weakness in internal controls; honest, but gave in to temptation)**

Consistent Patterns in Fraud Cases

- The #1 internal control weakness is “blind trust” (the “trusted employee”)
- Lack of Separation of Duties—The employee controls the entire process
- Passive Frauds—Driven by temptation or a weakness in internal controls
- Progressive—Frauds generally start out small
- Simple methods
- Repeat offenders
- Admit to what they think you know
- The employee seldom takes leave and/or nobody does the employee’s duties when absent
- The employee works evenings and weekends or at home

Fraud Prevention Tips

Payroll

- A foreign research scientist received an extra $1,450 when he was put on the payroll 21 days before he started work as a mechanism to pay his graduate school tuition.

Red Flags

Employee is not on site, or is not known to other department personnel.

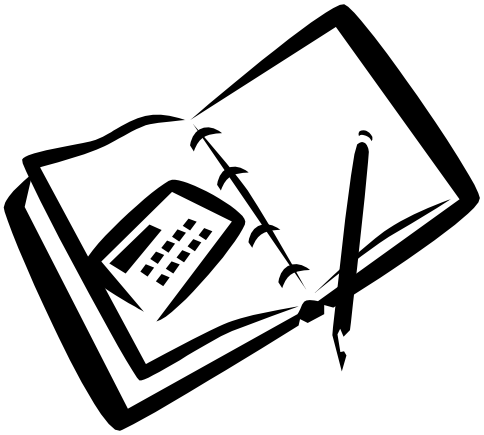
Information in the personnel file does not agree with payroll records.

Hours entered are unusual (e.g., 16.43; 20.56).

What can you do to prevent this type of fraud?

Controls: Documentation, Reconciliation, Review

- Ensure proper supporting documentation before entering into Workday.



Payroll

- An employee was instructed by management to pay herself 8 hours of overtime each pay period as a way to increase her pay. This practice went on for 16 years totaling over $27,000 in overpayments.

Red Flags

Same overtime hours each pay period.

What can you do to prevent this type of fraud?

Controls: Control environment

- Encourage employees to communicate problems, issues, or any deviation from established policies and procedures.
- Provide training on ethics and internal controls.

Purchasing: Petty Cash

- Employees have submitted receipts for non-University purchases.
- Employees have submitted duplicate receipts for fraudulent reimbursement.
- Employees have fabricated false receipts for fraudulent reimbursements.
- Employees may have easy access to websites and/or software that generate false receipts.

Red Flags

Description on the petty cash form does not match the receipt.

The top part of the cash register tape is cut off.

Same transaction number.

Unusual vendor/store location.

What can you do to prevent this type of fraud?

Controls: Separation, Authorization, Reconciliation, Review

- Separate the preparation, approval, and reconciliation functions among at least two employees.
- The person who authorizes petty cash should review supporting documents for reasonableness. (Supporting documents include cash register receipts, invoices, and certain credit card slips.)
- The person who reconciles the MyFD should investigate and resolve such things as missing supporting documentation and unusual or missing approval signatures.

Purchasing: Departmental Revolving Fund

- A petty cash custodian misappropriated $2,612 by diverting departmental petty cash funds into her personal checking account. She deposited reimbursement checks to her own checking account, and she issued petty cash checks to “cash” or to herself.
- A custodian of a departmental petty cash fund embezzled approximately $38,000 over four years. She wrote checks to “cash” herself and held back cash when depositing the petty cash reimbursement check.

Red Flags

Custodian is frequently “out of money” and tells employees they will have to wait for reimbursement.

Custodian works many evenings and weekends “to get work done.”

Custodian rarely takes time off.

Checks written to “cash.”

Checks written to custodian.

Overdraft notices from the bank.

Checks used out of sequence.

Missing supporting documentation.

What can you do to prevent this type of fraud?

Controls: Separation, Reconciliation, Review

- A manager or principal investigator should review for reasonableness and authorize petty cash reimbursement requests.
- The custodian should not approve his/her own expenditures.
- The department should not retain pre-authorized blank forms or checks.
- Maintain separate petty cash fund if cash is needed.
- An independent person should reconcile the bank statement to the check register and the authorized fund on a monthly basis.
- The bank reconciliation should include the following:
  - Review endorsements of canceled checks for any irregularities.
  - Account for all pre-numbered checks issued, including “voids.”
  - Review any checks made out to “cash” or to the custodian.
  - Include supporting documentation for reconciling items (e.g., outstanding checks, in-transit deposits).
  - Verify that deposits to the account are supported with a petty cash reimbursement. (No other funds should be deposited to the account.)
  - Date and sign the reconciliation.

Purchasing

- The Assistant Director misappropriated $7,375 in University resources over a two year period by using eProcurement and ProCard to purchase personal items.

Red Flags

One individual had full control of the purchasing process

Monitoring – reviewers not knowledgeable of department activities

What can you do to prevent this type of fraud?

Controls: Separation, Reconciliation, Review

- Support documents should be reviewed for reasonableness and reconciled to MyFD by someone other than the purchaser.
- Reconciliation should be performed in a timely manner by somebody who is has knowledge of department activities.
- Purchasing duties should be delegated to staff, with management approving and reviewing all purchase activity.

Purchasing: ProCard

- An employee was able to eliminate a second person from reconciling his ProCard transactions, resulting in a $200,000 misappropriated in two years.

Red Flags

Missing supporting documentation to support UW purpose.

Credit, error, repayment notation.

Explanations do not make sense.

Questionable vendor/merchant name and location.

Cardholder approved own purchases.

Reconciler could not access PaymentNet transactions.

Cardholder supervised reconciler.

Lack of understanding of reasonability.

What can you do to prevent this type of fraud?

Controls: Separation, Documentation, Reconciliation, Review

- Cardholder purchases should be approved by another person.
- Support documents should be reviewed for reasonableness and reconciled to the monthly ProCard statement and/or MyFD by someone other than the cardholder.
- Reconciler should verify/confirm cardholder notes such as credits, repayments, committee approvals.
- Print, sign, and date monthly statement to indicate reconciliation was performed by the cardholder and reviewer.

Purchasing

- Employees were able to purchase items using University budgets and then sell them on eBay or return to vendor for personal gain.
- Employees shipped personal items at University expense.

Red Flags

The budget used for the purchase.

The quantity of items purchased.

Destination to/from on shipping invoices.

What can you do to prevent this type of fraud?

Controls: Separation, Reconciliation, Review

- Support documents should be reviewed for reasonableness and reconciled to MyFD by someone other than the purchaser.
- Reconciliation should be performed in a timely manner.

Purchasing Review

The person who authorizes/reconciles purchases should review the following:

- ❒ The frequency with which the item is purchased
- ❒ The necessity of the item purchased
- ❒ The quantity and dollar amount on the cash register receipt
- ❒ The store location at which the item was purchased
- ❒ Day of the week the item was purchased
- ❒ Whether the description on the cash register or credit card receipt matches the description on the petty cash voucher, ProCard notes, or reimbursement request
- ❒ The validity of the type of documentation

Cash Receipts

- A manager was able to misappropriate at least $5,400 in 4 months by taking cash receipts without being identified. He took money from the cash register till and from locked money bags. The money could have been taken by at least 35 different employees.

Red Flags

Larger than normal daily shortages from cash register till.

There was no accountability by cashier.

The safe was left on "day lock."

Keys to the money bags were left on top of the safe.

What can you do to prevent this type of fraud?

Controls: Review/reconciliation, Safeguarding

- Have one cashier responsible for the cash drawer (per shift, per day).
- Limit access to the safe.
- Limit access to money bags and keys.
- Inform employees of responsibilities and accountability expectations.
- Management should review reports that are over and short, and look for unusual trends.
- Management should perform analytical reviews of revenue trends (i.e., compare actual to expected, compare prior time period to current time period).

Cash Receipts

- An employee was able to misappropriate $6,600 in 18 months from key deposits.

Red Flags

The department received overdraft notices for the key deposit bank account.

What can you do to prevent this type of fraud?

Controls: Separation, Reconciliation, Review

- Separate the duties of depositing funds and reconciling the bank statements and MyFD.
- Reconcile deposits to bank with the source document (i.e. cash receipt book, cash register "z" reading).
- Analytical review of annual revenues.

Travel

- A traveler was reimbursed $800 for personal travel that was combined with University travel (airfare, hotel, per diem, parking).
- A vice president misappropriated $3,600 by having the University reimburse him for personal travel.
- A traveler was reimbursed $900 for travel from an outside agency for presenting a talk. The University also reimbursed him.

Red Flags

No business connections or purpose at travel destination.

Insufficient documentation for UW business purpose.

Traveler presenting a “paper” or “talk.”

Travel to the same location several times.

Travel approved by subordinate.

What can you do to prevent this type of fraud?

Controls: Authorization, Review

- Person who approves travel should have knowledge of the traveler’s work.
- Review destination for reasonableness.
- Travel should be approved at level above the traveler.
- Person who approves eTravel should ask the traveler if he/she was reimbursed by another party.
- Compare travel reimbursement request to conference material/other travel documents to ensure appropriate reimbursement.

Travel

- Individual CTA (travel visa card) used for personal use
- Personal leg of trip claimed as University travel
- Free airline tickets for being “bumped” used for personal use
- Per diem claimed for voluntary “bump” from airline
- Airline tickets cancelled due to personal reasons, kept for personal use

Refunds

- A student employee processed 96 invalid refunds to his personal Husky Card resulting in the misappropriation of $32,494 in University funds over a period of three years.

Red Flags

Unrestricted access to the card machine

No monitoring of monthly budget activity

No daily reconciliation of sales and refund activity

What can you do to prevent this type of fraud?

Controls: Separation, Reconciliation, Review

- Restrict access for processing refunds to authorized personnel only
- Document and reconcile all refunds and voided transactions
- Reconcile/review monthly budget activity

Appendix

Internal Controls—A Guide to Separation of Duties: Procard Functions

PROCARD FUNCTIONS	This guide may vary depending on the organizational unit's structure and the number of employees available to perform these functions.

WHAT To Do	**WHY To Do It**	**WHO Should Do It**	
		Department With Only Two Employees	***Department With More Than Two Employees***
Review PaymentNet system (e.g., weekly email, transaction screen) to ensure transactions were made by the cardholder.	Ensure funds are used for authorized expenditures.	Cardholder	Cardholder
Verify that sales tax, budget number, and object code for each transaction are properly applied.	Ensure funds are properly charged to budgets.	Reconciler	Reconciler
Reconcile transactions to valid supporting documentation (e.g., itemized receipt, invoice, packing slip, and pre-approval documentation, if applicable).	Ensure funds are properly supported and approved.	Reconciler	Reconciler
Approve or dispute transactions.	Ensure purchases are appropriate, valid, and in compliance with applicable departmental, University, and procard policies.	Supervisor	Supervisor
Reconcile transactions on MyFD to the procard statement or PaymentNet.	Ensure transactions on MyFD are valid and properly supported.	Reconciler	BAR Reconciler

Note: Cardholders should not reconcile or approve their own transactions. For example, a reconciler who is also a cardholder should have their supervisor review and approve their transaction log.

Internal Controls—A Guide to Separation of Duties: Petty Cash Functions

PETTY CASH FUNCTIONS	This matrix is a guide. Separation of duties may vary depending on the organizational unit's structure and the number of employees available to perform petty cash functions.

WHAT To Do	**WHY To Do It**	**WHO Should Do It**	
		Department with Two Employees	***Department With More Than Two Employees***
Make payouts based on valid support documents (cash register receipt, paid invoice).	Ensure funds are not paid out for fictitious or non-University expenditures.	Custodian	Custodian
Reconcile fund, including bank account, if petty cash is maintained in checking account.	Ensure money is not missing from fund. Ensure other funds are not co-mingled.	Custodian	Someone other than the custodian
Request petty cash reimbursement from UW Accounting Operations.	Ensure money is not missing from fund. Ensure other funds are not co-mingled.	Custodian	An authorized person, other than the custodian
Authorize Washington State Invoice Voucher; review support documents.	Ensure payouts are reasonable and appropriate. Ensure money is not missing.	Supervisor	Supervisor

Internal Controls—A Guide to Separation of Duties: Cash Receipt Functions

CASH RECEIPT FUNCTIONS	This matrix is a guide. Separation of duties may vary depending on the organizational unit's structure and the number of employees available to perform cash receipts.

WHAT To Do	**WHY To Do It**	**WHO Should Do It**	
		Department With Only Two Employees	***Department With More Than Two Employees***
Take in cash and issue a pre-numbered receipt, or ring up on cash register.	Establish record of cash received.	Cashier	Cashier
Balance sales revenues to pre-numbered receipts or cash register total.	Ensure all cash receipts are accounted for.	Cashier	Supervisor
Prepare deposits in a timely manner.	Ensure cash receipts are deposited.	Cashier	Cashier or Independent Person
Reconcile cash receipt records (pre-numbered receipt book, cash register total) to validated cash transmittal and BAR. Investigate irregularities.	Ensure cash receipts are deposited.	Supervisor	Supervisor

Internal Controls—A Guide to Separation of Duties: Payroll Functions

Payroll Functions	This matrix is a guide. Separation of duties may vary depending on the organizational unit's structure and the number of employees and number of employees available to perform functions.

WHAT to Do	**WHY To Do It**	**WHO Should Do it**	
		Department with Two Employees	***Dept With More Than Two Employees***
Authorize new hires and payroll changes.	Ensure employee and pay is valid.	Supervisor or Principal Investigator	Supervisor or Principal Investigator
Enter payroll data into Workday.		Payroll Coordinator	Payroll Coordinator
Approve changes.	Ensure employee and pay is valid, and pay is accurate (correct classification, rate, and budget).	Supervisor	Supervisor
Approve time records.	Ensure records reflect actual hours worked and leave taken. Ensure timely completion of forms.	Supervisor	Supervisor
Review check register.	Ensure payroll is accurate.	Payroll Coordinator or Supervisor	Payroll Coordinator or Supervisor
Pick up and distribute checks.	Ensure payment is to valid employee.	Payroll Coordinator	Someone not involved with payroll function
Reconcile time records and payroll adjustments (i.e. RST).	Ensure information is accurate.	Payroll Coordinator	Someone not involved with payroll function
Review MyFD for reasonableness.	Ensure payroll is accurate.	Supervisor or Principal Investigator	Supervisor or Principal Investigator
Authorize monthly Grant & Contract Certification Reports.	Ensure payroll charged to grant is accurate.	Principal Investigator	Principal Investigator

Common Audit Findings

Payroll

Authorization

- Timesheets are not approved by employees and by supervisors with first-hand knowledge of hours worked.
- Overtime is not approved in advance or not approved at all.
- Timesheets are not approved on a timely basis.
- Grant and Contract Certification Reports are not approved by the Principal Investigator.

Documentation

- Timesheets do not contain detail needed to properly allocate employee time to specific projects.
- Hours worked by temporary employees are not documented (payment based on estimate or prearranged amount).
- Classified Staff and Professional Staff Level I employees do not complete timesheets with weekly totals.
- Late pay is not properly recorded.

Reconciliation/Review

- Excessive overtime is not being monitored.
- Departments do not review hours to ensure compliance with the 1,050 Rule for hourly employees.

Safeguarding

- Departments do not have formal checkout procedures when employees leave the department.

Purchasing/Petty Cash

Separation of Duties

Departmental Petty Cash

- The same person makes payouts and reconciles the bank statements to the check register, and to the authorized fund amount.
- The same person approves and processes reimbursements from the petty cash fund and authorizes the State of Washington invoice voucher to reimburse the fund.

Purchasing

- The person authorized to approve purchases online is the same person who reconciles transactions to MyFD.

Authorization

- Purchases are approved by individuals not familiar with the program or project.
- Travel is approved by an individual reporting to the claimant.
- Delegations of signature authority are not in writing or not updated.
- Petty cash voucher is returned to the requester after approval.
- Unauthorized cash funds.
- Prior approval is not obtained from sponsors when required (e.g., purchase of general purpose equipment).

Purchasing/Petty Cash, cont.

Documentation

- Evidence of receipt (e.g., a packing slip) is not obtained.
- Packing slips are not signed and dated.
- Interdepartmental charges are not properly supported.
- Void or cancelled checks are destroyed.
- Petty cash reimbursements are not adequately supported, e.g., description on Petty Cash Voucher does not match description on cash register receipt.

Reconciliation and Review

- Supporting documents are not reconciled to the MyFD.
- Discrepancies are not investigated and resolved.
- Reconciliation is not done in a timely manner.
- Packing slips are not compared to purchase requisitions.
- RIP invoices are not reconciled to packing slips and purchase requisitions.
- No review of excessive long distance calls.
- No independent review of MyFD by supervisors of small units where most fiscal duties are assigned to one person.
- No independent review of MyFD by principal investigators or designees.

Safeguarding

- Blank lines on petty cash vouchers are not crossed out.
- Petty cash checks payable to cash.
- Unrestricted access to critical blank forms.

Cash Receipts/Accounts Receivable

Separation of Duties

- The cashier reconciles cash received with revenue records without proper supervisory review.
- The cashier maintains the accounts receivable records.
- The cashier authorizes adjustments/cancellations of accounts receivable.
- The cashier authorizes voids and adjustments to the cash register.
- The cashier accepts and resolves customer complaints.

Authorization

- Voids, paid-outs, and other adjustments to cash receipts are not approved.
- Receivable write-offs and other adjustments to billings are not approved.
- Voids, paid-outs, and adjustments are not properly supported.
- Non-numbered Rediform receipts are used.

Reconciliation and Review

- “Z” readings of cash register machines are not accounted for, or non-resettable cumulative totals are not used during the reconciliation process.
- The “Z” tape is not used to reconcile deposit amounts.
- Deposits are not reconciled to source documents, such as pre-numbered cash receipts.
- Departments do not use the cashier-validated cash transmittal or bank-validated deposit slips when reconciling deposits to MyFD.

Safeguarding

- Deposits are not done daily or when $500 accumulates.
- Safe combination is not changed when a staff member with knowledge leaves.
- Access to the safe is not restricted.

Equipment

Separation of Duties

- The custodian performs the physical inventory.

Documentation

- Equipment is not tagged upon receipt. Departments often wait for the asset control sheet before equipment is tagged.

Reconciliation and Reviews

- Biennial physical inventories are not done in a timely manner or are not done at all.
- Pre-tag items are not cleared on a timely basis.

Information Systems Security

Data and Records Management

- It is unknown how and where employees are storing sensitive and confidential data.

Access Controls

- The database does not have unique user logon identification and password authentication controls.
- The department does not document the authorization that is needed to establish accountability and issue, alter, or revoke user access.
- The department has a shared user logon ID and password that is used to gain access to the University administrative systems. The user logon ID and password were written on a piece of paper and the secure ID was left in a visible location.
- The database does not have user access permissions that are based on the principles of least privilege and separation of duties.

Physical Security

- The servers, which contain sensitive and confidential data, are located in office areas that are not restricted to authorized personnel, physically secured, or protected from tampering and environmental hazards.

Personnel Security Measures

- Former student and employee's access to the file server was not revoked or disabled.

Others

Separation of Duties

- The storeroom clerk performs physical counts and authorizes adjustments to inventory.

Authorization

- Service center rates are not approved by Management Accounting and Analysis annually.
- Recharge center rates are not approved by the Dean's Office annually.

Documentation

- Department policies and procedures are not documented.
- Recharge/cost center rates and charges are not properly supported.
- Costs are transferred from one sponsored project to another without appropriate supporting documentation.
- Records are not maintained in accordance with UW Records Retention Policy.

UW Administrative Policy Statement:
Policy on Financial Irregularities and Other Related Illegal Acts

(47.10,* November 6, 2008)

Approved by the Executive Vice President by authority of Executive Order No. 5

1. Introduction

This policy establishes the procedures and responsibilities for reporting and resolving known or suspected financial irregularities and other related illegal acts. The University of Washington is required under the Revised Code of Washington—RCW 43.09.185— to report any suspected financial irregularity or other related illegal act to the State Auditor's Office.

2. Definitions

a. Financial Irregularity

A loss of funds or assets of the University resulting from any dishonest, fraudulent, or other related illegal act. Such acts include, but are not limited to:

- Forgery or alteration of reports, documents, or computer files.
- Misappropriation or misuse of University assets (i.e., equipment, supplies, cash).
- Authorizing or receiving compensation for goods not received or services not performed.
- Authorizing or receiving compensation for hours not worked.
- Any irregularity in the handling or reporting of money transactions.
- Use of University facilities and equipment for private financial gain.
- Acceptance of kickbacks or bribes.
- Other related illegal acts (i.e., misuse of a U-PASS, email account, or the Internet).

b. Suspected Financial Irregularity or Other Related Illegal Act

A reasonable belief or actual knowledge that a dishonest or fraudulent act is occurring or has occurred.

* Formerly numbered *Operations Manual* D47.0

UW Administrative Policy Statement:
Policy on Financial Irregularities and Other Related Illegal Acts

3. Policy

Faculty and staff should immediately report suspected financial irregularities or other related illegal acts to their department management or to the Department of Internal Audit. Once department management becomes aware of a suspected financial irregularity or other related illegal act, they must immediately report it to Internal Audit. If the discovery occurs after normal business hours (when Internal Audit is not available), the report may be made to the University Police who have a 24-hour-a-day response capability. This is particularly important if there is concern over the recovery of assets or protection of vital records.

Department managers should protect the accounting records from loss or destruction, but should not attempt to conduct their own investigation. Department managers should consult with the appropriate University personnel official before taking any personnel action.

Upon learning of the suspected financial irregularity or other related illegal act, Internal Audit will immediately notify:

- The State Auditor's Office.
- The University of Washington Division of the Attorney General's Office.
- The University Police.
- The University's Risk Management Office.
- The appropriate University personnel official.

UW Administrative Policy Statement:
Policy on Financial Irregularities and Other Related Illegal Acts

4. Investigation Procedures

Internal Audit, the University Police, and the UW Division of the Attorney General's Office will conduct a preliminary investigation to determine:

- Whether a financial loss has occurred;
- Whether the responsible party(ies) can be identified; and
- The extent of the loss.

The results of the preliminary investigation will determine if and when it is necessary to notify other University officials or the Prosecuting Attorney.

At the conclusion of the investigation, Internal Audit issues a written report to the State Auditor's Office, the University's Executive Vice President, and other appropriate University officials.

5. Recovery of Loss

Department managers, on their own, are not authorized to enter into a settlement to recover the suspected loss. All settlements for recovery of the loss must be approved by the State Auditor's Office and the Attorney General.

If the investigation performed by Internal Audit reveals a loss occurred, the University will seek full recovery which may include audit costs. The University's Student Fiscal Services, Receivables Unit, will coordinate the recovery action (see Administrative Policy Statement 47.4, "Policy on Financial Irregularities and Other Related Illegal Acts") and has the authority to approve recovery settlements on behalf of the University.

UW Administrative Policy Statement:
Policy on Financial Irregularities and Other Related Illegal Acts

6. Responsibilities

a. Faculty and Staff

Report any instance of suspected financial irregularity or other related illegal act to your management head or to Internal Audit (or the University Police, after normal business hours if there is a concern over recovery of assets or protection of vital records).

b. Management Head

- Immediately contact the Department of Internal Audit (or the University Police after normal business hours if there is a concern over recovery of assets or protection of vital records).
- Protect the accounting records from loss or destruction.
- Do not attempt to conduct your own investigation.
- Consult with the appropriate University personnel official before taking any personnel action.
- Do not enter into a recovery settlement.

c. Internal Audit

- Notify the State Auditor's Office, the UW Division of the Attorney General's Office, the University Police, the University's Risk Management Office, and the appropriate University personnel official.
- Conduct a preliminary investigation.
- Notify other University officials as necessary.
- Issue a written report to the State Auditor's Office, the Senior Vice President for Finance and Facilities, and other appropriate University officials.

UW Administrative Policy Statement:
Policy on Financial Irregularities and Other Related Illegal Acts

7. Additional Information

Questions, reports or other communications regarding financial irregularities or other related illegal acts should be directed to the **Department of Internal Audit**.

Phone: 206–543–4028

Campus mail: Box 354984

Email: iaudit@uw.edu

If there is a concern over recovery of assets or protection of vital records after normal business hours, contact the **University Police**.

Phone: 206–543–9331 (voice) or 206–543–3323 (TTY)

Campus mail: Box 355200

Email: uwpolice@uw.edu