Governor's Office of Crime Prevention and Policy (GOCPP)

Grants Fraud (Risks and Prevention) – Module 3 (Internal Controls)

Thursday, September 18, 2025

OFFICE OF THE GOVERNOR
Wes Moore

Maryland
GOVERNOR'S OFFICE OF CRIME PREVENTION AND POLICY

https://gocpp.maryland.gov/

This presentation is intended for general education and/or informational purposes only and does not replace specific and independent professional advice nor constitutes legal guidance. Material contained herein developed based on information available as of July 1, 2025.

General Housekeeping

- Videos of previous training session as well as the slides from this session will be available at https://gocpp.Maryland.gov/grants/.
- In order to receive a Certificate of Completion, all participants must complete the pre-training assessment (https://s.zoom.us/m/b9D6kT7ZS) and the post-training assessment (https://s.zoom.us/m/b9Ea1znbc). You can also access the assessments using the QR codes below:

Pre-Training Assessment

Post-Training Assessment

Maryland
GOVERNOR'S OFFICE OF CRIME PREVENTION AND POLICY

Internal Controls

Module 3

Learning Objectives

- **Define** fraud risk assessment and its importance in grants management.
- **Learn** practical steps and methodologies for identifying potential fraud risks within your organization.
- **Understand** key risk factors that can increase an organization's susceptibility to fraud.
- **Identify** and explain essential internal control activities relevant to grants management.
- **Learn** best practices for designing, implementing, and maintaining effective internal controls.
- **Recognize** how internal controls directly mitigate the fraud risks identified in the previous module.

Introduction to Risk Assessment: A Foundation for Prevention

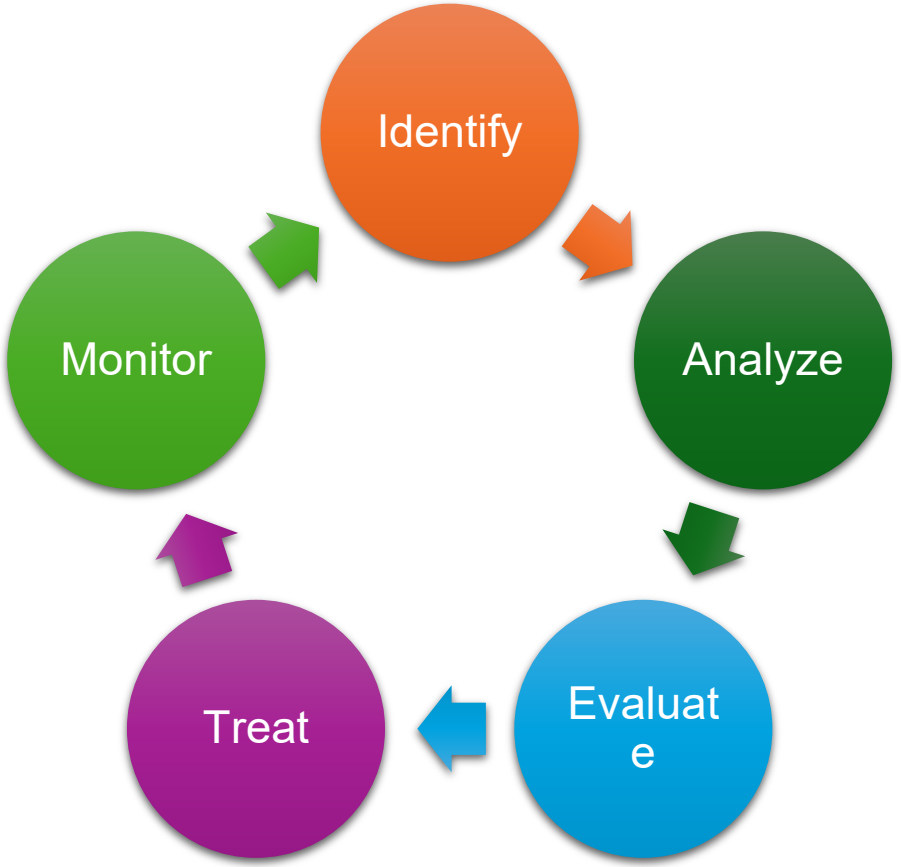
- You can't prevent what you don't know exists. Risk assessment is the proactive process of identifying, analyzing, and evaluating potential fraud threats. Risk assessment serves as your organization's first line of defense against fraud.

- **Why It's Crucial for Grants:**
  - Grants are often high-value and complex.
  - Specific regulations add layers of compliance risk.
  - Helps allocate resources effectively to mitigate the greatest threats.
  - Required by many grantors as a best practice.

- **Analogy:** Like checking the weather forecast before a trip – you prepare for potential storms.

What is Fraud Risk Assessment? A Systematic Approach

- Fraud risk assessment is a structured process to evaluate an organization's susceptibility to various fraud schemes.
- **Key Questions It Answers:**
  - Where are we vulnerable?
  - What types of fraud could occur?
  - Who might perpetrate it?
  - What is the potential impact if it occurs?
  - How likely is it to happen?
- **Goal:** To understand vulnerabilities and prioritize mitigation efforts.



Steps in Fraud Risk Assessment: The Process Overview

- The assessment journey involves several key steps, from identifying potential scenarios to ongoing monitoring.

- **Simplified Steps:**
  - **Identify Potential Fraud Scenarios:** Brainstorm what could go wrong.
  - **Analyze Likelihood and Impact:** How probable is it, and how bad would it be?
  - **Evaluate Existing Controls:** What measures are already in place?
  - **Develop Mitigation Strategies:** How can we reduce risk?
  - **Monitor and Review:** Is it working? Are new risks emerging?

- **Iterative Process:** Not a one-time event; it should be ongoing.

Brainstorming Potential Fraud Scenarios: Thinking Like a Fraudster

- A critical step in risk assessment is to brainstorm "what could go wrong" by thinking from a fraudster's perspective.
- **Methodology:** Gather a diverse group (finance, program, audit, legal). Ask:
  - "If I wanted to defraud this grant, how would I do it?"
  - "Where are the weak points in our processes?"
  - "What data could be manipulated?"
  - "What assets are most vulnerable?"
- **Focus on Grant Lifecycle:** Consider risks at application, award, expenditure, reporting, closeout.
- **Example:** “How could someone get paid for work not performed on Project X?”



Data Analysis for Risk Identification: Clues in the Numbers

- Leveraging existing financial and operational data can reveal hidden anomalies and patterns that suggest fraud risk.
- **What to Look For:**
  - Large, unexplained variances from budget.
  - Unusual spending spikes in certain categories.
  - Numerous small, round-dollar payments.
  - High volume of transactions with a single vendor.
  - Missing transaction sequences.
  - Repeated payments of identical amounts to different entities.
- **Tools:** Spreadsheets, basic analytical software.



Reviewing Past Incidents: Learning from History

- Examining past fraud attempts, near-misses, or errors provides valuable insights into an organization's vulnerabilities.
- **Process:**
  - Analyze internal audit reports.
  - Review past fraud investigations (even if unsubstantiated).
  - Examine whistleblower complaints.
  - Look at prior grantor audit findings.
- **Focus:** Not just *what* happened, but *how* it happened and *why* it wasn't detected earlier.



Interviewing Key Personnel: Insights from the Front Lines

- Engaging with employees directly involved in daily operations often uncovers invaluable insights into process weaknesses.
- **Who to Interview:**
  - Finance/Accounting staff
  - Program Managers
  - Procurement staff
  - Grant Administrators
  - Internal Audit (if applicable)
- **Approach:** Nonthreatening, open-ended questions focused on processes and control effectiveness, not accusations.
- **Visual:** Two people talking in a collaborative setting, or an ear listening to a speech bubble.



Conducting Fraud Risk Workshops: Collaborative Brainstorming

- Facilitated workshops bring diverse teams together to collaboratively identify and discuss potential fraud risks.
- **Benefits:**
  - Draws on diverse perspectives.
  - Increases ownership of the risk assessment process.
  - Fosters a culture of awareness.
  - Can use interactive exercises (e.g., scenario planning).
- **Key Output:** A comprehensive list of potential fraud scenarios specific to the organization and its grants.



Mapping Business Processes: Finding the Gaps

- Visualizing key grant-related processes through flowcharts helps identify control gaps and single points of failure.

- **What to Look For:**
  - **Control Gaps:** Points where no control exists.
  - **Single Points of Failure:** Where one person has too much authority.
  - **Complex or Manual Steps:** More prone to error and manipulation.
  - **Lack of Documentation:** Unclear procedures.



Considering External Factors: Beyond Internal Walls

- Fraud risk assessment must also consider broader external factors that can influence an organization's vulnerability.

- **Factors to Consider:**
  - **Economic Downturns:** Can increase pressure on individuals (financial hardship) or organizations (revenue shortfalls).
  - **Industry Trends:** New technologies, emerging fraud schemes in the sector.
  - **Regulatory Changes:** New compliance requirements that create new vulnerabilities.
  - **Vendor/Partner Risks:** Financial instability of key partners, ethical reputation.
  - **Natural Disasters/Crises:** Can create chaos and reduce oversight, increasing opportunity for fraud.

Grant Lifecycle Approach to Risk: Stage by Stage

- Fraud risks evolve throughout the grant lifecycle, requiring tailored attention at each stage from application to closeout.

- **Fraud Risks Evolve Throughout the Grant Lifecycle:**
  - **Application Phase:** Misrepresentation of capabilities, false certifications.
  - **Award Phase:** Undisclosed conflicts of interest, bribery for selection.
  - **Expenditure Phase:** False billing, ghost employees, diversion of funds, unallowable costs.
  - **Reporting Phase:** Falsified performance data, manipulated financial reports.
  - **Closeout Phase:** Failure to return unused funds, improper asset disposition.

- **Benefit:** Allows for targeted controls at each vulnerable stage.

Specific Grant Risk Areas: Where to Dig Deeper

- Certain areas within grants management are consistently identified as having higher fraud risk, requiring deeper scrutiny.

- **Common High-Risk Areas in Grants:**
  - **Procurement:** Vendor selection, bidding, invoice processing.
  - **Personnel Costs:** Timesheets, payroll, fringe benefits.
  - **Travel Expenses:** Reimbursements, per diems.
  - **Subawards/Subrecipients:** Monitoring, reporting, payment processing.
  - **Equipment & Inventory:** Tracking, disposition.
  - **In-Kind Contributions:** Valuation, documentation.
  - **Cash Receipts/Revenue Recognition:** If the grant involves revenue generation.

Documenting Risks: The Risk Register

- A systematic risk register is essential for recording identified risks, their characteristics, and planned responses.

- **Key Information in a Risk Register:**
  - Risk Description (e.g., "Ghost employees on payroll").
  - Fraud Scheme (e.g., "Asset Misappropriation").
  - Likelihood (e.g., High, Medium, Low).
  - Impact (e.g., Financial, Reputational, Operational).
  - Existing Controls.
  - Risk Owner.
  - Mitigation Actions (if needed).

- **Tool:** Spreadsheet or dedicated risk management software.

Assigning Ownership of Risks: Who is Responsible?

- Assigning clear ownership for each identified risk ensures accountability and promotes proactive management.
- **Who are Owners?** Often department heads, project managers, or specific functional leads.
- **Benefits:**
  - Ensures accountability.
  - Promotes proactive risk management.
  - Integrates risk management into daily operations.



Case Study Example of Risk Identification: Scenario

- Let's apply our knowledge by identifying potential fraud risks in a case study
- **Scenario:** "TechBridge Labs received a grant to equip a new community coding center. The grant requires purchasing specialized computers and software. The purchasing process involves a single Purchasing Manager who sources quotes, approves vendors, and authorizes payments up to $10,000. There's high pressure to spend the funds quickly to meet grant timelines. Additionally, recent staff turnover in the IT department means new personnel are handling equipment setup and inventory."
- **Question:** Based on this scenario, what potential fraud risks can you identify?

Introduction to Fraud Risk Factors: The Fraud Triangle Revisited

- **Definition:** The Fraud Triangle consists of conditions or circumstances that increase an organization's vulnerability or an individual's propensity to commit fraud.

- **The Fraud Triangle (Donald Cressey):**
  - **Pressure:** A perceived non-shareable financial need or motivation.
  - **Opportunity:** The ability to commit and conceal the fraud.
  - **Rationalization:** Justifying the fraudulent act.

- **Focus:** While we can't control "pressure" or "rationalization" directly, we *can* control "opportunity" through strong controls.

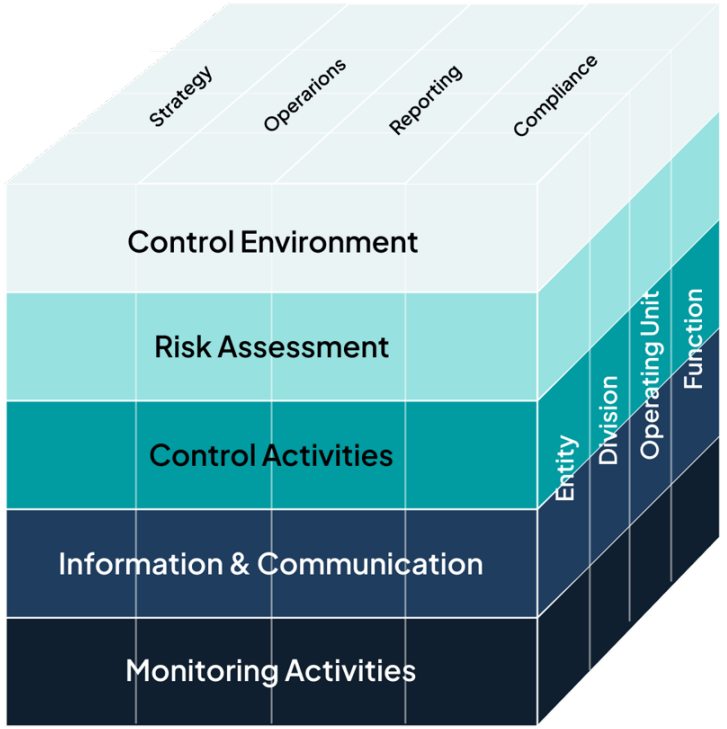
Introduction to Internal Controls: The Backbone of Fraud Prevention

- Internal controls are the essential framework that an organization uses to prevent, detect, and correct errors and fraud.
- **Why They're Crucial for Grants:**
  - Protect against misuse and fraud of grant funds.
  - Ensure compliance with complex grantor requirements.
  - Maintain accurate financial reporting for accountability.
  - Enhance efficiency and effectiveness of grant programs.
  - Build and maintain trust with grantors and the public.
- **Analogy:** Like the safety features in a car – seatbelts, airbags, antilock brakes – designed to prevent accidents or minimize damage.



What are Internal Controls? (COSO Framework)

- Internal controls are defined as the policies and procedures designed to ensure the integrity of financial and accounting information.
- The COSO Framework is a widely recognized and adopted model for designing, implementing, and assessing internal controls within an organization. Developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), its primary purpose is to help organizations achieve their objectives related to operations, reporting, and compliance.
- **Key Components (COSO):**
  - **Control Environment:** Tone at the top, ethical values.
  - **Risk Assessment:** Identifying and analyzing risks.
  - **Control Activities:** The actual policies and procedures.
  - **Information & Communication:** Flow of information.
  - **Monitoring Activities:** Ongoing evaluations.
- **Focus for This Module:** Primarily on "Control Activities."



COSO cube

Objectives of Internal Controls: The Four Pillars

- The primary goals of internal controls are to safeguard assets and ensure the reliability of financial reporting.

- **Primary Objectives:**
  - **Safeguard Assets:** Protecting financial resources, equipment, and other organizational property from theft or misuse.
  - **Ensure Accurate Financial Reporting:** Producing reliable and timely financial information.
  - **Promote Operational Efficiency:** Ensuring processes are effective and resources are used wisely.
  - **Encourage Compliance:** Adherence to laws, regulations, and grant agreement terms.

- **Direct Link to Fraud Prevention:** Controls reduce the "opportunity" element of the fraud triangle.

The Preventative vs. Reactive Distinction

- Internal controls can be either preventative, stopping an error from happening, or detective, identifying an error after it has occurred.
- **Preventative Controls:**
  - **Purpose:** Stop errors or fraud *before* they occur.
  - **Examples:** Segregation of duties, authorization limits, prenumbered documents.
  - **Analogy:** A lock on a door – prevents unauthorized entry.
- **Reactive Controls:**
  - **Purpose:** Identify errors or fraud *after* they have occurred.
  - **Examples:** Reconciliations, internal audits, surprise cash counts.
  - **Analogy:** An alarm system – alerts you to an intrusion.
- **Best Practice:** A robust control system includes a mix of both.



How Internal Controls Deter Fraud: Closing the Opportunity

- By establishing clear policies and oversight, internal controls directly reduce the opportunity for fraud.
- **Direct Impact:** Internal controls primarily target the "Opportunity" leg of the Fraud Triangle.
- **How They Deter:**
  - **Increased Difficulty:** Make it harder to commit fraud without being detected.
  - **Increased Risk of Detection:** Make it more likely that fraud will be caught.
  - **Reduced Temptation:** Knowing controls exist can deter potential fraudsters.
  - **Clarity of Expectations:** Employees understand acceptable conduct.
- **Result:** Even if pressure or rationalization exists, the lack of opportunity can prevent fraud.

Importance in Grants Management: Compliance and Confidence

- Strong internal controls are not only a best practice but are also often a mandatory requirement for compliance in grants management.
- **Specific Reasons for Grants:**
  - **Grantor Requirements:** Many grants (especially federal) mandate strong internal controls (e.g., Uniform Guidance).
  - **Accountability:** Demonstrates proper stewardship of public/private funds.
  - **Audit Readiness:** Preparedness for external audits and reviews.
  - **Funding Continuity:** Poor controls and fraud can lead to loss of current and future funding.
  - **Reputation:** Protects the organization's standing and ability to secure future grants.



Cost-Benefit of Internal Controls: An Investment, Not an Expense

- Implementing internal controls should be viewed as an investment in your organization's future, not just an expense.
- **The Cost of No Controls:**
  - Financial losses due to fraud.
  - Legal fees and investigations.
  - Reputational damage.
  - Loss of current/future grants.
  - Employee morale issues.
- **The Benefit of Strong Controls:**
  - Reduced fraud losses.
  - Improved efficiency and accuracy.
  - Enhanced compliance.
  - Stronger reputation.
  - Increased stakeholder confidence.
- **Key:** Controls should be commensurate with the level of risk.

Management's Role in Internal Controls: Setting the Tone

- An ethical "tone at the top" is essential for establishing and reinforcing a culture of strong internal controls.
- **Responsibilities:**
  - **Establish a strong control environment:** Emphasize integrity and ethical values.
  - **Implement and enforce policies:** Ensure controls are documented and followed.
  - **Provide resources:** Ensure adequate staff, training, and systems.
  - **Model ethical behavior:** Lead by example.
  - **Oversee and monitor:** Regularly review control effectiveness.
  - **Promote accountability:** Hold individuals responsible for control failures.
- **Impact:** Without management buy-in, controls are often ineffective.



Employee Responsibility in Internal Controls: Everyone Plays a Part

- Every employee has a role to play in the internal control system, from following procedures to reporting concerns.
- **Responsibilities:**
  - **Adhere to Policies and Procedures:** Follow established controls.
  - **Report Concerns:** Utilize hotlines or other reporting mechanisms.
  - **Be Vigilant:** Watch for red flags in their daily work.
  - **Seek Clarification:** Ask questions if processes are unclear.
  - **Participate in Training:** Understand their role in the control system.
- **Key:** Controls are only as effective as the people who execute and observe them.



Segregation of Duties: The Cornerstone Control

- A cornerstone of internal controls is ensuring that no single person has control over all parts of a transaction.

- **Key Incompatible Functions (ARCC):**
  - **Authorization:** Approving a transaction.
  - **Recording:** Entering the transaction into the accounting system.
  - **Custody:** Handling or having access to assets (cash, inventory).
  - **Reconciliation:** Comparing records to ensure accuracy.

- **Example:** The person who approves an invoice should not be the same person who processes the payment.



Authorization Procedures: Formal Approvals

- Formal authorization procedures ensure that all transactions and decisions are properly approved and documented.

- **Key Elements:**
  - **Approval Limits:** Monetary thresholds for different levels of management.
  - **Specific Approvers:** Clearly designated individuals responsible for certain approvals.
  - **Documented Approvals:** Signatures, electronic approvals, or other auditable evidence.
  - **Purpose-Driven Approval:** Approvals should confirm the legitimacy and allowability of the expense/activity.

- **Examples in Grants:** Approval of purchase orders, travel requests, expense reimbursements, budget modifications, subaward agreements.

- **Visual:** A document with multiple signature lines, or a stamp indicating "Approved."

Reconciliation & Review: The Verification Step

- Regularly comparing financial records and conducting independent reviews is a crucial detective control.
- **Importance:** A key detective control to spot errors, omissions, or deliberate manipulation.
- **Examples in Grants:**
  - Bank account reconciliations (statement vs. ledger).
  - Grant expenditure reports vs. general ledger.
  - Payroll records vs. timesheets.
  - Inventory counts vs. inventory records.
  - Subrecipient financial reports vs. their underlying documentation.
- **Key:** Should be done regularly and, ideally, by someone independent of the original transaction.



Physical Safeguards: Protecting Tangible Assets

- Physical safeguards are put in place to protect tangible assets, such as cash, equipment, and sensitive documents.

- **Examples in Grants:**
  - Securing cash in a locked safe.
  - Controlling access to equipment, inventory, and sensitive documents.
  - Restricting access to server rooms or data centers.
  - Maintaining a robust inventory system for grant-purchased equipment.
  - Using security cameras or alarms.

- **Impact:** Directly reduces the opportunity for asset misappropriation.



Performance Reviews: Monitoring Against Expectations

- Regularly monitoring performance against approved plans and budgets can help detect unusual activities.
- **Importance:** Helps identify unusual trends, significant variances, or underperformance that could be a red flag for fraud.
- **Examples in Grants:**
  - Analyzing budget vs. actual expenditures monthly/quarterly.
  - Reviewing program activity reports against planned milestones.
  - Comparing staff time charged to projects vs. expected effort.
  - Benchmarking costs against industry averages.
- **Key:** Requires thorough investigation of significant deviations.

Information Technology Controls: Securing Digital Assets

- IT controls are vital for protecting digital data and systems from unauthorized access and manipulation.
- **Examples in Grants:**
  - **Access Controls:** Strong passwords, multifactor authentication, role-based access to financial/grant systems.
  - **Data Backups:** Regular backups and offsite storage.
  - **Change Management:** Controlled changes to systems and data.
  - **Network Security:** Firewalls, intrusion detection.
  - **Automated Matching:** System checks (e.g., matching PO to invoice).
  - **Audit Trails:** System logs of user activity.
- **Impact:** Prevents unauthorized data manipulation, protecting against financial reporting fraud and data theft.



Policies and Procedures: Clear Guidelines

- Clearly written policies and procedures provide employees with the necessary guidance to perform their duties correctly and ethically.
- **Importance:**
  - Communicate expectations clearly.
  - Ensure consistency in operations.
  - Provide a basis for training.
  - Serve as a reference for employees.
  - Provide a standard against which compliance can be measured.
- **Key for Grants:** Specific policies for procurement, travel, subrecipient monitoring, cost allowability, timekeeping, etc.
- **Impact:** Reduces ambiguity, making it harder to claim ignorance of rules.
- **Visual:** A stack of policy binders or a digital document library.



Budgetary Controls: Adhering to Financial Plans

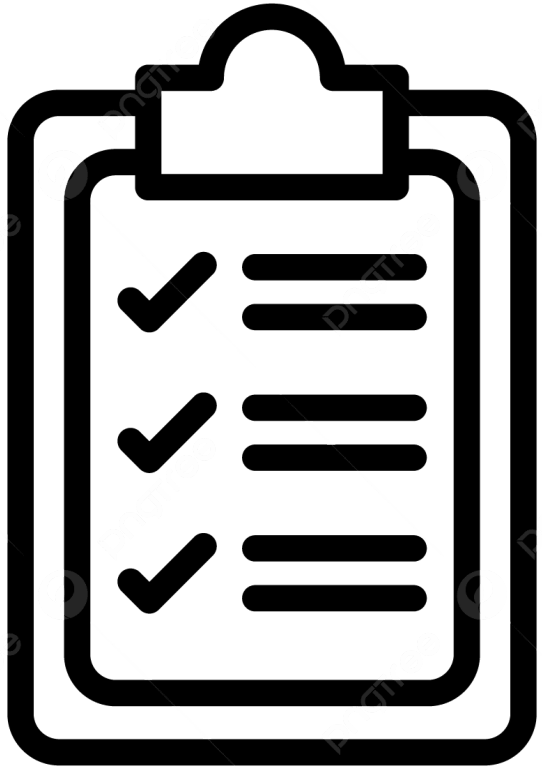
- Budgetary controls involve closely monitoring expenses to ensure they do not exceed the approved amounts.

- **Importance:**
  - Ensures funds are used for their intended purpose.
  - Highlights potential overspending or unusual expenses.
  - Facilitates financial planning and forecasting.
  - Critical for grant compliance (spending within approved grant budgets).

- **Key:** Requires regular review and explanation for significant deviations.

Vendor Management Controls: Vetting Your Partners

- Proper controls in vendor management ensure that you are working with legitimate, qualified partners.
- **Examples:**
  - **Vendor Vetting:** Background checks, verifying business registration.
  - **Approved Vendor List:** Limiting purchases to pre-approved suppliers.
  - **Competitive Bidding:** Requiring multiple quotes for significant purchases.
  - **Independent Verification:** Cross-checking vendor addresses/EINs.
  - **Regular Review:** Periodically reviewing vendor performance and pricing.
- **Impact:** Reduces risk of ghost vendors, false billing, and kickbacks.



Payroll Controls: Ensuring Legitimate Payments

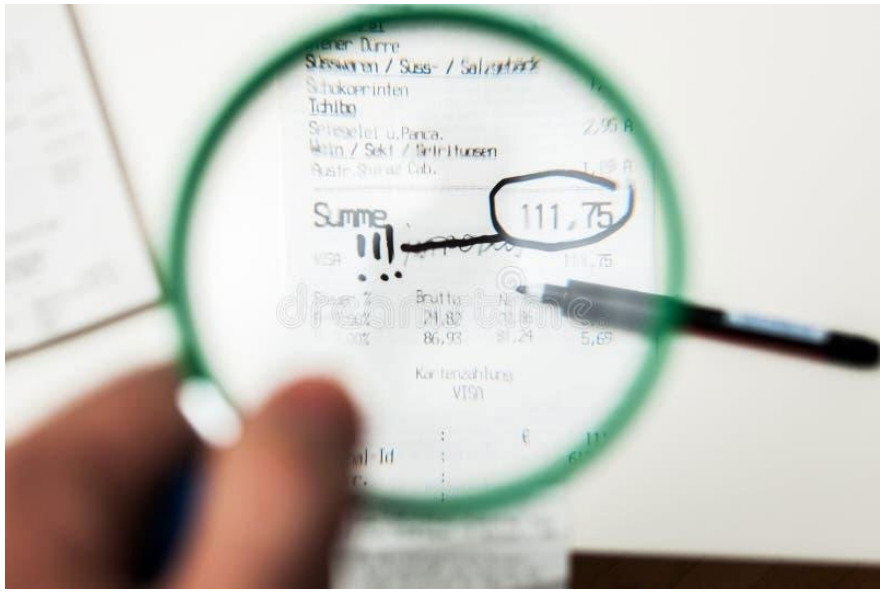
- Controls are necessary in the payroll process to ensure that all payments are legitimate and accurately calculated.

- **Examples:**
  - **Segregation of Duties:** Separate HR (hiring), timekeeping, payroll processing, and bank reconciliation functions.
  - **Approval of Timesheets:** Manager approval of hours worked.
  - **Verification of New Hires:** Independent verification of employee identity and banking details.
  - **Periodic Payroll Reconciliations:** Comparing payroll register to bank statements and HR records.
  - **Review of Payroll Changes:** Independent review of changes to pay rates or deductions.

- **Impact:** Prevents ghost employees and fraudulent payroll schemes.

Travel Expense Controls: Managing Reimbursements

- Clear policies and a robust review process for travel expenses help prevent fraud in this area.
- **Examples:**
  - **Pre-Approval of Travel:** Requiring authorization before travel.
  - **Detailed Expense Reports:** Requiring itemized receipts for all expenditures.
  - **Per Diem Policies:** Clear rates for meals and lodging.
  - **Prohibition of Personal Expenses:** Clearly stating what is unallowable.
  - **Manager Review:** Independent review and approval of expense reports.
  - **Receipt Verification:** Matching expenses to supporting documentation.
- **Impact:** Reduces travel fraud and ensures compliance with grant travel policies.



Subaward Monitoring Controls: Oversight Down the Chain

- When working with subrecipients, it is essential to have controls in place to monitor their performance and financial activities.

- **Examples:**
  - **Subrecipient Risk Assessment:** Evaluating their financial capacity and control environment.
  - **Detailed Subaward Agreements:** Clearly outlining responsibilities and reporting requirements.
  - **Regular Financial Reporting from Subrecipients:** And thorough review by the prime.
  - **Site Visits/Audits of Subrecipients:** Periodic checks on their operations and records.
  - **Performance Monitoring:** Verifying programmatic progress.
  - **Timely Payment Processing:** To avoid creating pressure for the subrecipient.

- **Impact:** Mitigates the risk of subrecipient fraud that can directly impact the prime grantee.

Grant Closeout Procedures: The Final Accountability

- A formal closeout process ensures that all grant funds are properly accounted for and all requirements have been met.

- **Examples:**
  - **Final Financial Reconciliation:** All expenditures reconciled, unspent funds returned.
  - **Final Performance Reporting:** All objectives accounted for.
  - **Equipment Disposition:** Proper accounting for and transfer/disposal of grant-purchased assets.
  - **Document Retention:** Ensuring all records are properly archived.
  - **Audit Resolution:** Addressing any outstanding audit findings.

- **Impact:** Prevents fraud related to leftover funds, asset misuse, or false final reporting.

Interactive Exercise: "Control vs. No Control" Scenario

- Let's apply your knowledge to identify whether a given scenario demonstrates strong or weak internal controls.

- **Instructions:** We will present a short scenario. You decide if it demonstrates a strong internal control, a weak internal control, or no control at all, and why.
  - **Scenario 1:** "All invoices over $500 require approval from the Department Head and the Finance Director before payment."
  - **Scenario 2:** "The same person who collects cash donations also deposits them and reconciles the bank statement."
  - **Scenario 3:** "There are locked cabinets for grant-funded equipment, but the key is left on top of the cabinet.“

Best Practices: Regular Assessment and Updates

- Internal controls are not a one-time setup; they must be regularly assessed and updated to remain effective.
- **Key:** Internal controls are not a one-time setup. They must evolve.
- **Why Update?**
  - New grant programs or activities introduce new risks.
  - Changes in regulations require new compliance measures.
  - Technology changes can create new vulnerabilities or opportunities for automation.
  - Identified fraud incidents expose control weaknesses.
  - Organizational growth or restructuring.
- **Methodology:** Periodically review the risk assessment and adjust controls accordingly.

Best Practices: Training and Communication

- Ongoing training and communication ensure that all employees understand their role in the control environment.
- **Importance:** Controls are only effective if understood and implemented correctly.
- **Key Elements:**
  - **Mandatory Training:** For all employees, especially those in finance, procurement, and management.
  - **Clear Policies:** Easily accessible and understandable.
  - **Regular Communication:** Reminders about control procedures and ethical expectations.
  - **Onboarding:** Integrate control training into new employee orientation.
  - **Specific Training:** Tailored for roles with high fraud risk.
- **Impact:** Increases awareness, reduces errors, and strengthens the control environment.

Best Practices: Independent Reviews/Audits

- Periodic reviews by internal or external auditors provide an independent and objective evaluation of your control system.

- **Types of Reviews:**
  - **Internal Audits:** Conducted by an independent internal function.
  - **External Audits:** By independent accounting firms (e.g., A-133/Single Audit for federal grants).
  - **Grantor Monitoring Visits:** Direct oversight by the funding agency.
  - **Surprise Audits:** Unannounced checks on high-risk areas.

- **Focus:** Not just on compliance, but on *effectiveness* of controls in preventing/detecting fraud.

Best Practices: Whistleblower Protection

- Protecting employees who report fraud or misconduct is a crucial part of a healthy control environment.
- **Importance:** Employees are often the first to detect fraud. A safe reporting environment is crucial.
- **Elements:**
  - **Clear Reporting Channels:** Hotlines, direct to HR/Legal/Board.
  - **Anonymity Options:** Where legally permissible.
  - **Nonretaliation Policy:** Explicitly stating protection for good-faith reporters.
  - **Communication:** Employees must know about the policy.
  - **Prompt Investigation:** All reports must be taken seriously and investigated.
- **Impact:** Encourages internal reporting, leading to earlier detection.

Best Practices: Continuous Improvement

- A mindset of continuous improvement ensures that your internal control system remains strong and adaptable.
- **Key:** Internal controls are not a static state but an ongoing process of refinement and adaptation.
- **Involves:**
  - Regular self-assessments.
  - Learning from new fraud cases (internal and external).
  - Staying updated on best practices and regulatory changes.
  - Embedding risk and control thinking into daily operations.
- **Impact:** Ensures the control system remains robust and relevant over time.

Best Practices: Grant-Specific Control Considerations

- Controls should be tailored to the specific requirements and unique risks of each individual grant.
- **Adaptation is key:** While general controls apply, grants often have unique requirements.
- **Considerations:**
  - **Allowability of Costs:** Specific controls to ensure expenses meet grant guidelines.
  - **Cost-Share/Matching Funds:** Controls to track and verify in-kind or cash match.
  - **Performance Reporting:** Controls to ensure accuracy of programmatic data.
  - **Subrecipient Management:** Dedicated controls for monitoring subawards.
  - **Grant Period Compliance:** Controls to ensure expenses fall within the grant period.
  - **Prior Approvals:** Specific controls for grant-required prior approvals.

Case Study: Implementing Effective Internal Controls - Scenario

- Let's examine a case study to see how the implementation of strong internal controls can successfully prevent fraud.
- **Scenario:** "YouthWorks, a nonprofit receiving several federal grants, recently experienced a small, nonfraudulent error where expenses were incorrectly charged to the wrong grant. While not fraud, this highlighted a weakness in their financial coding and review process. The Board decided to use this incident to proactively strengthen their controls against future errors and potential fraud. They engaged a consultant to help."
- **Challenge:** How could YouthWorks implement effective internal controls to prevent similar errors and deter fraud?

Module Summary & Key Takeaways

- To summarize, a well-designed and consistently applied system of internal controls is your most effective tool for preventing grants fraud.

- **Recap:**
  - Internal controls are crucial for safeguarding assets, ensuring accurate reporting, and promoting compliance.
  - They are designed to prevent (and detect) fraud by closing "opportunity" gaps.
  - Key controls include segregation of duties, authorization, reconciliation, and documentation.
  - Effective implementation requires clear policies, training, independent reviews, and strong leadership.
  - Controls must be continuously assessed and updated to remain effective.

- **Action Item:** Review your own organization's internal controls. Are they clearly defined? Are they consistently followed? Where might there be gaps?