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

## Grants Fraud (Risks and Prevention) – Module 4 (Fraud Prevention Measures)

**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

# Fraud Prevention Measures

## Module 4

# Learning Objectives

- **Explain** the importance of a comprehensive approach to fraud prevention, extending beyond internal controls.
- **Highlight** the critical role of employee training and ethical awareness in deterring fraud.
- **Describe** how effective hotlines and anonymous reporting mechanisms contribute to early detection.
- **Emphasize** the necessity of regular reviews and continuous monitoring to maintain vigilance.
- **Outline** strategies for fostering an anti-fraud culture within your organization.

# Introduction to Proactive Prevention: Beyond Just Controls

- While internal controls are essential, a truly effective fraud prevention strategy extends to proactive measures that foster an ethical culture.

- **Why It's Critical:**
  - No control system is foolproof; human elements are always present.
  - Prevention aims to deter fraud from occurring in the first place, saving significant resources and reputational damage.
  - Fosters an ethical environment where fraud is less likely to thrive.
  - Empowers employees to be part of the solution.

- **Analogy:** Internal controls are like the security system on your house; prevention measures are like Neighborhood Watch, good lighting, and strong community ties.

# Employee Training: Your First Line of Defense

- Your employees are your organization’s first line of defense against fraud, and training is what empowers them.

- **Why Invest in Training?**
  - Increases awareness of fraud risks and types.
  - Educates on internal control procedures and their importance.
  - Clarifies reporting mechanisms and responsibilities.
  - Reinforces ethical behavior and organizational values.
  - Reduces rationalization by highlighting consequences.

- **Impact:** Turns every employee into a potential fraud detector.



# What to Cover in Training: Comprehensive Education

- Effective fraud training should cover a broad range of topics, from defining fraud to identifying its warning signs.
- **Key Topics for Fraud Prevention Training:**
  - **Definition of Fraud:** What it is and isn't (Module 1 recap).
  - **Common Fraud Schemes in Grants:** Real-world examples (Module 2 recap).
  - **Fraud Red Flags:** How to identify suspicious indicators.
  - **Internal Controls:** Explain key controls and why they are in place (Module 4 recap).
  - **Organizational Policies:** Code of conduct, ethics policy, conflict of interest.
  - **Reporting Mechanisms:** How to report suspicions (next section).
  - **Consequences of Fraud:** For individuals and the organization.
  - **Whistleblower Protection:** Assurance of safety for good-faith reporting.
- **Tailor Content:** Adapt to different roles and levels within the organization.



# Who Needs Training? Broadening the Net

- Although every employee should receive basic training, some roles require more specific and detailed instruction.

- **Target Audience:**
  - **All Employees:** Basic fraud awareness for everyone.
  - **Management & Leadership:** Setting the "tone at the top," oversight responsibilities.
  - **Finance & Accounting Staff:** Deep dive into financial controls, transaction monitoring.
  - **Procurement Staff:** Vendor vetting, competitive bidding, contract management.
  - **Program Managers/Staff:** Monitoring grant expenditures, performance reporting, subrecipient oversight.
  - **Human Resources:** Payroll, hiring, employee relations.
  - **Board Members:** Oversight, fiduciary duties, risk management.

- **Key:** Training should be tailored to the specific fraud risks and control responsibilities of each group.

# Training Methods: Engaging Your Workforce

- To maximize engagement and retention, you can use a variety of training methods, including both in-person and digital formats.

- **Options for Delivery:**
  - **In-Person Workshops:** Interactive, allows for Q&A and discussion.
  - **Online Modules/E-Learning:** Accessible, self-paced, trackable completion.
  - **Webinars:** Good for remote teams, can include live Q&A.
  - **Case Study Discussions:** Applying knowledge to real-world scenarios.
  - **Guest Speakers:** Law enforcement, forensic accountants, ethics experts.
  - **Regular Refresher Courses:** Keep knowledge current and reinforce concepts.
  - **Quizzes/Knowledge Checks:** To assess understanding.

- **Best Practice:** A blended approach often yields the best results.

# Importance of Ongoing Training: Continuous Reinforcement

- Fraud prevention training is not a one-time event; it requires continuous reinforcement to be effective.

- **Why Repetition Matters:**
  - **Refreshes Knowledge:** People forget over time.
  - **Adapts to New Risks:** Fraud schemes evolve, regulations change.
  - **Reinforces Culture:** Consistent messaging on ethics and vigilance.
  - **Addresses Turnover:** Ensures new employees are brought up to speed.
  - **Maintains Vigilance:** Keeps fraud prevention top of mind.

- **Frequency:** Annual refreshers are a good baseline, with more frequent updates as needed.



# Building a Culture of Awareness: Making It Part of the DNA

- The goal of training is to build a culture of integrity where fraud prevention is a shared responsibility.
- **Beyond Formal Training:** Fraud prevention should be an integral part of the organizational culture.
- **How to Foster It:**
  - **Regular Communication:** Newsletters, intranet articles, posters, emails about fraud topics.
  - **Leadership Messaging:** Management regularly speaks about integrity and controls.
  - **Celebrate Ethical Behavior:** Acknowledge and reward ethical actions.
  - **Integrate into Performance Reviews:** Include adherence to ethical guidelines and controls.
  - **Open-Door Policy:** Encourage employees to ask questions and raise concerns without fear.
- **Impact:** Creates an environment where fraud is less likely to be tolerated or hidden.

# Role of Management in Training: Leading by Example

- Management's active participation in and support of training is crucial for its success.
- **Key Responsibilities:**
  - **Actively Participate:** Attend training sessions alongside their teams.
  - **Champion the Cause:** Publicly advocate for fraud prevention.
  - **Allocate Resources:** Ensure sufficient budget and time for training.
  - **Enforce Policies:** Consistent application of control and ethics policies.
  - **Address Concerns:** Take employee concerns about fraud seriously.
- **Impact:** Employees are more likely to take training seriously when they see management committed to it.
- **Visual:** A leader at the head of a classroom, or a manager empowering their team.

# Training on Ethical Conduct: Beyond Just Rules

- Effective training goes beyond simply listing rules and instead focuses on ethical decision-making and a shared sense of integrity.
- **Importance:** Fraud prevention isn't just about rules, it's about fostering a strong ethical foundation.
- **Topics:**
  - Organizational values and mission.
  - Personal integrity and professional responsibility.
  - Consequences of unethical behavior (personal and organizational).
  - Ethical decision-making frameworks.
  - Reporting ethical dilemmas.
- **Goal:** To strengthen the "rationalization" leg of the fraud triangle by making it harder for individuals to justify dishonest acts.



# Specific Training for Grant-Related Roles: Tailored Knowledge

- Employees in key grant-related roles require specialized training tailored to their specific risks and responsibilities.
- **Customization is Key:** Certain roles have unique vulnerabilities in grants management.
- **Examples:**
  - **Procurement:** Training on federal procurement rules (e.g., Uniform Guidance), bid analysis, vendor due diligence.
  - **Project Managers:** Cost allowability, proper documentation of project activities, subrecipient monitoring.
  - **Research Staff:** Data integrity, avoiding research misconduct, proper charging of time and effort.
  - **HR/Payroll:** Grant-funded positions, timekeeping policies, benefits allocation.
- **Benefit:** Ensures that those closest to the specific risks have the targeted knowledge to prevent and detect fraud.

# Addressing Resistance to Training: Emphasize Value

- To overcome resistance, it is important to clearly communicate the personal and professional benefits of fraud prevention training.
- **Common Resistance:** "Too busy," "I already know this," "It's not my job.“
- **How to Address:**
  - **Explain the "Why":** Connect training directly to protecting the organization's mission and future funding.
  - **Highlight Benefits:** Show how it protects individual jobs and reputation.
  - **Make it Engaging:** Use interactive methods, real-world stories.
  - **Leadership Mandate:** Demonstrate management's commitment.
  - **Convenience:** Offer flexible scheduling, online options.
- **Key:** Position training as an essential tool for success, not just a compliance checkbox.



# Measuring Training Effectiveness: Beyond Completion Rates

- To ensure your training is having the desired impact, you must measure its effectiveness through various methods.

- **Metrics Beyond "Did they attend?":**
  - **Knowledge Checks/Quizzes:** Assess understanding of key concepts.
  - **Post-Training Surveys:** Gauge participant satisfaction and perceived value.
  - **Observation:** Do employees apply learned behaviors?
  - **Reduction in Errors:** Decreased noncompliance findings in audits.
  - **Increase in Hotline Tips:** More reports of suspected fraud (indicating increased awareness and trust).
  - **Feedback from Auditors/Grantors:** Positive comments on control environment.

- **Purpose:** To continuously improve training programs and ensure they meet organizational needs.

# The Power of Whistleblowers: Often the First to Know

- Internal tips from employees are often the most effective way to detect fraud, and they should be encouraged.
- **Fact:** A significant percentage of fraud (often 40-50%+) is detected through tips, most often from employees.
- **Why?**
  - Employees are intimately familiar with daily operations.
  - They are uniquely positioned to spot anomalies or suspicious behavior.
  - They may have moral objections to fraudulent activities.
- **Conclusion:** Creating a safe and effective reporting environment is paramount for fraud detection.



# Why Anonymous Reporting? The Fear Factor

- Anonymous reporting mechanisms are vital for overcoming the fear of retaliation and encouraging employees to speak up.
- **Reason for Anonymity:** Fear of retaliation is the primary deterrent for employees to report wrongdoing.
- **Fears Include:**
  - Losing their job.
  - Being ostracized by colleagues.
  - Damage to their career.
  - Facing legal repercussions.
  - Being wrongly accused.
- **Benefit of Anonymity:** Encourages reporting from those who might otherwise stay silent, increasing the likelihood of early detection.



# Types of Reporting Mechanisms: Multiple Pathways

- A variety of reporting mechanisms, such as hotlines, email, or web forms, should be available to employees.

- **Variety of Channels:**
  - **Dedicated Hotline (Third-Party):** Often preferred for anonymity and independence.
  - **Ethics/Compliance Email Address:** Monitored by a designated impartial party.
  - **Secure Web Form:** Anonymous submission via a website.
  - **Direct to Supervisor/Manager:** For those comfortable with this route.
  - **Direct to HR/Legal/Internal Audit:** For more sensitive issues.
  - **Direct to Board Chair/Committee:** For senior management concerns.

- **Key:** Offer multiple, accessible, and trusted channels.

# Essential Elements of a Hotline System: Building Trust

- A successful hotline system is built on key elements, including accessibility, anonymity, and a clear process for handling tips.

- **For a Truly Effective System:**
  - **Accessibility:** Easy to find and use.
  - **Anonymity:** Guaranteed when desired and legally possible.
  - **Independence:** Managed by a neutral party (internal or external).
  - **Clarity:** Clear instructions on what to report and how.
  - **Prompt Response:** All reports must be acknowledged and investigated swiftly.
  - **Confidentiality:** Protection of caller identity and information.
  - **Non-Retaliation Policy:** Explicitly stated and enforced.

# Communicating the Hotline: Making It Visible

- Even the best hotline system is useless if employees are unaware of its existence or how to use it.
- **Crucial Step:** A hotline is useless if no one knows about it or trusts it.
- **Methods of Communication:**
  - Prominent display on the organization's intranet and website.
  - Posters in common areas (breakrooms, notice boards).
  - Included in employee handbooks and onboarding materials.
  - Mentioned during ethics and fraud prevention training sessions.
  - Regular reminders from management.
  - On the back of employee badges or pay stubs.
- **Consistency:** The message must be consistent and reassuring.



# Protecting Whistleblowers: Legal and Ethical Imperatives

- Protecting whistleblowers from retaliation is not only an ethical obligation but also a legal requirement.
- **Legal Protections:** Various laws (e.g., Sarbanes-Oxley, Dodd-Frank, specific federal grant regulations) protect whistleblowers from retaliation.
- **Organizational Commitment:**
  - Explicit nonretaliation policy.
  - Clear procedures for addressing alleged retaliation.
  - Training for managers on how to handle reports and avoid retaliation.
  - Confidentiality (to the extent possible).
- **Ethical Obligation:** Fosters a just and transparent workplace.
- **Impact:** Builds trust, encourages reporting, and reduces the cost of fraud.

# Investigating Reports Promptly and Fairly: Building Trust

- Responding to all reports with prompt and fair investigation is essential for building and maintaining employee trust.
- **Why It Matters:** The credibility of the reporting system hinges on how reports are handled.
- **Key Principles:**
  - **Timeliness:** Investigate quickly to preserve evidence and demonstrate commitment.
  - **Objectivity:** Conduct investigations impartially, without bias.
  - **Thoroughness:** Follow all leads and gather sufficient evidence.
  - **Confidentiality:** Protect identities to the extent possible.
  - **Communication (to Reporter, if known):** Provide updates, where appropriate, without compromising investigation.
  - **Action:** Take appropriate disciplinary, corrective, or legal action based on findings.
- **Impact:** Reinforces the system's value and encourages future reporting.

# Role of a Compliance Officer: Overseeing Reporting

- A designated compliance officer or equivalent role is often responsible for overseeing the entire reporting process.

- **Responsibilities:**
  - **Managing the Hotline:** Ensuring reports are received and triaged.
  - **Oversight of Investigations:** Ensuring investigations are conducted properly.
  - **Policy Development:** Creating and updating ethics and reporting policies.
  - **Training & Communication:** Promoting awareness of compliance programs.
  - **Advising Management:** On compliance risks and corrective actions.
  - **Liaison with External Parties:** When necessary (e.g., legal counsel, regulators).

- **Key:** This role needs independence and authority to be effective.



# Best Practices for Hotline Implementation: A Checklist

- Following best practices for your hotline system will increase its effectiveness and credibility.

- **Ensure:**
  - **Independence:** Third-party provider or dedicated internal function.
  - **Accessibility:** 24/7, multiple languages, multiple channels.
  - **Anonymity Guaranteed:** Clear policy and technical capability.
  - **Clear Policies:** What to report, how it's handled, nonretaliation.
  - **High-Level Buy-in:** Board and senior management support.
  - **Regular Promotion:** Keep it visible.
  - **Prompt & Consistent Response:** Investigate every credible report.
  - **Feedback Loop:** Communicate outcomes (if possible, without compromising anonymity).

# Beyond Audits: Continuous Monitoring

- While audits are important, a continuous monitoring approach provides an ongoing layer of oversight.
- **Core Idea:** While annual audits are important, continuous monitoring involves ongoing, automated, or semi-automated processes to detect anomalies or control failures.
- **How It Differs from Audits:**
  - **Frequency:** Real-time or near real-time vs. annual/biennial.
  - **Scope:** Focus on specific transactions/data vs. broad financial statements.
  - **Automation:** Often leverages technology.
- **Benefit:** Catches issues much faster, potentially preventing larger losses.

# Types of Regular Reviews: Varied Approaches

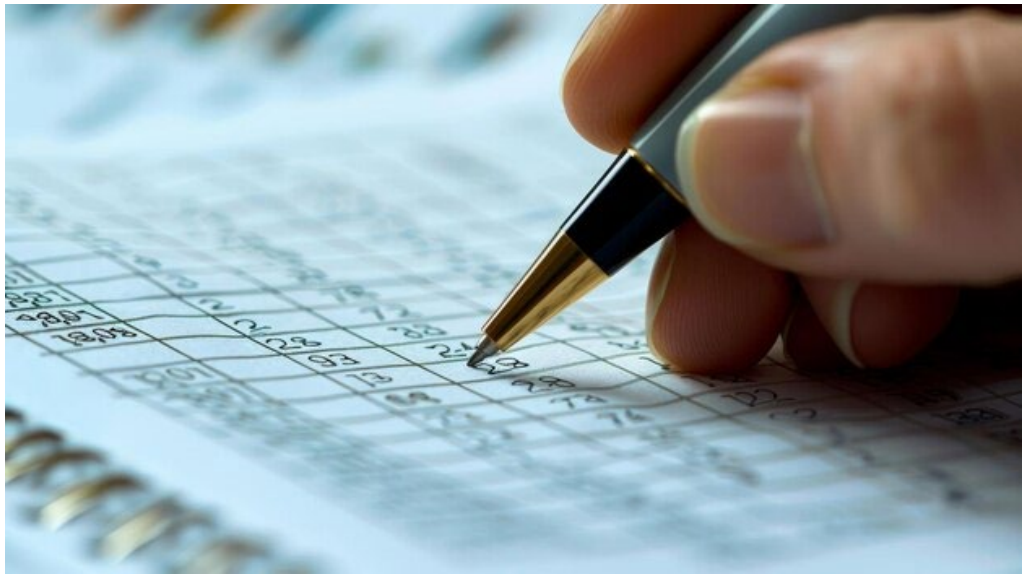
- There are many types of regular reviews you can implement to monitor grant activities effectively.

- **Methods for Ongoing Scrutiny:**
  - **Transactional Reviews:** Looking at individual transactions.
  - **Reconciliations:** As discussed in Module 4.
  - **Analytical Procedures:** Comparing data sets for unusual trends.
  - **Surprise Audits/Inspections:** Unannounced checks.
  - **Management Reviews:** Regular review of operational and financial reports by supervisors.

- **Key:** Diversify your review methods to cover different aspects of operations.

# Financial Transaction Reviews: Scrutinizing the Details

- Careful review of financial transactions, such as invoices and payroll, is a key preventative measure.
- **Focus:** Examining individual financial transactions for appropriateness, authorization, and supporting documentation.
- **What to Look For:**
  - Unusual vendors, amounts, or transaction dates.
  - Missing or questionable approvals.
  - Invoices without proper supporting documentation.
  - Duplicate payments.
  - Split purchases to avoid approval limits.
  - High volume of manual journal entries.
  - Expenses that seem inconsistent with grant purpose.
- **Who Does It:** Designated financial staff, internal audit, or managers.



# Operational Reviews: Beyond the Finances

- Operational reviews focus on programmatic activities to ensure they are aligned with grant goals and requirements.
- **Focus:** Assessing the effectiveness and integrity of programmatic operations, not just financial transactions.
- **What to Look For:**
  - Discrepancies between reported program progress and actual activity.
  - Verification of beneficiary lists and services provided.
  - Physical inspection of assets (equipment, inventory).
  - Review of staff time allocation to specific programs.
  - Compliance with specific grant programmatic requirements.
  - Effectiveness of subrecipient activities.
- **Who Does It:** Program managers, internal audit, or a dedicated compliance team.

# Budget vs. Actual Analysis: Spotting Discrepancies

- Regularly comparing your budget to actual expenditures can quickly highlight inconsistencies or unauthorized spending.
- **Method:** Regularly comparing actual expenditures and revenues against the approved grant budget.
- **Why It's a Detection Tool:**
  - **Significant Overspending:** Could indicate misuse of funds or attempts to hide costs.
  - **Significant Underspending:** Could indicate non-delivery of services, or funds being held for improper use.
  - **Unusual Variances:** Unexpected shifts in spending patterns within budget categories.
- **Key:** Requires thorough investigation of *all* significant variances, not just overruns.



# Independent Reviewers: Adding a Layer of Objectivity

- Using independent reviewers for checks and balances helps ensure objectivity and prevents fraud.
- **Principle:** Reviews are most effective when performed by someone independent of the original transaction or process.
- **Examples:**
  - A supervisor reviews their team's expense reports.
  - An internal auditor reviews financial reconciliations.
  - A different department reviews procurement activities.
  - Board committees (e.g., finance, audit) review high-level financial reports.
- **Impact:** Reduces the opportunity for collusion and increases the likelihood of detecting errors or fraud.

# Frequency of Reviews: Matching Risk to Vigilance

- The frequency of your reviews should be tailored to the specific risks and volume of transactions associated with each grant.

- **Considerations:** The optimal frequency of reviews depends on the risk level and volume of transactions.
  - **High-Risk Areas/Activities:** Daily, weekly, or monthly (e.g., cash handling, large procurements).
  - **Moderate Risk:** Monthly or quarterly (e.g., general ledger reconciliations, expense report reviews).
  - **Lower Risk:** Annually or periodically (e.g., asset inventory checks).

- **Key:** Establish a clear schedule for all review activities and ensure adherence.

# Documenting Reviews: Evidence of Oversight

- Properly documenting all reviews provides a clear evidence trail of your due diligence and oversight.
- **Importance:** If a review isn't documented, it's hard to prove it happened or what was found.
- **What to Document:**
  - Date of review.
  - Who performed the review.
  - What was reviewed (specific transactions, period).
  - Findings (errors, red flags, compliance issues).
  - Corrective actions taken or recommended.
  - Signatures/initials of reviewer.
- **Benefit:** Provides an audit trail for future reference and demonstrates due diligence.



# Follow-Up on Anomalies: Don't Dismiss Red Flags

- Finding an anomaly is not enough; you must also have a clear process for investigating and resolving any identified red flags.
- **Key Principle:** Detection is useless without action. Any red flag or unusual finding from a review *must* be investigated.
- **Steps:**
  - **Inquire:** Ask questions to the responsible parties.
  - **Gather Evidence:** Request supporting documentation.
  - **Corroborate**: Verify information with independent sources.
  - **Escalate:** If suspicion persists or evidence mounts, escalate to appropriate channels (e.g., internal audit, legal, compliance, management).
- **Impact:** Prevents small issues from becoming large frauds.

# Benefits of Proactive Review: Stronger Organizations

- Proactive reviews offer numerous benefits, including stronger controls and enhanced grant compliance.

- **Overall Advantages:**
  - **Earlier Detection:** Catches fraud faster, minimizing losses.
  - **Enhanced Control Effectiveness:** Identifies and fixes control weaknesses.
  - **Improved Compliance:** Ensures adherence to grant regulations.
  - **Increased Efficiency:** Streamlines processes by identifying bottlenecks.
  - **Greater Accountability:** Promotes ownership of financial integrity.
  - **Stronger Reputation:** Builds trust with grantors and stakeholders.

- **Conclusion:** Proactive review is an essential component of a robust fraud prevention strategy.

# Module Summary & Key Takeaways

- To conclude, a combination of employee training, anonymous reporting, and continuous review forms a powerful defense against fraud.

- **Recap:**
  - Effective fraud prevention goes beyond internal controls, focusing on proactive measures.
  - Employee training is paramount, empowering staff to recognize and report fraud.
  - Robust, trusted, and well-communicated hotlines/reporting mechanisms are crucial for detection.
  - Regular, documented reviews and continuous monitoring provide ongoing vigilance.
  - A strong ethical culture and leadership commitment underpin all successful prevention efforts.

- **Action Item:** Consider which of these prevention measures you can strengthen or implement in your organization to create a more resilient defense against grants fraud.