

The Anti-Fraud, Waste and Abuse Framework Workshop


Training for Federal, State & Local Grantees & Subgrantees

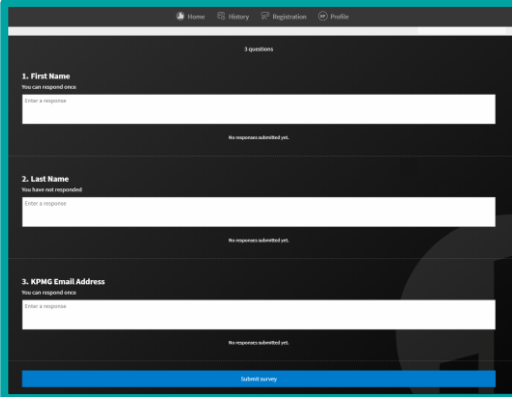
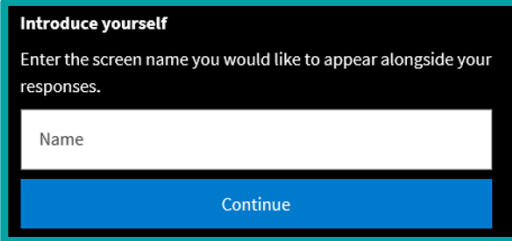
January 2025



Would You Like CPE for this Session?

During this session we will be utilizing Poll Everywhere to track responses to discussion questions.

1. From your laptop OR mobile device, navigate to:  <https://pollev.com/fraudworkshop>
2. Introduce yourself: Please enter your FULL NAME when prompted (do not skip!) and click/tap Continue.
3. Complete the Check In shown on screen. Complete all three fields and then click Submit.
4. Keep the Poll Everywhere window open. You will need it throughout the training.



If you are having any trouble joining or submitting answers, communicate your issue by raising your hand.

Check In

0 surveys completed

0 surveys underway

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

OSC Training Facilitators



Stacey Alles
State of Colorado



Gina Salazar
State of Colorado

KPMG Training Facilitators



Tom Stanton
KPMG



Steven D'Antuono
KPMG



Jeffrey Thomas
KPMG



Lekshmy Sankar
KPMG



Andrew Neville
KPMG



Jeremy Cirillo
KPMG

KPMG Training Support



Linnea Garland
KPMG



Cody Bowles
KPMG



Hope Hackmann
KPMG



Kaitlin Forman
KPMG

Learning Objectives



The objective of this training is to provide practical guidance for departments looking to begin, advance, or benchmark their fraud risk management (FRM) programs against industry best practices. This workshop includes key questions, checklists, and insights to enhance your department's fraud, waste, and abuse (FWA) program and facilitate proactive FWA management.

Participants should be familiar with the following:

- ✓ The benefits of having a fraud, waste, and abuse (FWA) framework in place
- ✓ The types of fraud risks relevant to the programs or projects their department manages
- ✓ Detection and prevention techniques
- ✓ The processes for reporting suspected fraud, waste, and abuse within their department

Training Schedule (Day 1)

Time	Topic
9:00am – 9:05am	Introductions
9:05am – 9:30am	What is Fraud, Waste, and Abuse and Why You Need A Framework
9:30am – 10:30am	Assessing Your Existing Fraud Framework
10:30am – 10:45am	Break
10:45am – 11:30am	Identify Fraud, Waste and Abuse Risks and Schemes
11:30am – 12:00pm	The Importance of Internal Controls
12:00pm – 1:30pm	Lunch
1:30pm – 2:00pm	How to Conduct your FWA Risk Assessment
2:00pm – 2:30pm	How to Conduct a Successful Investigation
2:30pm – 3:00pm	Pulling It All Together - Documenting Your Fraud, Waste and Abuse Policy

Training Schedule (Day 2)

Time	Topic
9:00 – 9:30am	Riskier Federal Grant Projects That May Be Vulnerable To Fraud
9:30am – 10:00am	Using Data Analytics to Uncover Fraud, Waste and Abuse
10:00am – 10:15 am	Break
10:15am – 11:15am	Case Study - Applicant Programs
11:15am – 12:15pm	Government Agencies Cyber Risks

Day 1

What agency are you a part of?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What is Fraud, Waste and Abuse



What is Fraud, Waste, and Abuse? (1 of 3)



Fraud is defined as attempting to obtain something of value through willful misrepresentation that is intended to result in financial or personal gain. Fraud includes underreporting income to receive federal subsidies for food and housing or selling counterfeit electronics to an agency.

Other examples include, but are not limited to, the following:

- **Falsification of information** in applications, contracts, etc.
- Billing for services not rendered or **duplication of payments**;
- **Alteration of documents** or forgery, which may include contracts, purchase orders, etc.
- Bribery or kickbacks;
- False claims or bid rigging;
- Theft, embezzlement, or other misapplication of funds or assets;
- **Falsifying eligibility.**

What is Fraud, Waste, and Abuse? (2 of 3)



Waste is defined as the thoughtless or careless expenditure, mishandling, and/or abuse of resources to the detriment (or potential detriment) of the U.S. Government. Failure to observe laws, rules or regulations when handling public funds leading to a wrongful use of public funds may constitute waste and mismanagement.

For example, incurring in unnecessary costs resulting from inefficient or ineffective practices, systems, or controls, such as, but are not limited to, the following:

- Purchasing **unnecessary** supplies, material, and equipment;
- Purchasing supplies **without regard to cost**;
- Using supplies, materials, and equipment **carelessly resulting in unnecessary waste and replacement.**

What is Fraud, Waste, and Abuse? (3 of 3)



Abuse is defined as excessive or improper use of a thing, or to use something in a manner contrary to the natural or legal rules for its use. Abuse can occur in financial or non-financial settings.

Examples include, but are not limited to, the following:

- Making procurement or vendor selections that are **contrary to existing policies or are unnecessarily extravagant or expensive**;
- **Receiving favor** for awarding contracts to certain vendors;
- Using one's position **for personal gain or to gain an advantage over another**;
- Failure to report damage to equipment or property;
- Creating unneeded overtime; and
- Requesting staff to perform **personal errands or work tasks for a supervisor or manager**.

Jon Stewart Questions Defense Deputy Secretary On Budget



Which of the following would be considered fraud?

Making honest mistakes

Deliberately deceiving to secure an unfair gain

Being inefficient at work

Failing to report to work on time

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following would be considered fraud?

Making honest mistakes

0%

Deliberately deceiving to secure an unfair gain

0%

Being inefficient at work

0%

Failing to report to work on time

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following would be considered fraud?

Making honest mistakes

0%

Deliberately deceiving to secure an unfair gain

0%

Being inefficient at work

0%

Failing to report to work on time

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following would be considered waste?

Intentionally destroying company property

Using more resources than necessary due to carelessness or poor planning

Reporting minor errors to supervisors

Efficiently completing a task

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following would be considered waste?

Intentionally destroying company property

0%

Using more resources than necessary due to carelessness or poor planning

0%

Reporting minor errors to supervisors

0%

Efficiently completing a task

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following would be considered waste?

Intentionally destroying company property

0%

Using more resources than necessary due to carelessness or poor planning

0%

Reporting minor errors to supervisors

0%

Efficiently completing a task

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following is considered abuse?

Taking long breaks

Misusing company resources for personal gain

Anonymously reporting fraud

Giving constructive feedback

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following is considered abuse?

Taking long breaks

0%

Misusing company resources for personal gain

0%

Anonymously reporting fraud

0%

Giving constructive feedback

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following is considered abuse?

Taking long breaks

0%

Misusing company resources for personal gain

0%

Anonymously reporting fraud

0%

Giving constructive feedback

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

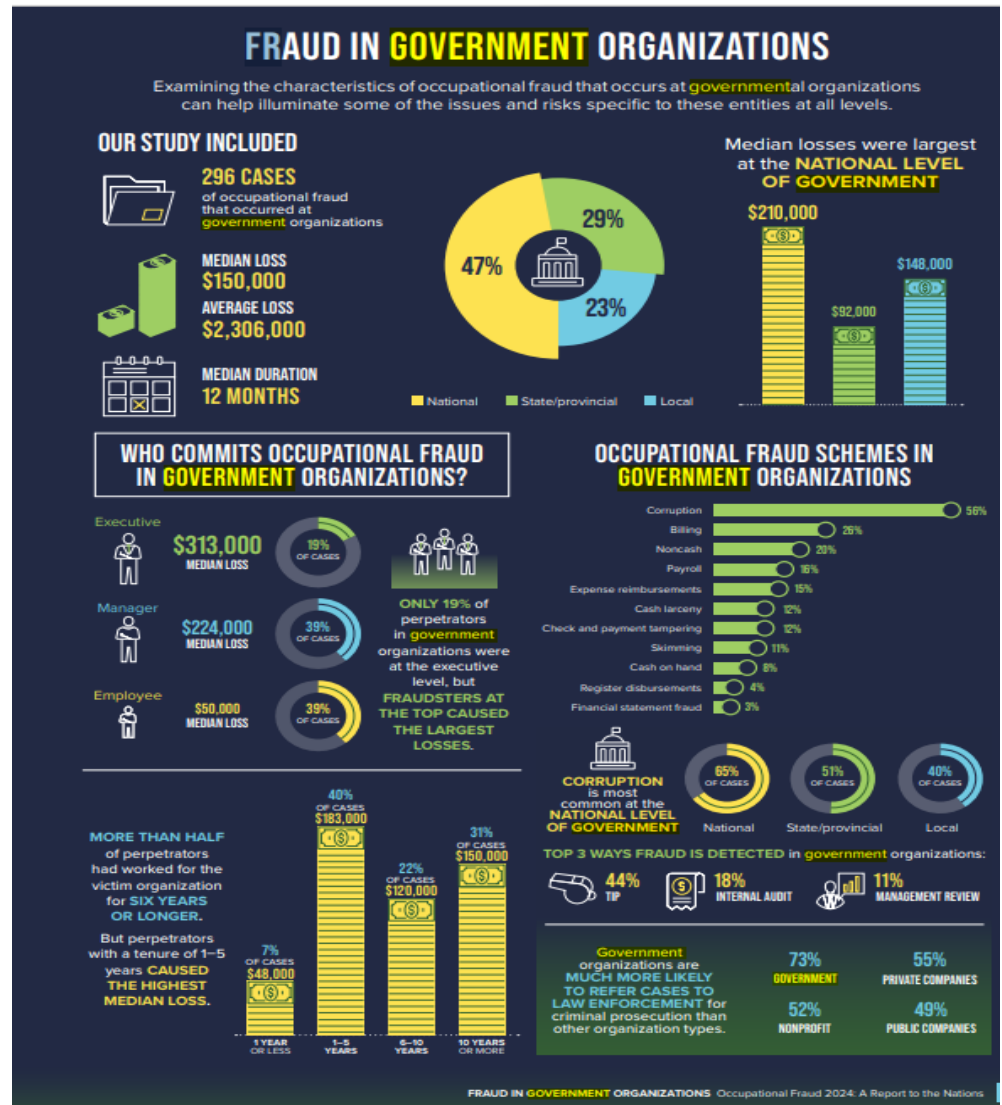
Why Do You Need an Anti-Fraud, Waste, and Abuse Framework



FWA Framework (1 of 3)

Fraud, waste, and abuse is happening at your department, you just don't know it

Then again, maybe you do, but you are not sure how pervasive the problem is, where to begin your anti-FWA journey, or how to enhance your current FWA risk management practices. Either way, FWA is big business at state and local agencies across the globe. According to the [ACFE 2024 Report to the Nations](#), CFEs estimate that organizations lose 5% of their revenue to fraud each year.



Source: © 2024 Association of Certified Fraud Examiners, Inc., Report to the Nations on Occupational Fraud and Abuse.

Feeding Our Future Scandal Rocks Minnesota Beyond Twin Cities



Have you witnessed fraud, waste, or abuse in your department? In what scenarios?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

FWA Framework (2 of 3)

This workshop is designed to help reduce fraud risk by assisting departments create a fraud framework via a phased approach.

A structured fraud framework helps to identify, prevent, and respond to potentially fraudulent activities effectively. Here are several reasons why a fraud framework is beneficial:

- ✓ **Risk Assessment:** A fraud framework enables departments to assess their unique vulnerabilities to fraud based on their operations, financial transactions, and specific programs.
- ✓ **Prevention and Detection:** Establishing policies and procedures can help prevent fraud from occurring. This includes implementing internal controls, conducting regular training for employees, and promoting a culture of integrity and accountability.
- ✓ **Consistent Practices:** By having a defined framework, departments can ensure consistent approaches in handling fraud-related cases, which aids in accountability and transparency.
- ✓ **Regulatory Compliance:** A comprehensive fraud framework helps ensure compliance with federal and state regulations, reducing the risk of penalties and legal repercussions.

FWA Framework (3 of 3)

- ✓ **Effective Reporting Mechanisms:** A fraud framework should include clear reporting channels for employees and the public to report suspected fraud without fear of retaliation.
- ✓ **Timely Response:** An established framework allows departments to respond quickly and effectively to incidents of fraud, minimizing potential losses and protecting public funds.
- ✓ **Continuous Improvement:** A fraud framework promotes regular reviews and updates of policies and procedures based on lessons learned from past incidents, emerging trends, and evolving risks.
- ✓ **Stakeholder Confidence:** A robust fraud framework builds trust among stakeholders, including the public, as it demonstrates that the department is committed to ethical practices and safeguarding resources.

Combating FWA is an ongoing challenge, but this workshop will help you stay a step ahead.

Minnesota Gov. Tim Walz Unveils Measures to Combat Fraud



RAW: WALZ ANNOUNCES FRAUD INVESTIGATION UNIT

Assess Your Existing Fraud Framework and Determine Where You Want to Be



Does your department currently have a Fraud, Waste, and Abuse framework?

0

Yes

No

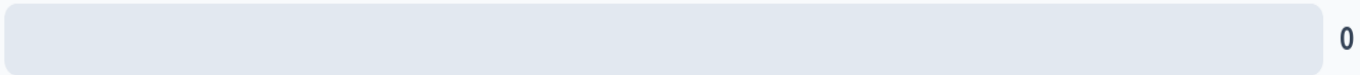
Somewhat

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

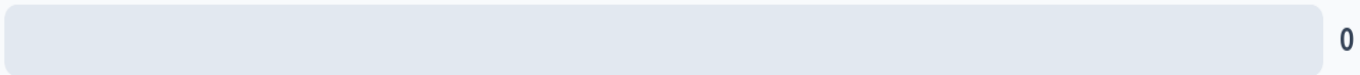
Does your department currently have a Fraud, Waste, and Abuse framework?

0

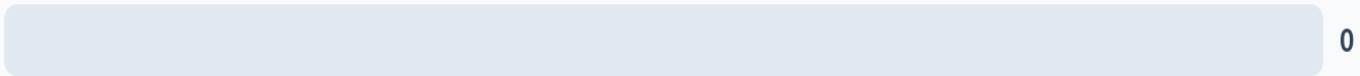
Yes



No



Somewhat

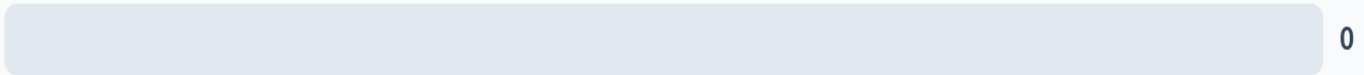


Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

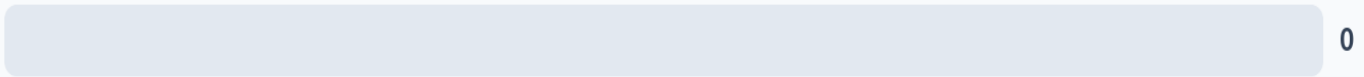
Does your department currently have a Fraud, Waste, and Abuse framework?

0

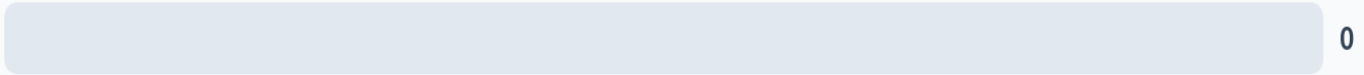
Yes



No



Somewhat



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Assess Existing State of Your Fraud Framework (1 of 5)

Understand Where You Are and Where You Want to Be

- ✓ FWA risk management should be **right-sized** and **tailored** for the unique needs of each department, and not every department requires the same level of FWA risk management.
- ✓ For example, departments with limited fraud exposure or those that are willing to accept more fraud risk might not need to aim for the highest level of FWA risk maturity. Instead, they might aim for basic or moderate levels as a goal state, as detailed in the next slide.
- ✓ The first step in this process is **understanding** where your departments FWA risk management program stands today (i.e., the current state).
- ✓ Once you understand your current state, you can **identify your long-term vision** and **goal state**. This process will allow you to develop a roadmap for the future and focus on gaps that need to be addressed to propel efforts from the current to the goal state, ensuring resources are effectively utilized in areas of high impact and high priority.

Assess Existing State of Your Fraud Framework (2 of 5)

Understand Where You Are and Where You Want to Be

FWA Pillars	Ineffective Phase 1	Basic Phase 2	Moderate Phase 3	Effective Phase 4	Best-in-Practice Phase 5
FWA Risk Governance	<ul style="list-style-type: none"> FWA policies and procedures are not documented, constantly changing, and reactive. Assessments not being performed Success is likely contingent upon individual efforts and may not be deemed repeatable due to the lack of sufficiently defined and documented processes that would enable replication 	<ul style="list-style-type: none"> The department is aware of the need for a more formal FWA approach Assessments are performed; however, FWA risk definitions vary across the department. FWA risks are managed in silos and department wide risks are not routinely considered. Risks are managed in a reactive way 	<ul style="list-style-type: none"> There are established sets of defined and documented standard processes in place. The approaches are standardized and can be consistently repeated. Fraud, waste, and abuse risk management aligns with both the external and internal environments of the department and is integrated into the department's enterprise risk program. Executive and deputy directors receive FWA risk overviews or reports Roles, responsibilities, and key performance measurements are defined and documented 	<ul style="list-style-type: none"> FWA risk management activities across the department are aligned with controls and key performance indicators Key performance indicators are defined and our measured Information on FWA risks is collected, analyzed, and made accessible to executives and deputy directors. A process for informing management of changes to FWA risk profiles has been established and is functioning effectively Full integration of the FWA pillars into management processes has been achieved 	<ul style="list-style-type: none"> The department is dedicated to enhancing FWA risk management by implementing both gradual and innovative improvements Executive and deputy directors discuss FWA risk with a goal of strategic, operational, and profitability improvements Fraud risk tolerance has been defined, and fraud risk assessments are structured to alert the executive and deputy directors whenever established thresholds are surpassed The department consistently keeps under review the nature of FWA risks it faces, given these are likely to change over time or program and fraud prevention, detection and responses measures are updated accordingly.
FWA Risk Assessment					
FWA Control Activities					
FWA Investigation & Corrective Action					
FWA Monitoring Activities					

At which phase would you rate your department's current fraud framework?

Phase 1

Phase 2

Phase 3

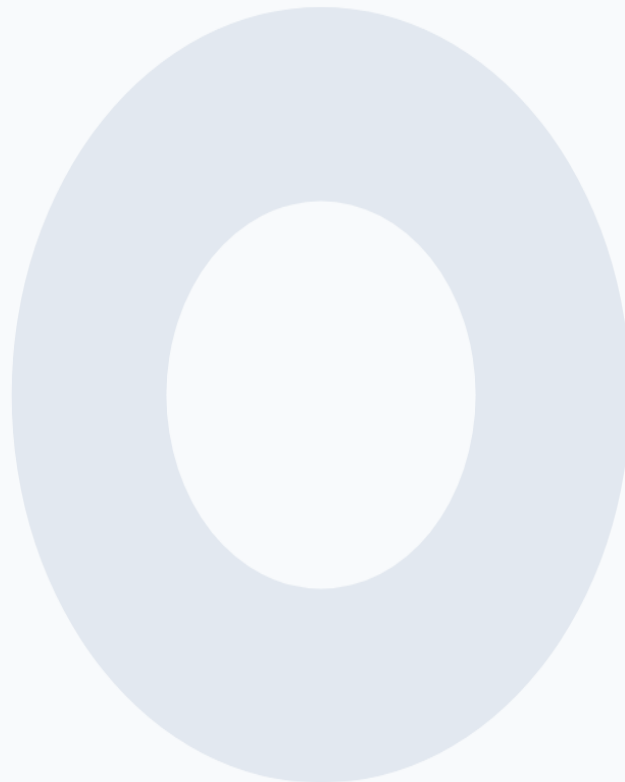
Phase 4

Phase 5

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

At which phase would you rate your department's current fraud framework?

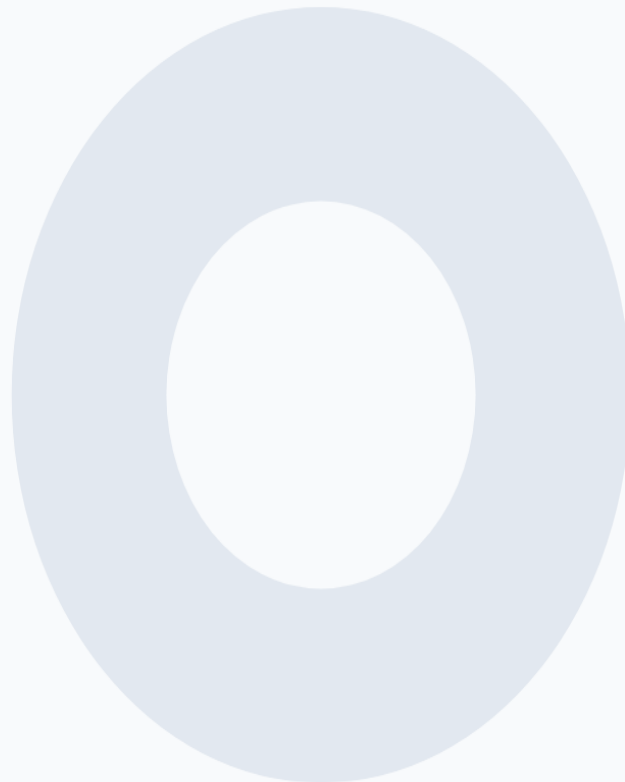
Phase 1 Phase 2 Phase 3 Phase 4 Phase 5



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

At which phase would you rate your department's current fraud framework?

Phase 1 Phase 2 Phase 3 Phase 4 Phase 5



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Assess Existing State of Your Fraud Framework (3 of 5)

The table below outlines key questions and a checklist to help your department conduct a maturity assessment and develop a roadmap for the future, in line with leading practices and guidance.

Key Questions	Checklist
<ul style="list-style-type: none"> • Which stage outlined in the maturity model most closely aligns with the current state of your FWA risk management program? <ul style="list-style-type: none"> ○ How does this vary across each of the five FWA pillars? 	<ul style="list-style-type: none"> <input type="checkbox"/> Identify your current state. Evaluate your department's current FWA efforts and identify your current state both overall and across each federal program. You can leverage the Enterprise FWA Maturity Assessment Model and the ACFE's FRM Scorecards to assist in evaluating the current state of your FWA risk management program and related activities
<ul style="list-style-type: none"> • What is the long-term vision for your FWA risk management program? <ul style="list-style-type: none"> ○ Which stage outlined in the model most closely aligns with your long-term vision? ○ How does your long-term vision vary across each of the five FWA pillars? 	<ul style="list-style-type: none"> <input type="checkbox"/> Identify your goal state. Identify your department's goal state both overall.

Assess Existing State of Your Fraud Framework (4 of 5)

Key Questions	Checklist
<ul style="list-style-type: none">• What do you need to accomplish in both the short- and long-term to achieve your goal state?<ul style="list-style-type: none">○ What gaps exist between your current state and your goal state?○ How will you prioritize FWA risk management efforts and activities related to closing those gaps?	<ul style="list-style-type: none">❑ Develop a comprehensive FWA risk management strategy and roadmap. Your strategy and roadmap should align to your vision and goal state, including both short- and long-term plans to achieve your goal state based on the gaps identified. You can do this by pinpointing and prioritizing the gaps between your current level of maturity and your goal state both overall and across each of the five FWA pillars. For example, the ACFE's FRM Scorecards will highlight where current gaps are across each of the five pillars.

Assess Existing State of Your Fraud Framework (5 of 5)

- The ACFE has developed [interactive FRM Scorecards](#), which can be used to assess the components of your department's existing FRM program.
 - ✓ The scorecards are based on the **five FRM principles** found in the ACFE/COSO Fraud Risk Management Guide.
 - ✓ They support an organization's periodic self-assessment and can be leveraged to easily identify gaps in your current FWA risk management program and to assist in identifying your program's current state.
- When establishing a goal state and roadmap for an FWA program, be sure to align the plan with broader department objectives.
- Advanced FWA controls may not be tolerated by the department if they create excessive complexity or impede core business processes. Strike a balance and be flexible as the needs of the department evolve over time.

Break



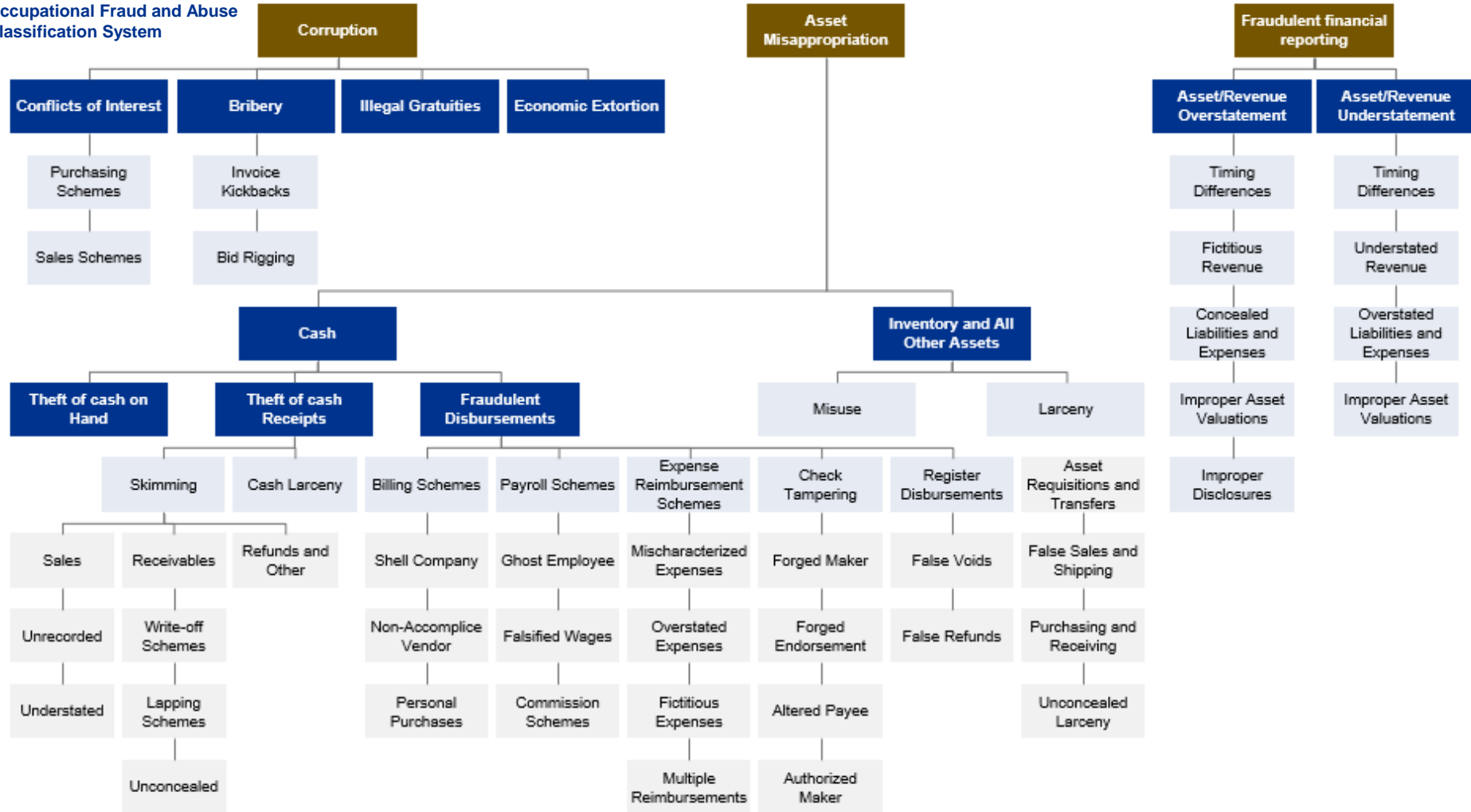
Identify Fraud, Waste and Abuse Schemes



Identifying the Likely FWA Schemes

There is no shortage of fraud schemes....

Occupational Fraud and Abuse Classification System



Source: © 2024 Association of Certified Fraud Examiners, Inc., Report to the Nations on Occupational Fraud and Abuse.

Grant Fraud Risks

“Grant fraud,” encompasses a wide range of improper activities often summarized in three general categories: conflicts of interest, materially false statements, and theft.

- ✓ A **conflict of interest** may occur when an entity engages in transactions involving undisclosed related parties. For example, a grant recipient hiring a relative as an employee or as a vendor to supply grant-funded products and services may constitute a conflict of interest. Also, a conflict may result where a grant recipient purchases goods or services from a business in which the grant recipient has an ownership interest. Conflicts may also occur in the grant award-making process or sub-award process at the federal, state, or local level.
- ✓ Grant fraud may also involve **materially false statements to the government**. Such misstatements may be misleading to the grant-awarding body and may occur during the application process or during the implementation of the grant program. This type of fraud may include false certifications that grant recipients will use grant funds properly or abide by particular requirements. Grant recipients that fail to maintain adequate supporting documentation about the use of funds, misrepresent elements of costs, or attempt to charge unallowable costs to a federal grant have potentially made false statements or presented false claims to the government. These activities have different consequences depending on many factors, including the level of intent of the individuals involved.
- ✓ **Theft** is one of the more common grant fraud issues and it can take many forms. For example, creative bookkeepers may create fictitious transactions, and employees may misuse a credit card designated for grant-funded purchases.

Identifying the Likely FWA Schemes for Your Project (1 of 6)

Identifying the likely FWA schemes that your department is vulnerable to, both internal and external, is imperative to informing your FWA risk assessment. Thinking like a fraudster and brainstorming the various FWA schemes that could be used to commit FWA within or against your department is a key step

The state owes me, and it won't hurt anyone if I steal one small check, right?

Jeff always leaves his computer unlocked.

When he steps away, I can hack into applicant account information to sell on the dark web - or change payee information to my bank account.

My supervisor and I both need fast cash. I will add overtime hours to my time sheet, and we will split the profits.

Former Quincy Official Facing Charges for Allegedly Embezzling City Funds



**CBS NEWS
BOSTON**

For each federal program, does your department currently take the time to identify the possible fraud schemes that could occur?

Yes

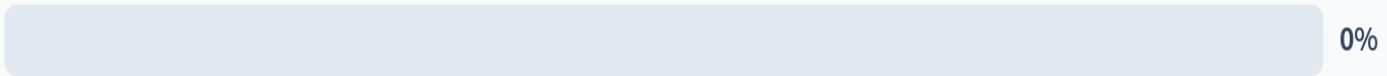
No

Sometimes

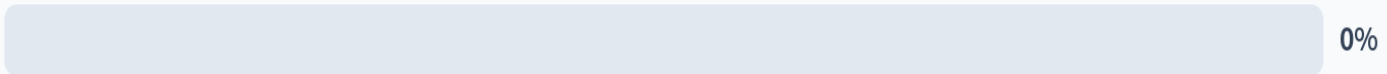
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

For each federal program, does your department currently take the time to identify the possible fraud schemes that could occur?

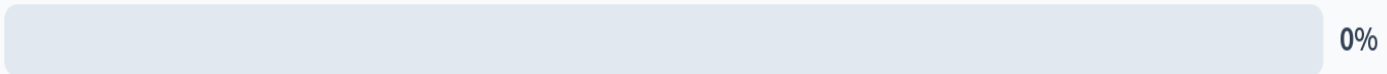
Yes



No



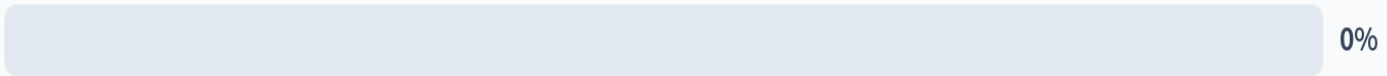
Sometimes



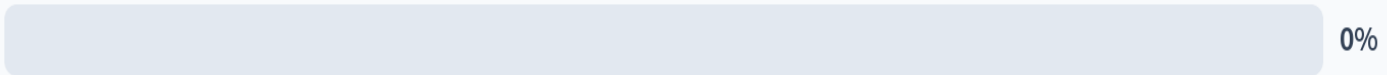
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

For each federal program, does your department currently take the time to identify the possible fraud schemes that could occur?

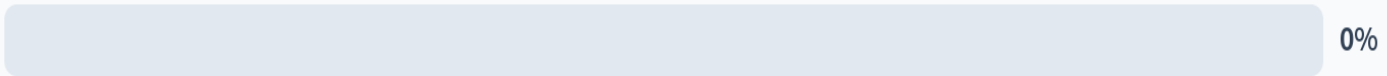
Yes



No



Sometimes



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Identifying the Likely FWA Schemes for Your Project (2 of 6)

You can accomplish this effort by developing a comprehensive [FWA Risk Map](#), which identifies significant FWA scenarios across your entire department. A FWA Risk Map is a resource that outlines identified potential FWA schemes and other related information for each scheme, such as actor and FWA risk entry point, for various areas across your department and is a resource you will be able to employ across your FWA risk management activities. For an example, see the sample **FWA Risk Map** template below.

Business Unit	Internal or External	General Fraud Category	Fraud Scheme Type	Actor	Fraud Risk Entry Point	Underlying Fraud Risk
Payroll	Internal	Asset Misappropriation	Payroll	Payroll Employee / Management	Payroll Records	A payroll employee or member of a management submits an authorized pay rate increase, either for themselves or another internal party / accomplice
Payroll	Internal	Asset Misappropriation	Payroll	Payroll Employee / Management	Payroll Records	A payroll employee or member of management creates a fake employee in the payroll records and falsifies the payment record so that the direct deposit information is replaced with bank account information of his / her own

Identifying the Likely FWA Schemes for Your Project (3 of 6)

- Utilizing the concept of **thinking like a fraudster**, you can work to identify and develop FWA scenarios based on known FWA events and investigations, existing risks identified through other risk management efforts, industry and general fraud risk research, and discussions with process owners and key stakeholders.
- The benefits of a FWA risk map are boundless; it will improve and provide your organization with a comprehensive understanding of FWA vulnerabilities and provide key inputs for the FWA risk assessment process. Further, the FWA risk map is an artifact that you can continue to refine and use to assess FWA risks going-forward.



Identifying the Likely FWA Schemes (4 of 6)

The tables below outlines key questions and a checklist to help your department identify FWA risks.

Points of Focus	Key Questions
<ul style="list-style-type: none">• Includes entity, subsidiary, division, operating unit, and functional levels• Analyzes internal and external factors• Considers various types of fraud, waste and abuse• Specifically considers the risk of management override of controls• Assesses personnel or departments involved and all aspects of the Fraud Triangle	<ul style="list-style-type: none">• How will you break down your fraud risk map to include your entire department (i.e., Management, employees, subrecipients, contractors, etc.)?• What type of information do you want your FWA risk map to include? How can you translate that into an effective template?• How might a perpetrator exploit any weaknesses in the system of controls?<ul style="list-style-type: none">○ What internal FWA schemes is your department vulnerable to?○ How could a perpetrator override or circumvent controls?○ Who might have a motive or incentive to commit FWA?○ What type of external FWA schemes is your department vulnerable to?• What types of FWA are most prevalent based on known occurrences? What other internal data can you leverage to identify potential FWA schemes?• Have you considered non-financial FWA risks and schemes?

Identifying the Likely FWA Schemes (5 of 6)

Checklist

- Determine how you want to break out your FWA risk map. This can be by department, grant program, project etc., be sure to consider the entire department and recognize that FWA can happen at any level or within any component of the department. Further, ensure that the way you break out your FWA risk map aligns with how you plan to conduct your FWA risk assessment.
- Develop your FWA risk map framework in line with how you want to break out your FWA risk map as determined in the previous step. You can leverage the [ACFE's Risk Assessment and Follow-Up Action Templates](#) to assist in developing a framework for your FWA risk map. While this resource can provide a useful starting point, you should tailor your FWA risk map to meet the needs and objectives of your FWA risk management program and FWA risk assessment.
- Identify internal and external FWA schemes for each area of your FWA risk map. For example, if you chose to break it out by grant program, then do this for each program.

Identifying the Likely FWA Schemes (6 of 6)

Checklist

- Key considerations include:
 - When identifying FWA schemes, do so in a group setting whenever possible. Your efforts will benefit from conversations between relevant stakeholders who understand the functional area for which you are brainstorming FWA schemes.
 - Consider both the actor (i.e., the perpetrator) and the FWA risk entry points (i.e., the function or process that the actor capitalizes on to carry out the FWA scheme).
 - Remember that not all FWA is financial. Some FWA can affect a department's reputation even if it doesn't lead to major financial loss.
 - Leverage available resources—including existing risk registers at your department, along with industry emerging trends and research—to ensure your listing is comprehensive. For example, the ACFE's [Fraud Tree](#) outlines the complete classification of internal, or occupational, fraud, which you can use to identify any additional internal risks you might not have considered.
- Integrate all the identified FWA schemes into a comprehensive FWA risk map for your department.
- Periodically refresh and iterate the FWA risk map as part of your ongoing FWA risk management and FWA risk assessment activities.

The Importance of Internal Controls



The Importance of Internal Controls (1 of 4)

- ✓ Internal controls in government projects help to ensure that grant projects are effectively implemented in an efficient manner that minimizes the risk for grant fraud, waste, and abuse. Internal controls can also help ensure that government funds are used for the designated purpose, adequate documentation is maintained for grant charges, and grant objectives are accomplished.
- ✓ Departments must establish and maintain effective internal controls over there federal award, thereby providing reasonable assurance that its awards are managed in compliances with federal statutes, regulations, and terms and conditions of the award (2 CFR 200.303(a)).
- ✓ The Uniform Guidance states that non-federal entities (e.g., Colorado Departments - [PolicyInternalControl.pdf - Google Drive](#)) must have internal controls and that those internal controls should either be in compliance with GAO's Standards for Internal Control in the Federal Government, or with the Internal Control-Integrated Framework established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2 CFR 200.303).

The Importance of Internal Controls (2 of 4)

Standards for Internal Control in the Federal Government (Green Book)

- ✓ The **Federal Managers' Financial Integrity Act** (FMFIA) required the GAO to establish standards for internal controls. In response the GAO issued the Standards for Internal Controls in the Federal Government, also known as the "Green Book."
- ✓ The Green Book provides a framework for **designing, implementing, and operating** an effective internal control system. Although it establishes internal controls for federal agencies for both program and financial management, the Greenbook should be in Colorado adopted by all departments.
- ✓ The Green Book describes the relationship that exists between a department's objectives, the five components of internal control and the department's structure.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) Integrated Framework

- ✓ The (COSO) is a **joint initiative of five private sector organizations** whose mission is to provide thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.

The Importance of Internal Controls (3 of 4)

The five components of internal control, provides a comprehensive framework for establishing and maintaining effective internal controls within an organization. These components are:

1. Control Environment - The control environment sets the tone of an organization and influences the control consciousness of its employees. It includes the organizational culture, ethical values, governance structure, and the integrity of management and staff.

Key Elements:

- Leadership commitment to ethical behavior and integrity
- Organizational structure and assignment of authority and responsibility
- Human resource policies that promote a strong ethical culture

2. Risk Assessment - Risk assessment involves identifying and analyzing risks that could prevent the organization from achieving its objectives. This component ensures that risks are understood, timely responses are implemented, and a plan for mitigating those risks is established.

Key Elements:

- Identification of potential internal and external risks
- Assessment of the likelihood and impact of those risks
- Development of strategies to mitigate identified risks



© 2013. COSO. All rights reserved. Used by permission.

The Importance of Internal Controls (4 of 4)

3. Control Activities - Control activities are the specific policies and procedures that help ensure that risk responses are effectively carried out. These activities are designed to mitigate risks and ensure that management's directives are executed.

Key Elements:

- Establishing clear policies and procedures
- Implementing physical and logical access controls
- Approval processes, reconciliations, and reviews to prevent and detect errors or fraud

4. Information and Communication - Effective internal control relies on timely, relevant, and accurate information being communicated both internally and externally. This component emphasizes the importance of quality information, and the communication channels used to disseminate pertinent information.

Key Elements:

- Accurate and timely collection and dissemination of information
- Supporting communication systems and channels for employees
- Mechanisms for reporting failures in internal controls or compliance issues

5. Monitoring Activities - Monitoring activities involve ongoing and separate evaluations of the effectiveness of internal controls. This component ensures that the systems remain effective over time and that any deficiencies are identified and addressed promptly.

Key Elements:

- Regular monitoring and evaluation of control processes
- Independent audits and assessments of controls
- Continuous feedback loops for improving and adapting controls as needed

Internal Control Components and Principles (1 of 2)

Area	The Green Book	Committee of Sponsoring Organizations of the Treadway Commission (COSO)
Control Environment	1. The oversight body and management should demonstrate a commitment to integrity and ethical values.	1. Commitment to integrity and ethical values
	2. The oversight body should oversee the entity's internal control system.	2. Independent board of directors' oversight
	3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.	3. Structures, reporting lines, authorities, and responsibilities
	4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.	4. Priority to attract, develop, and retain competent people
	5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.	5. People held accountable for internal control
Risk Assessment	6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.	6. Clear objectives specified
	7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.	7. Risk identified to achievement of objectives
	8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.	8. Potential for fraud considered
	9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.	9. Significant changes identified and assessed

Internal Control Components and Principles (2 of 2)

Area	The Green Book	Committee of Sponsoring Organizations of the Treadway Commission (COSO)
Control Activities	10. Management should design control activities to achieve objectives and respond to risks.	10. Control activities selected and developed
	11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.	11. General IT controls selected and developed
	12. Management should implement control activities through policies.	12. Controls developed through policy and procedure
Information and Communication	13. Management should use quality information to achieve the entity's objectives.	13. Quality information obtained, generated, and used
	14. Management should internally communicate the necessary quality information to achieve the entity's objectives.	14. Internal control information internally communicated
	15. Management should externally communicate the necessary quality information to achieve the entity's objectives.	15. Internal information externally communicated
Monitoring Activities	16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.	16. Ongoing and separate evaluations conducted
	17. Management should remediate identified internal control deficiencies on a timely basis.	17. Internal control deficiencies evaluated and communicated

Source: Grants Management Body of Knowledge (GMBOK) Guide

The Grants Management Lifecycle and Internal Controls (1 of 4)

Pre-award Phase:

- ✓ In preparation for potentially receiving a federal award, your department has the opportunity to examine its departments operations, determine whether control activities align with the departments mission, goals, and objectives, and test existing controls' effectiveness and efficiency.
- ✓ It is a good practice for your department to ensure, before receiving an award, that management personnel and staff responsible for the award are trained in the applicable, federal and state laws, regulations, and specific terms and conditions.

Award Phase:

- ✓ When your department receives a federal award, it should share the award notice with its administrative, finance and program divisions.
- ✓ Each of these divisions will have responsibility for unique components in the award announcement. Providing them with timely notice will help them identify whether additional control activities are needed to satisfy the award terms and conditions.

Post-Award Phase:

- ✓ At the post-award stage of the grants management lifecycle, a department's internal controls are tested.
- ✓ Specific control activities, once established, should be reviewed and evaluated to verify compliance can be maintained.

The Grants Management Lifecycle and Internal Controls (2 of 4)

Monitoring Phase:

- ✓ When a department is both a recipient and a pass-through entity, its burden of responsibility regarding internal controls increases.
- ✓ In addition to ensuring that its own internal control systems and activities are maintained and monitored, it must also verify that the efficiency and effectiveness of its subrecipient's internal controls. The pass-through entity will evaluate and monitor subrecipients for compliance with applicable laws and, regulations, and terms and conditions of the federal award.

Closeout Phase:

- ✓ During the closeout phase, the department will further test the reliability of its reporting for internal and external use at both its operational and functional levels.
- ✓ The department ensures that final grant reports are accurate and reflect the departments efforts to meet the federal award requirements.

The Grants Management Lifecycle and Internal Controls (3 of 4)

Examples of enterprise controls that will help prevent common mismanagement are as follows:

Adequate Monitoring:

- ✓ Grant recipients should monitor the grant work on a regular basis, as this will help prevent mismanagement.
- ✓ Discrepancies discovered as a result of monitoring activities should be examined in a timely manner and any mismanagement concerns should be resolved quickly.
- ✓ Grant recipients must maintain documentation of expenses incurred and documented proof of site visits of contractors and sub-grant recipients.

Formal Organizational Documents:

- ✓ The structure of the organization should be explicitly documented.
- ✓ Qualifications for members of Boards of Directors should be formally approved to help ensure qualified individuals provide direction for the organization. Board members should not include employees of the organization to avoid the appearance of conflicts of interest.
- ✓ Audit committees should report to the Board of Directors to ensure audit findings and potential fraud are adequately reported and that the Board has the opportunity to hold organization officials accountable.
- ✓ Audit Committees should not report directly to the president or equivalent officer that may be held accountable for any mismanagement, but the appropriate management officials should be provided a copy of the audit findings and an opportunity to respond to help ensure all the facts are presented to the Board.

The Grants Management Lifecycle and Internal Controls (4 of 4)

Formal Organizational Documents (continued):

- ✓ Board meetings should be memorialized in meeting minutes that identify key decisions to help ensure organization officials can easily refer to decision items and requirements, and provide some continuity for future administering officials.
- ✓ In addition, grant recipients should maintain an updated organizational chart establishing clear lines of responsibility and authority to help ensure efficient operations.

Formal Written Policies:

- ✓ Formal written policies setting forth procedures help ensure operational effectiveness and efficiency by providing written guidance to which grant recipients and other officials can refer. The policies should be adequately written to ensure officials have clear and relevant guidance for the completion of duties and responsibilities.
- ✓ Written policies enable grant administrators to provide appropriate oversight over the life of a grant, and help ensure effective continuity of operations in case of personnel turnover.

✓

Reconciliations:

- ✓ Grant recipients should perform reconciliations in order to ensure grant activity is accurately recorded and reported and to help prevent and detect fraud. At a minimum, periodic and frequent reconciliations should be performed for bank statements, accounting records, checks for payment, credit card statements, grant drawdowns, Federal Financial Reports submitted to federal agencies, and other grant-related administrative and programmatic activity.
- ✓ The grant recipient organization should separate reconciliation duties in order to ensure the opportunity for fraud is reduced. For example, individuals responsible for authorizing checks for payment should not perform bank statement reconciliations.

Lunch



How to Conduct Your FWA Risk Assessment



Does your department currently conduct a fraud risk assessment for each federal grant program?

Yes

No

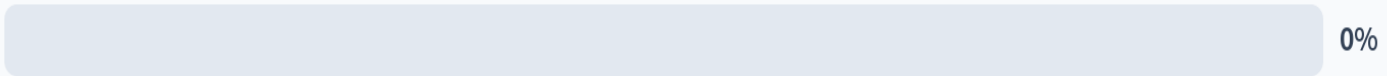
Unsure

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

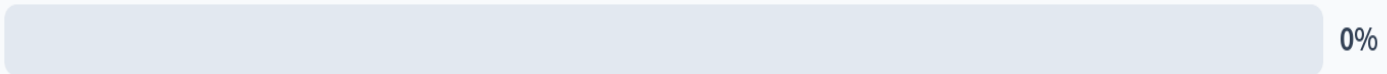


Does your department currently conduct a fraud risk assessment for each federal grant program?

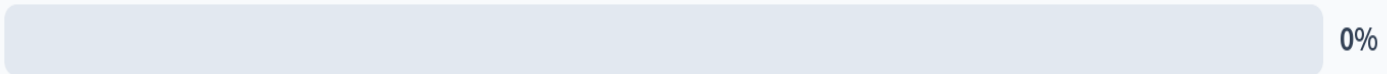
Yes



No



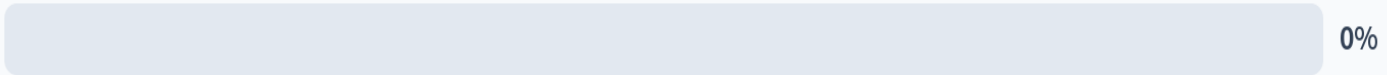
Unsure



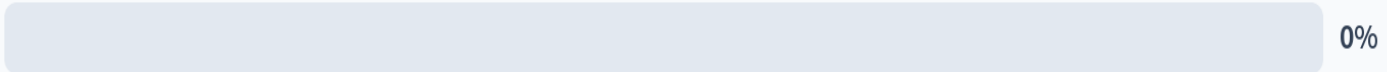
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Does your department currently conduct a fraud risk assessment for each federal grant program?

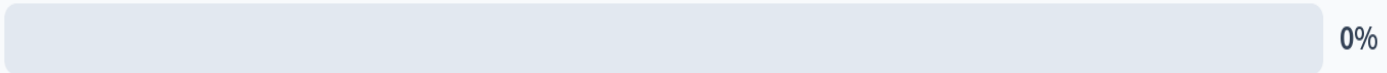
Yes



No



Unsure



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

If your department does currently conduct a fraud risk assessment for each federal program, how often is the assessment conducted?

Quarterly

Semi-annually

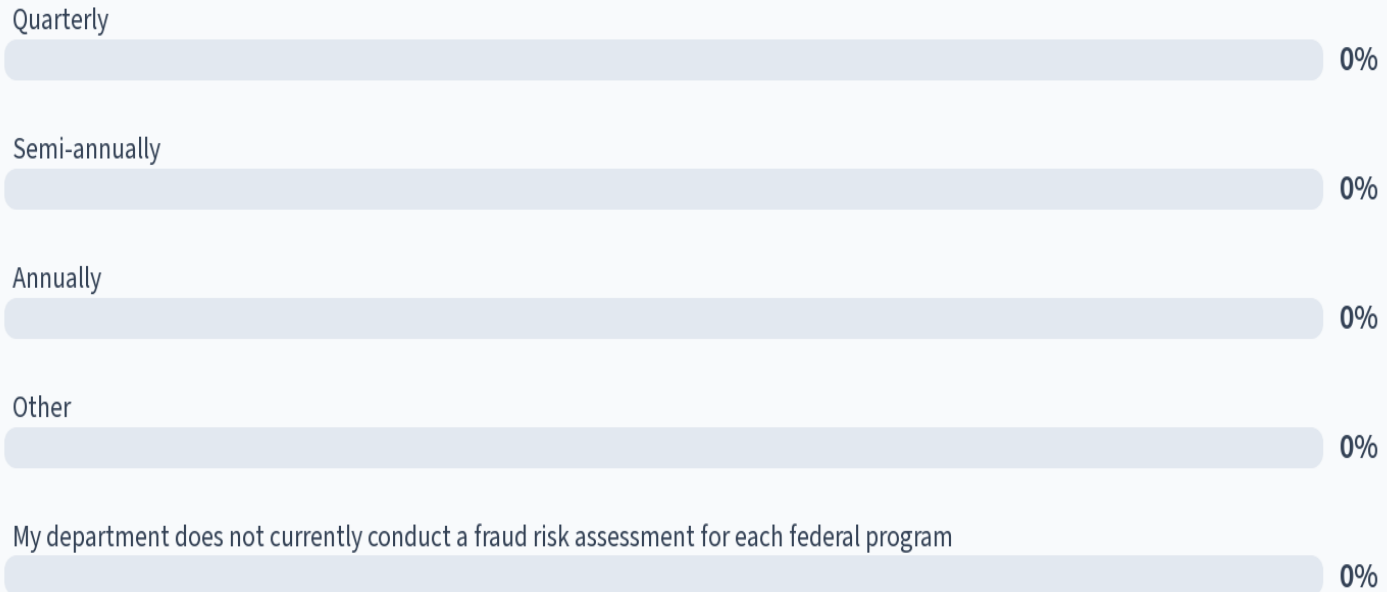
Annually

Other

My department does not currently conduct a fraud risk assessment for each feder...

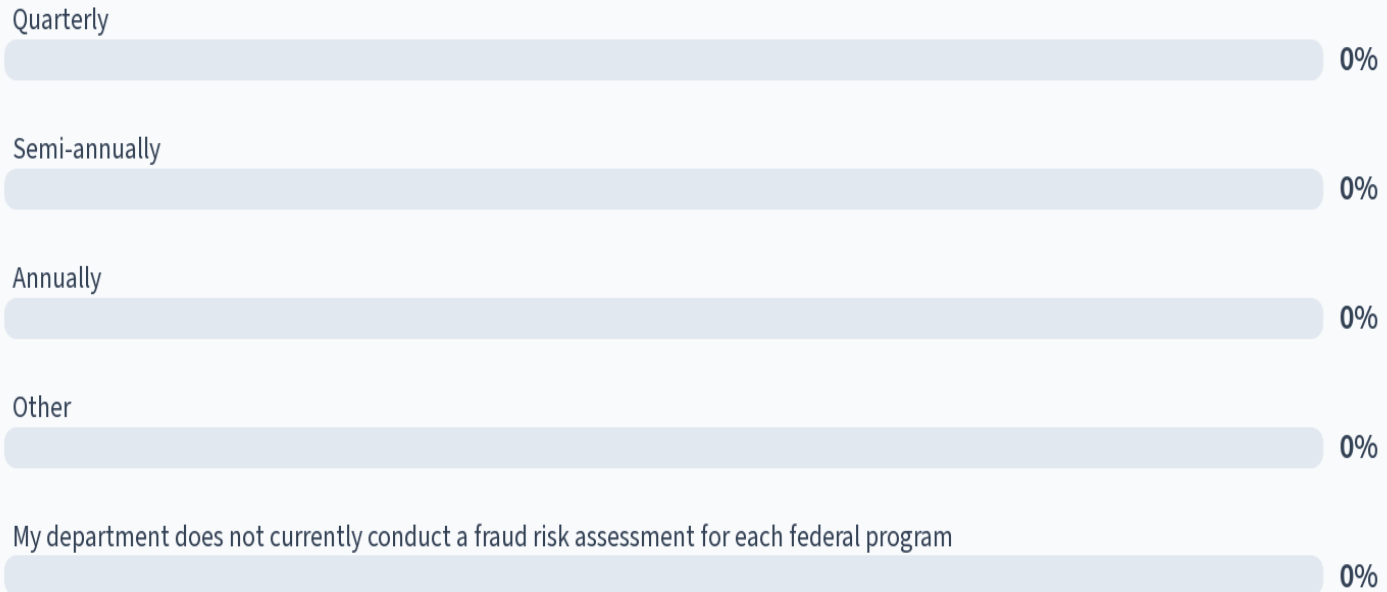
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

If your department does currently conduct a fraud risk assessment for each federal program, how often is the assessment conducted?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

If your department does currently conduct a fraud risk assessment for each federal program, how often is the assessment conducted?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

How to Conduct Your Fraud Risk Assessment

Conducting a FWA risk assessment helps you understand exactly where your processes might be vulnerable to FWA and allows for a holistic and detailed look at the FWA risks across the department. Every department faces a variety of risks from both internal and external sources, and a FWA risk assessment is a tool that your department can leverage to identify and understand risks and provide the basis for how risks will be managed by your department. Further, the FWA risk assessment process is a proactive measure that can increase the perception of detection.

Therefore, the process should be visible throughout your department, which means you should communicate broadly, promoting the process at all levels of the department. It is important to remember that a FWA risk assessment is an art and not a science, so your FWA risk assessment methodology or approach should be tailored to the unique vulnerabilities and strategic goals of your department and program or project.

Steps to Conduct the FWA Risk Assessment:



Establish the FWA risk assessment team - Establish the FWA risk assessment team, including clearly defining the members' roles and responsibilities and ensuring that the appropriate levels of management are involved.



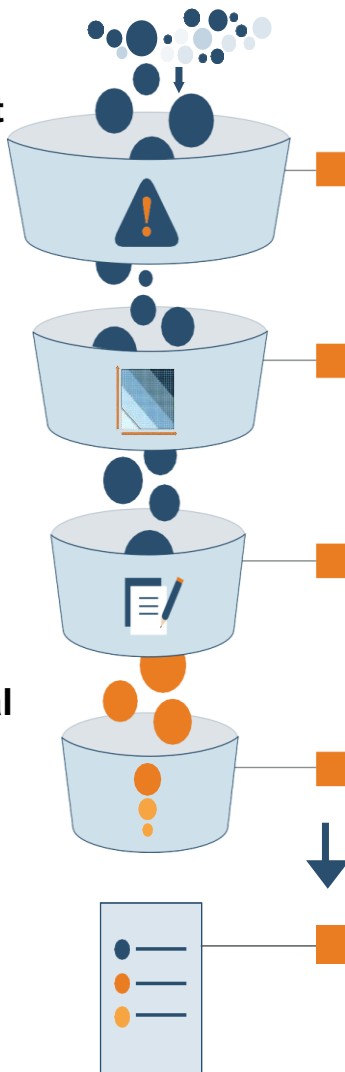
Determine your starting point - You can either implement a department wide FWA risk assessment or a targeted FWA risk assessment by project. It might be beneficial to forgo a department wide assessment and instead conduct a pilot in a particular project. This approach will allow you to test your methodology and implement lessons learned as you expand your assessment across other areas of the department.



Conducting Your Fraud Risk Assessment

Universe of Potential Fraud Risks

Inherent Fraud Risks



Identify inherent fraud risks affecting the program:

Department determine where fraud can occur and the types of fraud the program faces, such as fraud related to financial reporting, misappropriation of assets, or corruption. Managers may consider factors that are specific to fraud risks, including incentives, opportunity, and rationalization to commit fraud

Assess the likelihood and impact of inherent fraud risks:

Departments conduct quantitative or qualitative assessments, or both, of the likelihood and impact of inherent risks, including the impact of fraud risks on the program's finances, reputation, and compliance. The specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors

Determine fraud risk tolerance:

According to *Standards for Internal Control in the Federal Government* risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks, and it may vary depending on the circumstances of the program

Examine the suitability of existing fraud controls and prioritize residual fraud risks:

Department considers the extent to which existing control activities mitigate the likelihood and impact of inherent risks. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. Managers then rank residual fraud risks in order of priority, using the likelihood and impact analysis, as well as risk tolerance, to inform prioritization

Document the program's fraud risk profile:

Effectively assessing fraud risks involves documenting the key findings and conclusions from the actions above, including the analysis of the types of fraud risks, their perceived likelihood and impact, risk tolerance, and the prioritization of risks

Source: GAO. | GAO-15-593SP

Conducting Your Fraud Risk Assessment (1 of 2)

The following table outlines several key questions and a checklist, intended to help your department conduct a comprehensive FWA risk assessment, in line with the Guide's leading practices and guidance.

Points of focus

- Involves appropriate levels of management
- Estimates the likelihood and significance of risks identified
- Identifies existing FWA control activities and assesses their effectiveness
- Determines how to respond to risks
- Uses data analytics techniques for FWA risk assessment and FWA risk responses
- Performs periodic reassessments and assesses changes to fraud risk
- Documents the risk assessment

Key questions

- Who will be on your FWA risk assessment team? What are their roles and responsibilities?
- Where do you want to start your FWA risk assessment?
- Does your department leverage a likelihood and impact scale for other risk assessment efforts that you can leverage for assessing FWA risk? If not, how do you plan to develop those scales?
- How will you educate stakeholders on the FWA risk assessment process to ensure understanding of key terms and procedures?
- How will you document and evaluate existing FWA controls throughout the assessment process?
- What factors should you consider when prioritizing FWA risks? Will this be based solely on likelihood and impact scores, or will other information be considered?
- How will you respond to high-priority risks identified? How can you leverage your roadmap and strategy to inform this process?
- How often will you perform a FWA risk assessment? What changes will initiate a reassessment?

Conducting Your Fraud Risk Assessment (2 of 2)

Note: The ACFE has developed [Risk Assessment and Follow-Up Action Templates](#) that you can leverage throughout the FWA risk assessment process. This spreadsheet provides a risk assessment matrix for you to document your department's FWA risks and controls. The template automatically creates a heat map showing the significance and likelihood of each identified FWA exposure, a FWA risk ranking page displaying each FWA risk exposure from most to least severe, and a control-activities matrix showing the identification and evaluation of existing control activities related to each FWA risk exposure. It also provides space to identify additional control activities and to record the department's response plan for each exposure.

Conducting Your Fraud Risk Assessment Checklist (1 of 2)

- Establish the FWA risk assessment team, including clearly defining the members' roles and responsibilities and ensuring that the appropriate levels of management are involved. This should be informed by the established FWARM governance structure and roles and responsibilities.
- Determine your starting place. You can either implement a department wide FWA risk assessment or a targeted FWA risk assessment. It might be beneficial to forgo a department -wide assessment and instead conduct a pilot in a particular area to start small. This approach will allow you to test your methodology and implement lessons learned as you expand your assessment across other areas of the department . Either way, ensure that your starting place aligns to the roadmap and strategy you developed in.
- Identify all FWA schemes.
- Estimate the likelihood and impact of each FWA scheme. If your department already has likelihood and impact scales developed for other risk management efforts, you might be able to leverage those here for consistency and to ensure that the FWA risk assessment results can roll up across your department. You might also want to assess FWA risks on an inherent and residual basis. If you choose to do this, the key to this being effective is stakeholder communication to ensure understanding of these terms. Without that understanding, the results will not be insightful.

Conducting Your Fraud Risk Assessment Checklist (2 of 2)

- Identify existing FWA controls and their effectiveness. Departments usually have existing controls in place that serve as preventive or detective FWA control activities. As part of the FWA risk assessment process, the risk assessment team examines each specific FWA scheme or risk and identifies the existing related control activities. In some cases, there might be several existing controls. In other cases, the risk assessment team might conclude that no controls exist. After identifying existing control activities, the risk assessment team evaluates how effective these existing FWA control activities are in terms of mitigating FWA risk.
- Prioritize FWA schemes. Prioritizing risks will help you determine how to apply resources to effectively respond to the most important risks. In scoring and prioritizing risks, the risk assessment team should use the likelihood and impact assessments, as well as the presence and effectiveness of related control activities. For example, if a FWA risk lacks effective controls, it would be scored as a higher priority or a more significant risk than one with multiple effective controls in place.
- Assess and respond to high priority or significant FWA schemes. You may choose to strengthen existing control activities, add control activities, or consider using data analytics to combat high-priority or significant risks identified. Either way, the chosen response should align with your organization's FWA risk tolerance and the roadmap and strategy.
- Document the risk assessment. This can be done in a number of ways, but key items to document include the methodology deployed, the assessment results, and the organization's response strategies.
- Reassess periodically, considering changes external to the organization, operational changes, and leadership changes.

Conducting an Investigation



Does your department currently have a dedicated group or team that handles investigations?

0

Yes

No

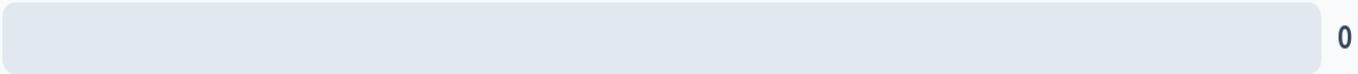
Somewhat

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

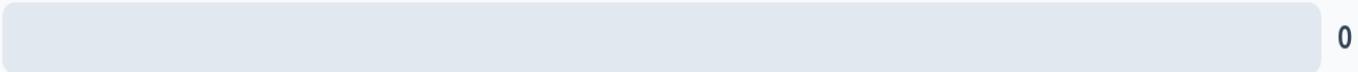
Does your department currently have a dedicated group or team that handles investigations?

0

Yes



No



Somewhat

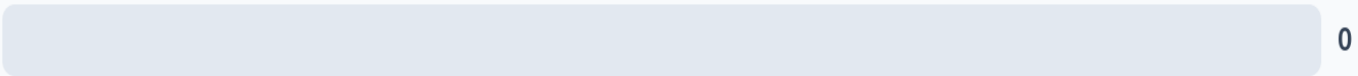


Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Does your department currently have a dedicated group or team that handles investigations?

0

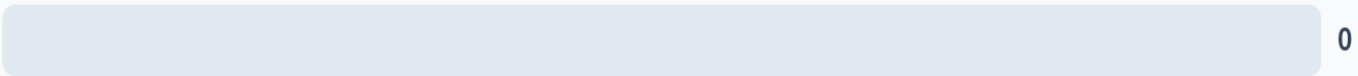
Yes



No



Somewhat



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Conducting a Successful Investigation (1 of 3)

You've received allegations of fraud. What's next?

Investigations are a critical component of uncovering not only fraud within your organization, but also a range of associated other corporate crimes, such as money laundering, corruption, and bribery. Investigations also act as an effective fraud deterrence practice, showcasing the organization's commitment to high ethical standards and creating the perception of detection.

All investigations should be conducted with integrity and objectivity. The following are typical components and factors to consider as part of conducting investigations.

Investigations will typically include the following components:

- Evidence gathering
- Computer forensics
- Develop and test hypotheses
- Gather external records
- Witness interviewing
- Perform data analysis

The investigation will involve different steps depending on the kind of allegation, but below are some general factors to consider:

- Time sensitivity
- Confidentiality
- Legal privileges
- Objectivity

Minnesota Lacked Fraud Evidence vs Feeding Our Future Before FBI Got Involved

FEEDING OUR FUTURE

We utilize the Child and Adult Care Food Program to increase healthy food access for Minnesota's youth and seniors.

5:00 NEWS

5:00 69°



COLORADO

Office of the State Controller

Department of Personnel & Administration

Conducting A Successful Investigation (2 of 3)

Conducting Investigations Includes:

- Communicating investigation results
- Taking corrective action
- Evaluating investigation performance

Key Questions:

The following key questions focus on the elements and considerations in developing an effective investigative work plan:

- Do you have a documented investigative work plan to guide each investigation?
- How will you ensure that investigations are conducted independently without influence?
- How might the work plan change from investigation to investigation?
- How might the work plan expand or contract based on facts discovered during the investigation?

Conducting A Successful Investigation (3 of 3)

Key Questions (continued):

- How does your organization assess the scope, severity, credibility, and implications of potential fraud? Is this clear in the work plan?
- How does your organization determine discipline, remediation, asset recovery, or other activities to address the findings of an investigation? Is this clear in the work plan?
- Does the investigation team have access to subject-matter experts if needed, including forensic accountants and experts in fields such as computer forensics?
- What actions are taken upon the completion of an investigation, such as disciplinary action, training, and civil action? How is the appropriate action determined?

Your Investigation Checklist

The following checklist outlines high-level steps needed to conduct an investigation. However, this process should align with and be guided by your established investigation and response protocols. Planning is essential to an effective investigation; as such, the foundation of your investigation is rooted in your investigative work plan.

- Develop the investigation work plan:** Your investigative work plan should define and assign each investigative task to the appropriate team member. The plan should prioritize tasks and should be iterative as the investigation is carried out based on facts uncovered.

- Implement the investigative work plan:** As the work plan is implemented, consider changes based on the unique circumstances of the investigation. During this stage, the investigative team will gather evidence, perform analysis, conduct interviews, etc. The team will need to document and track information related to steps taken and information collected.

If allegations are substantiated or appear as if they are likely to have occurred, the investigative team will need to evaluate the root cause.

Following the investigation, several steps should be implemented to close the loop:

- Communicate the results, leveraging established communication channels and procedures.
- Take corrective actions and monitor implementation, leveraging established monitoring mechanisms to ensure effective implementation of corrective action following a fraud investigation.
- Evaluate investigation performance, leveraging established mechanisms for performance evaluation to solicit objective feedback.

Pulling it All Together - Documenting Your Fraud, Waste and Abuse Policy



Does your agency have documented policies on fraud, waste, and abuse in place?

Yes

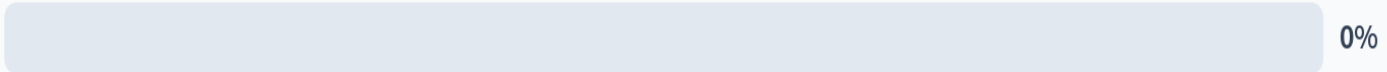
No

Not sure

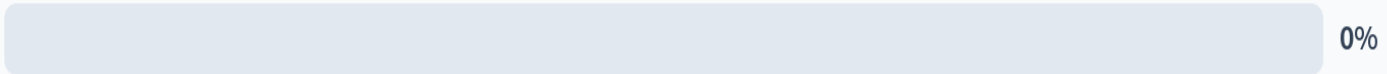
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Does your agency have documented policies on fraud, waste, and abuse in place?

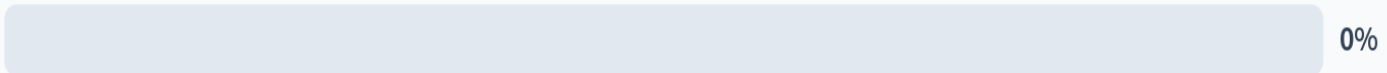
Yes



No



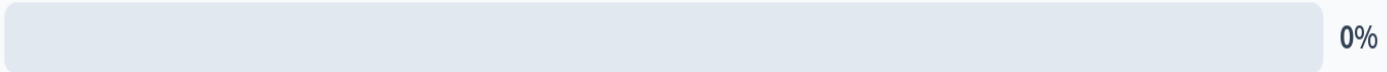
Not sure



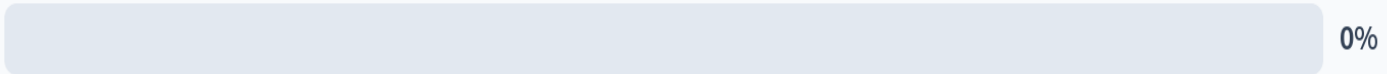
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Does your agency have documented policies on fraud, waste, and abuse in place?

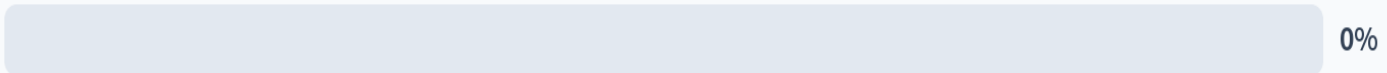
Yes



No



Not sure



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Key Elements of a FWA Policy (1 of 2)

A comprehensive fraud policy for a government department is essential to prevent, detect, and respond to fraud, waste, and abuse. Here are the key elements that should be included in such a policy, along with what each section should address:

Policy Statement: Clearly articulate the department's commitment to preventing and addressing fraud, waste, and abuse. Specify who the policy applies to, including employees, contractors, and any third parties involved in departmental operations.

Definitions: Provide a clear definition of fraud, including examples (e.g., misrepresentation, falsification of records); Waste, define waste and how it differs from fraud, focusing on inefficient or careless use of resources; and abuse explain what constitutes abuse, including misuse of authority or resources for personal gain.

Objectives of the Policy: Outline the goals of the policy in preventing fraud and promoting ethical behavior. Describe the mechanisms in place to identify potential FWA. Explain how the department will respond to incidents of fraud, including investigation and disciplinary measures.

Roles and Responsibilities: Define the roles of management in fostering a culture of integrity and accountability. Outline the expectations for employees regarding reporting suspected fraud and adhering to ethical standards. Identify the designated individual or team responsible for overseeing the implementation of the fraud policy and managing investigations.

Key Elements of a FWA Policy (2 of 2)

Reporting Mechanisms: Establish procedures for employees and the public to report suspected fraud anonymously (e.g., hotlines, online reporting systems). Include assurances that individuals who report fraud in good faith will be protected from retaliation.

Investigation Procedures: Describe the process for conducting an initial assessment of reported fraud allegations. Outline the steps for a thorough investigation, including timelines, documentation, and the involvement of relevant stakeholders (e.g., legal, HR). Emphasize the importance of maintaining confidentiality throughout the investigation process.

Consequences of Fraud: Clearly state the potential disciplinary actions for individuals found to have committed fraud, waste, or abuse, including termination and legal action. Address the department's right to recover any losses incurred due to fraudulent activities.

Training and Awareness: Outline the training programs that will be provided to employees regarding fraud prevention, detection, and reporting. Describe initiatives to keep fraud awareness at the forefront of the department's culture.

Monitoring and Review: Explain how the department will monitor operations and transactions to detect potential fraud. Establish a schedule for reviewing and updating the fraud policy to ensure its effectiveness and relevance.

Collaboration with Law Enforcement: Describe how the department will collaborate with law enforcement agencies and other relevant organizations in cases of fraud. Outline any legal obligations to report certain types of fraud to law enforcement.

Sample Fraud Policy

A comprehensive fraud policy for a government department that includes the following:

- ✓ Policy Statement
- ✓ Definitions
- ✓ Program Objectives
- ✓ Reporting Mechanisms
- ✓ Investigation Procedures
- ✓ Consequences of Fraud
- ✓ Training and Awareness
- ✓ Monitoring and Review
- ✓ Collaboration with Other Departments



American Rescue Plan Act (ARPA) State and Local Fiscal Recovery Fund (SLFRF) & Section 9817 Fraud, Waste, and Abuse Guidance Document	
Background	2
Purpose	2
Resources	2
Definitions	2
Guidance Document	3
Fraud Guidance	3
Fraud Guidance for ARPA HCBS Grantees	4
Investigating and Reporting Instances of Suspected Fraud by ARPA HCBS Grantees	4
Remediation of Suspected Fraud by ARPA HCBS Grantees	4
Fraud Guidance for SLFRF Subrecipients	4
Investigating and Reporting Instances of Suspected Fraud by SLFRF Subrecipients	5
Remediation of Suspected Fraud by SLFRF Subrecipients	5
Fraud Guidance for HCPF Employees Working with ARPA HCBS and SLFRF Funded Activities	6
Investigating and Reporting Instances of Suspected Fraud by HCPF Employees Working on ARPA HCBS and SLFRF Funded Activities	6
Remediation of Suspected Fraud by Employees Working on ARPA HCBS and SLFRF Funded Activities	6
Waste and Abuse Guidance	7
Waste and Abuse Policy for ARPA HCBS Grantees	7
Investigating and Reporting Waste and Abuse by ARPA HCBS Grantees	7
Remediation of Waste and Abuse by ARPA HCBS Grantees	7
Waste and Abuse Guidance for SLFRF Subrecipients	7
Investigating and Reporting Waste and Abuse by SLFRF Subrecipients	8
Remediation of Waste and Abuse by SLFRF Subrecipients	8
Waste and Abuse Guidance for HCPF Employees Working on ARPA HCBS and SLFRF Funded Activities	8
Investigating and Reporting Waste and Abuse by HCPF Employees Working on ARPA HCBS and SLFRF Funded Activities	8
Remediation of Waste and Abuse by HCPF Employees Working on ARPA HCBS and SLFRF Funded Activities	8
Administration of Guidance	9
Change Log	9

Source: HCPF

What role does employee training play in preventing fraud?

It is unnecessary and time-consuming

It helps employees understand and detect fraud

It only applies to new hires

It has no impact on fraud prevention

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What role does employee training play in preventing fraud?

It is unnecessary and time-consuming

0%

It helps employees understand and detect fraud

0%

It only applies to new hires

0%

It has no impact on fraud prevention

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What role does employee training play in preventing fraud?

It is unnecessary and time-consuming

0%

It helps employees understand and detect fraud

0%

It only applies to new hires

0%

It has no impact on fraud prevention

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What kind of training would you find most useful in helping you better recognize and prevent fraud in your role?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following is NOT an effective tool for fraud prevention?

Regular financial audits

Strong employee training programs

Weak financial controls

A clear whistleblower policy

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following is NOT an effective tool for fraud prevention?

Regular financial audits

0%

Strong employee training programs

0%

Weak financial controls

0%

A clear whistleblower policy

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which of the following is NOT an effective tool for fraud prevention?

Regular financial audits

0%

Strong employee training programs

0%

Weak financial controls

0%

A clear whistleblower policy

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What are your main concerns about fraud, waste, or abuse in your workplace?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Day 2

What was your main takeaway from Day 1?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

If you suspect fraud, what should you do first?

Confront the person directly

Report it to a supervisor or through a fraud hotline

Keep it to yourself

Announce it to all employees

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

If you suspect fraud, what should you do first?

Confront the person directly

0%

Report it to a supervisor or through a fraud hotline

0%

Keep it to yourself

0%

Announce it to all employees

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

If you suspect fraud, what should you do first?

Confront the person directly

0%

Report it to a supervisor or through a fraud hotline

0%

Keep it to yourself

0%

Announce it to all employees

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Have you ever reported a suspicious activity at work? If so, what was your experience like?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What additional resources or support do you need to feel more confident in identifying fraud, waste, or abuse?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What should an organization do after identifying a fraud incident?

Ignore it if it's small

Conduct an investigation and take appropriate action

Immediately terminate all employees involved

Publicize it broadly within the company

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What should an organization do after identifying a fraud incident?

Ignore it if it's small

0%

Conduct an investigation and take appropriate action

0%

Immediately terminate all employees involved

0%

Publicize it broadly within the company

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What should an organization do after identifying a fraud incident?

Ignore it if it's small

0%

Conduct an investigation and take appropriate action

0%

Immediately terminate all employees involved

0%

Publicize it broadly within the company

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What questions do you still have about fraud, waste, and abuse?

Nobody has responded yet.

Hang tight! Responses are coming in.

Riskier Federal Grant Projects That May Be Vulnerable to Fraud

Case Studies



Riskier Federal Grant Projects that may be Vulnerable to Fraud (1 of 2)

Riskier federal grant projects that may be vulnerable to fraud and mitigating controls:

Large Infrastructure Projects: Major construction or infrastructure projects often involve significant sums of money, making them targets for fraud through bid rigging or kickbacks.

Grants to Nonprofits: Funding distributed to nonprofit organizations can be vulnerable if there is insufficient due diligence in the selection process or lack of follow-up audits.

Emergency Relief Programs: Programs aimed at providing quick financial assistance can be exploited if the verification of eligibility is not rigorous.

Procurement of Goods and Services: Projects involving procurement can be susceptible to fraud, especially if there are inadequate checks in place for vendor selection and invoicing practices.

Community Development Projects: Initiatives that involve community engagement might not have stringent oversight, making it easier for funds to be mismanaged or misused.

Riskier Federal Grant Projects that may be Vulnerable to Fraud (2 of 2)

Subrecipient Agreements: When funds are passed down to subrecipients, the risk of mismanagement or noncompliance increases, particularly if there are unclear guidelines and lack of monitoring.

Technology Ventures: Projects that involve new technologies or software development might lack transparency, leading to opportunities for fraud during the procurement and implementation phases.

Public-Private Partnerships: In contracts involving private entities, there can be potential for conflicts of interest or misallocation of funds if not properly monitored.

Case Study - Fictitious Vendor Scheme (1 of 2)

Scenario: A department head is concerned that someone has stolen money by creating fictitious vendors and invoices and is directing payments to their or a related party's bank account.

What should the department head document?

- Who created the new vendor profile?
- Is the creation of new accounts one of that person's duties or does that person have access that is irrelevant to their job?
- Is the vendor listing regularly reviewed to ensure that active vendor accounts are valid?
- Can you tell which employee created the new account?

What Preventative Controls should be in place?

- **Background Checks:** Ensure a valid Taxpayer ID # and W-9 on file and having someone verify that the vendor's website and phone number are current and active.
- **Cross Reference Vendor Information:** Cross-reference vendor information with third-party databases to confirm legitimacy.
- **Three-way Match:** Implement a three-way match process that compares the purchase order, receiving report and invoice before payment is approved.
- **Management Review and Approval:** Require management review and approval for high value invoices from new vendors.
- **Monitor Change Logs:** To help prevent unauthorized changes to Vendor information, utilize change logs to monitor and keep an audit trail of modifications to sensitive vendor information from either the Administration change logs views or view changes right from the vendor record view.

Case Study - Fictitious Vendor Scheme (2 of 2)

- **Segregation of Duties:** The core principle of the segregation of duties is that no one person should be able to abuse the system on their own. For example, the person receiving cash should not be the same person who is responsible for recording how much was received, depositing those funds, or reconciling the bank account.
- **IT passwords and access controls:** Ideally, organizations should employ the principle of least privilege, which means that users should only have the level of access required to do their required tasks and no more than that.
- **Physical controls over assets:** Similar to IT access controls, individuals in an organization should only have access to physical parts of the organization (such as machine rooms) if this is required for their job.

What detective controls should be in place?

- **Review of Payment Patterns:** Regularly review payment patterns for vendors, looking for signs of irregularities, such as payments made shortly after vendor creation.
- **Data Analytics and Monitoring:** Use data analytic tools to monitor vendor transactions for unusual patterns, such as high frequency invoices from a single vendor or round-number amounts.
- **Vendor Bank Accounts to Employee Bank Accounts:** Use analytics to compare employee and vendor bank account information.
- **Review of Vendor Lists:** conduct periodic reviews of the vendor master list and look for duplicate vendors, vendors with incomplete information.

Case Study – Applicants Applying for Benefits Using False Identities (1 of 2)

Scenario: A department head is concerned that applicants are applying for benefits using false identities.

Initial Question: What should the department head document?

- What conditions or actions are most likely to cause or increase the chances of the fraud risk occurring?
- Which group or individual within the program is responsible for addressing the risk?
- What controls does the program already have in place to reduce the likelihood and impact of the inherent fraud risk?

Case Study – Applicants Applying for Benefits Using False Identities (2 of 2)

What Preventative Controls should be in place?

- **Robust Identity Verification Procedures:** Implement strict identity verification processes that require applicants to provide multiple forms of identification (e.g., government-issued ID, Social Security number, birth certificate) and use technology to authenticate documents and verify identities against official databases.
- **Data Matching with Government Databases:** Cross-reference applicant information with government databases (e.g., Social Security Administration, Department of Motor Vehicles) to verify identity and eligibility. Automated checks can quickly identify discrepancies and flag suspicious applications.
- **Application Limits and Monitoring:** Implement limits on the number of applications that can be submitted from a single IP address or device within a specific timeframe. This helps to prevent mass applications that may indicate fraudulent activity.

What detective controls should be in place?

- **Fraud Detection Algorithms:** Utilize data analytics and machine learning algorithms to identify patterns indicative of fraudulent applications (e.g., multiple applications from the same IP address or similar names). Regularly update algorithms to adapt to emerging fraud trends.
- **Link Analysis:** Link analysis can be used to identify and prevent fraud by helping you find accounts connected by suspicious shared details, find accounts connected to known fraudsters, and find suspicious activity between accounts that may initially seem unrelated.

Using Data Analytics to Prevent, and Detect Fraud, Waste and Abuse

Case Study – Applicant Programs



Data Analytics Fundamentals to Prevent and Detect Fraud, Waste and Abuse

- **The use of data analytics** is a powerful FWA prevention, detection, and investigation tool, making it an important part of an effective and holistic FWARM program.
- Many anti-fraud analytics tests can be easily implemented using basic spreadsheet software, while the most advanced departments are leveraging robotics, machine learning, and artificial intelligence to enhance their anti-fraud analytics programs.
- When in doubt, start small with a pilot approach to reduce initial investment and gain quick wins for your department's FWARM program.
- **Whether basic or complex, data analysis of some sort is critical for elevating your department's FWA detection and prevention efforts.**



Using Data Analytics to Prevent and Detect Fraud, Waste, and Abuse (1 of 2)

There are a lot of analytic techniques out there, and each one brings with it unique benefits and insights. However, **not all analytic techniques are equal** – certain techniques are better suited for certain objectives or analyses than others.

At a high level, there are five different analytic techniques ranging from simple to more advanced. This is not a comprehensive listing; there are many options out there and what you choose depends on your department's priorities.

Data Analytic Techniques

Rule-based analytics



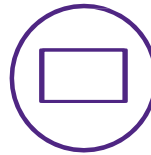
Known patterns

Anomaly detection analytics



Unknown patterns

Network / link analytics



Complex patterns

Network / link analytics



Linked patterns

Text analytics



Text patterns



Using Data Analytics to Prevent and Detect Fraud, Waste and Abuse (2 of 2)

The following table outlines key questions and a checklist, intended to help your department implement data analytics to combat FWA, in line with leading practices and guidance.

Key Questions

- Who will be responsible for your anti-fraud analytics program?
- How can your FRM strategy help you decide what priority level of fraud schemes you will target with analytics?
- What data is available related to your selected fraud schemes? Who are the relevant stakeholders you will need to work with to access and collect this data? Will you need to integrate data from multiple sources?
- What analytics techniques and tests will you implement? What resources and level of investment will be required?
- What type of reporting will be required? What stakeholders will you report results to, and how often will reporting occur?
- How will findings be remediated and corrected? How will you integrate this process with the fraud risk assessment?

Note: The ACFE developed an [Anti- Fraud Data Analytics Tests interactive tool](#), which provides numerous data analytics tests that can be used to help identify the red flags of various occupational fraud schemes. This tool is based on the structure of the [ACFE's Fraud Tree](#). You can drill down to a specific scheme type and see data analytics tests that are relevant to that fraud risk



Checklist (1 of 2)

The following checklist provides a framework for implementing an anti-fraud analytics program. It is important to take an iterative approach to analytics, so you can ensure that tests are designed and validated carefully. Further, the implementation of analytics should align with your overall FRM roadmap and strategy. You will also need to determine who will be responsible for your anti-fraud analytics program, which should be informed by the established FRM governance structure and roles and responsibilities.

- Design Your Analytics:** Map the prioritized fraud schemes identified through your fraud risk assessment to potential data sources and assess availability of relevant data. Once data is identified and availability is confirmed, determine the analytic techniques and tests you wish to implement.
- Collect the Data:** Work with relevant stakeholders across your organization to collect data. As part of this process, you will need to extract, transform/normalize, and validate the data to ensure that it will provide meaningful results when analyzed (i.e., to avoid “garbage in, garbage out”).
- Execute Your Analytics Techniques and Tests:** As execution proceeds, iterate and modify based on the data received, data quality, user feedback, and test results. This process will be ongoing and will require refining your models as needed to ensure the effectiveness of the techniques and the accuracy and relevance of the results.

Checklist (2 of 2)

- **Report Your Findings and Observations to Relevant Stakeholders:** Reporting should be in line with the established FRM governance structure. For example, if a potential fraud event is uncovered, then it should be referred to your organization's investigative body as outlined in your fraud risk policy. However, reporting should not stop there. You should report on key outcomes to other relevant stakeholders to ensure your findings and observations inform the FRM program and lead to lessons-learned that can be incorporated to strengthen current controls and mitigating activities. For example, if your intended audience is senior leadership, then presenting your findings and recommendations in a visual manner and focusing on the most important items needed for decision-making may be best. However, if you are presenting to business unit stakeholders, then tailor the results to highlight the items that affect their day-to-day work or items that they have ownership of so that they are aware of their risks and can begin work on mitigating them.

- **Implement Remediation and Corrective Action Activities:** Based on the response strategies identified through your fraud risk assessment and the established FRM governance structure, implement remediation and corrective actions. For example, if your results indicate that one type of fraud is a significant concern, then that information should feed back into your fraud risk assessment results to inform the response strategy and risk prioritization. Remember, all remediation and corrective action should also align to your overall FRM strategy and your long-term goals and vision of your FRM program.

Which tool is commonly used to detect anomalies in financial data?

Data Visualization Software

Anti-Virus Software

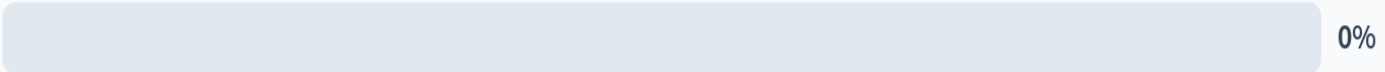
Time Management Software

Employee Scheduling Tools

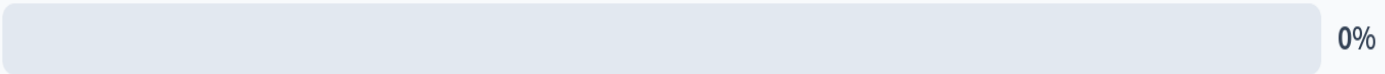
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which tool is commonly used to detect anomalies in financial data?

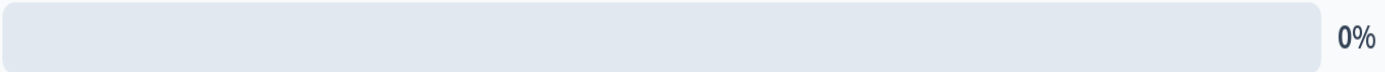
Data Visualization Software



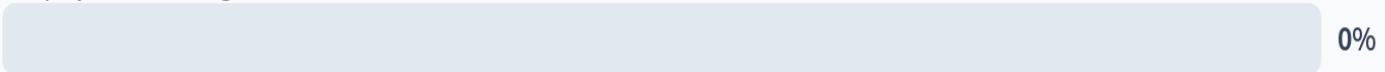
Anti-Virus Software



Time Management Software



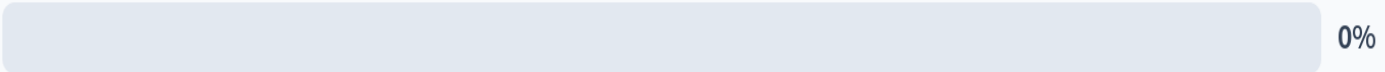
Employee Scheduling Tools



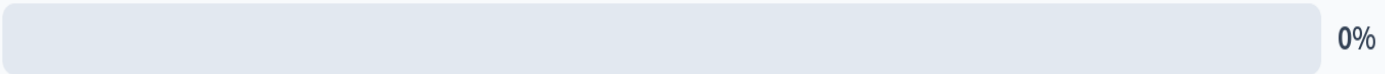
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Which tool is commonly used to detect anomalies in financial data?

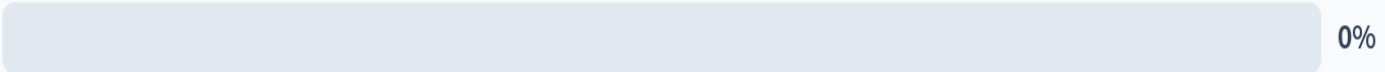
Data Visualization Software



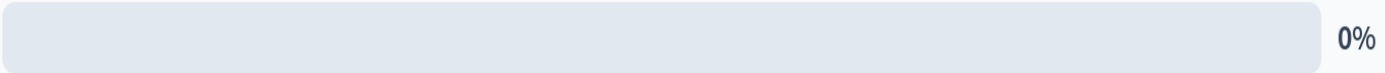
Anti-Virus Software



Time Management Software



Employee Scheduling Tools







Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Case Study – Applicant Programs



Where and How to Look for Fraud

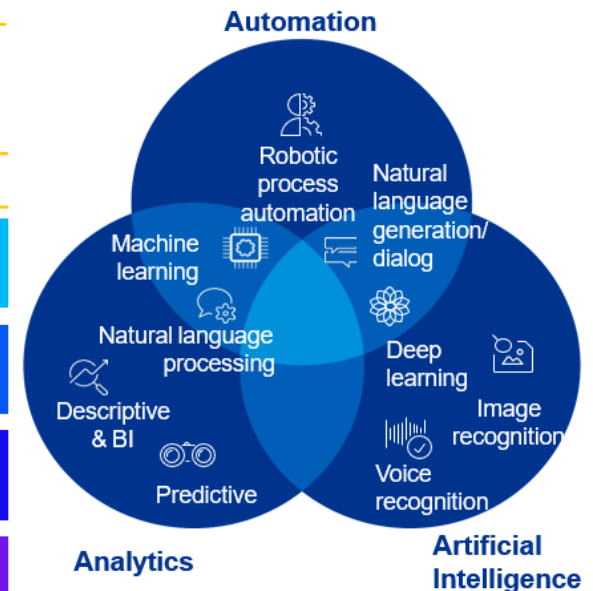
Finding fraud can be challenging and knowing where to look is half the battle. Leveraging broad sources of data and advanced modeling techniques, including machine learning, natural language processing, computer vision, and graph analytics assist with detecting actionable patterns and trends in data to reduce fraud, waste, and abuse risks posed by bad actors.

 Suspicious documents	 Suspicious ID info	 Suspicious applicant info	 Suspicious behavior
Applicant intentionally provides misleading or falsified documents that are required to receive benefits	Applicant unable to be verified through direct contact or provide materially false personal identification info	Information submitted with the application is intentionally misrepresented and cannot be validated with supporting documentation or outreach	Applicant behavior or actions taken are intended to mislead or persuade application case managers

Red flags we identify

Non-standard documents	Discrepancies with state-verified identifiers	Misrepresentation of applicant data	Aggressive pressure for decision-making
Inconsistent dates	Invalid phone numbers or emails	Fake addresses	
Manually altered documents	Shared unit addresses or contact information among applicants	Forged outstanding debts	Non-traditional communication preferences
Lack of verifiable docs (e.g., tax forms, utility bills, ID, etc.)	Lack of applicant verification through trusted data sources	Multiple claims for the same property	Frequent changes to application details
		Use of non-residential addresses	Lack of knowledge of basic information
		Discrepancies in listed addresses	
		Unsupported high claims	

Using Innovation to Identify Fraud



Falsification of Information

Fraudsters falsify documents through methods such as synthetic identity theft, altering existing documents, counterfeiting, and digital manipulation. These tactics include combining real and fake information, creating fake documents from scratch, hacking, and using fake supporting documents to deceive institutions and individuals.

What is synthetic identity fraud?

- ✓ When a criminal creates a fake identify by combining real and fictitious information

How often does it happen?

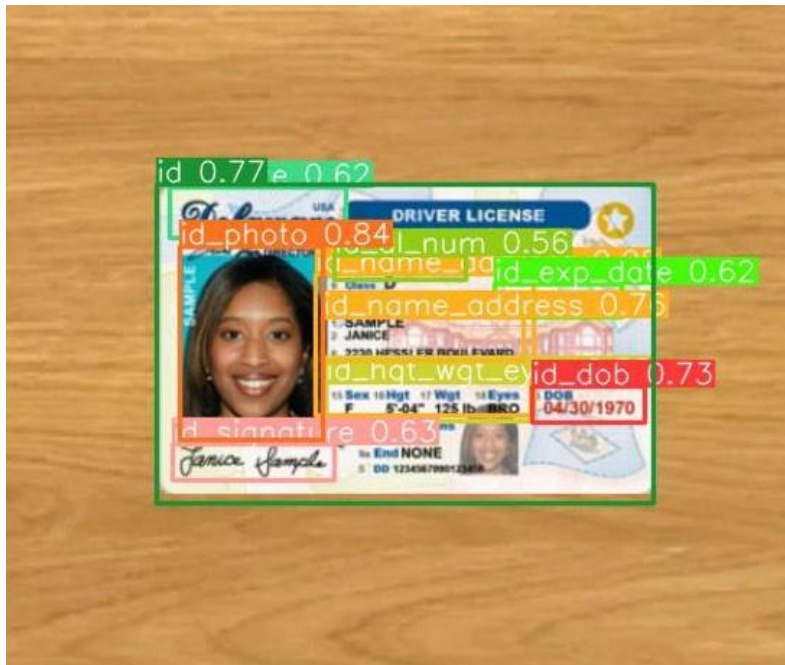
- ✓ According to a 2022 study, 46 percent of organizations faced this type of fraud

How can I catch it?

- ✓ Isolate and crop image within photo ID using objective detection models like YOLOv5
- ✓ Use packages such as OpenCV or PIL to encode the image into a format that can be processed and analyzed by computers
- ✓ Compare image encoding to one another using distance equations such as cosine similarity (using packages such as sklearn or scipy)



Example #1 – Using Object Detection Models with OCR



Object Detection Crop



OCR

“DL. No. 98765438”

“DOB 04/30/1970”

“Exp 04/30/2022”

“F 5-04 125lb BRO”

“Sample Janice”

“Delaware”

Alteration of Documents

Technology has made it easier than ever for fraudsters to alter or modify documents to pass eligibility requirements and/or receive more benefits than they are eligible for. What can you do to prevent it?

Tactical Steps



Check the document's metadata for conflicting authors and dates, and/or programmatic tags

Check for images embedded in the document where text should be

Check the text's font style and font size for consistency throughout the document

Use Natural Language Processing (NLP) techniques such as Term Frequency – Inverse Document Frequency to identify unusual patterns

Open-Source Solutions



Tika and **PIL** are powerful python packages for examining a document's metadata

PyMuPDF is able to scan provide text and image positions within a document

pdfminer and **PyMuPDF** are common packages used to identify a text's font style and size

scikit-learn and **spacy** are popular packages for NLP solutions

Example #2– Addition of Images to Document

Fraudsters commonly alter their documentation to make it appear more authentic:

- ✓ One common technique of deception is to paste a “Verified by PDFFiller” image next to a signature to simulate that a third-party has authenticated the document.
- ✓ Another technique is to modify the text within a document by pasting an edited image over the address or amount past due on a utility bill. This type of deception can be identified by comparing the ratio of images within a document to the number of words found in the document.

acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and other than interest and dividends, you are not required to sign this certification, but you must provide your correct TIN. See the instructions.	
Sign Here	Signature of U.S. person ▶ <i>Michelle Jackson</i>
	Date ▶ 11/27/2021
General Instructions • Form 1099-DIV (dividends, including those for	

Duplication of Benefits

Fraudsters frequently attempt to receive duplicate benefits by submitting multiple applications using various combinations of their name, email address, and mailing address. Fraudsters attempt to evade duplication checks by:

- 1) Using multiple email addresses that share the same username but a different email domain.
- 2) Adding dots, numeric digits, or other special characters to the email username that are either ignored by the email domain provider or aliases to the same parent email address.
- 3) Alternating between using abbreviations versus spelling out the full word within mailing addresses.

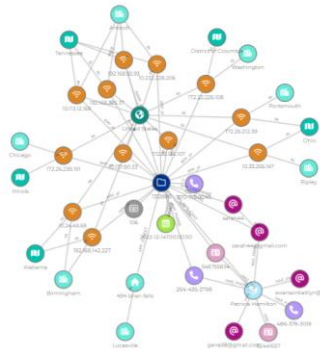
Mailing Addresses	Tenant Email Address
<p>Tenants use a similar mailing address that alternates between listing Rd vs. Road and N vs. North</p> <p>570 North Capitol Road 570 N Capitol Road 570 N Capitol Rd.</p>	<p>Tenants use a similar email address containing the prefix <u>lfc1099</u> followed by 3 digits</p> <p>lfc1099-001@yahoo.com lfc1099-002@yahoo.com lfc1099-003@yahoo.com</p>

Other AI- Enabled Solutions for Detecting Fraud

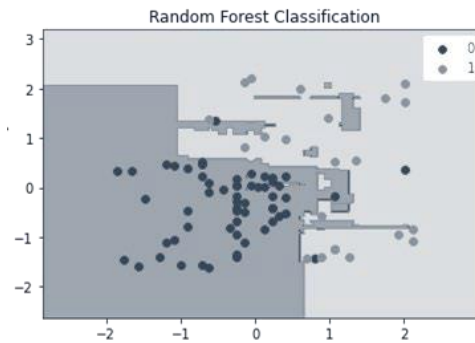
Graph analytics and machine learning models can be used to identify suspicious patterns and anomalies often associated with fraud.

- ✓ Graph algorithms and visualization tools can uncover hidden relationships and connections between entities, **such as accounts or transactions, revealing complex fraud networks.**
- ✓ Machine learning models analyze vast amounts of data to **detect unusual behavior** and **predict fraudulent activities**, continuously improving their accuracy through training on new data.

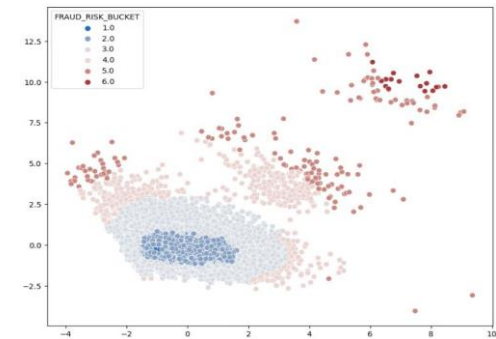
Graph Analytics



Supervised Machine Learning Model



Unsupervised Machine Learning Model



Fraud Detection Using Link/Graph analytics

Fraud is often identified through shared information or interactions between entities. Identifying and tracking complex interactions and to create new relationships make graph an excellent tool for investigating potential fraud. Combining structured and unstructured data to detect potentially problematic behavior including:

- ✓ **Communications analysis to detect problematic relationships**
- ✓ **Entity resolution to link connected identities**
- ✓ **Linking documents (e.g. contracts) through shared attributes**
- ✓ **Providing enhanced exploratory analysis during investigations**

Enhance fraud prediction models with graph features

Identify shared or similar features for applications and individuals
Graph algorithms: Centrality

Graph Improvements:

Speed ✓	Scale ✓
Cost	Clarity

Identify similar entities based on shared characteristics

A starting point when lacking fraud/not fraud labels for fraud prediction modeling
Graph algorithms: Similarity & Link Prediction, Community/Clustering

Graph Improvements:

Speed ✓	Scale ✓
Cost ✓	Clarity

Investigate individual cases to find broader connections

Deep dive into connected or suspicious applications to identify potential patterns or fraud rings
Graph algorithms: Path Finding, Centrality, Community/Clustering

Graph Improvements:

Speed ✓	Scale ✓
Cost ✓	Clarity ✓

Government Department Cyber Security Threats



Threat Landscape



Government agencies face heightened cyber risks protecting: sensitive data and critical infrastructure protection responsibilities



Complex interconnected digital environments



Expanding attack surfaces from cloud adoption and digital transformation



Rising nation-state activities and sophisticated threats



Prime targets for ransomware and other cyber attacks

Top Threat Categories



Volatile Threats

- » Attacks against AI applications and systems
- » Identity impersonation and deepfakes
- » Cyber-physical systems (CPS) attacks
- » IT/Security infrastructure threats
- » Supply chain compromises



Complex Threats

- » Advanced phishing and social engineering
- » Ransomware/extortionware campaigns
- » API abuse and exploitation
- » Account takeover and credential compromise
- » Zero-day exploitation
- » Business email compromise (BEC)

Key Risk Areas for Government Agencies

- Critical infrastructure vulnerabilities
- Supply chain compromise
- Cloud infrastructure vulnerabilities
- Legacy system exposures
- Third-party vendor vulnerabilities
- Network security gaps



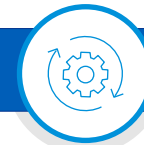
Infrastructure Risks



Emerging Risks

- AI/ML system vulnerabilities
- Digital transformation challenges
- Cross-border data compliance

Operational Risks



- Data breaches and leaks
- Service disruption and downtime
- Mission-critical system compromise
- Loss of public trust and confidence
- Unauthorized data access
- Regulatory compliance failures
- Resource and staffing constraints

Cyber Risk Mitigation Framework

01

Continuous Threat Exposure Management (CTEM)



- Regular assessment of attack surfaces
- Risk-based vulnerability management
- Proactive threat hunting
- Continuous monitoring and validation
- Third-party risk assessment
- Asset discovery and classification

02

Security Control Implementation



- Zero trust architecture adoption
- Multi-factor authentication
- Network segmentation
- Data encryption and classification
- Access control and privilege management
- Cloud security controls
- Supply chain security controls

03

Incident Response & Recovery



- Documented response procedures
- Regular tabletop exercises
- Cross-agency coordination
- Backup and recovery testing
- Incident communication plans
- Business continuity planning
- Lessons learned process

Recommendations

Strategic Priorities



- 01 Implement continuous threat exposure management
- 02 Enhance cyber-physical systems security
- 03 Strengthen supply chain risk management
- 04 Develop AI/ML security and governance frameworks
- 05 Improve cross-agency threat intelligence sharing

Tactical Steps



- Regular vulnerability and security assessment
- Security awareness and behavior training
- Third-party and supply chain assessments
- Incident response planning
- Security automation and orchestration

Who should you report suspected fraud, waste, or abuse to?

Only to your colleagues

External media outlets

Your supervisor or designated reporting channel

No one; it is not your responsibility

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Who should you report suspected fraud, waste, or abuse to?

Only to your colleagues

0%

External media outlets

0%

Your supervisor or designated reporting channel

0%

No one; it is not your responsibility

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Who should you report suspected fraud, waste, or abuse to?

Only to your colleagues

0%

External media outlets

0%

Your supervisor or designated reporting channel

0%

No one; it is not your responsibility

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

How important do you think it is for your agency to establish documented fraud, waste, and abuse policies?

Very important

Somewhat important

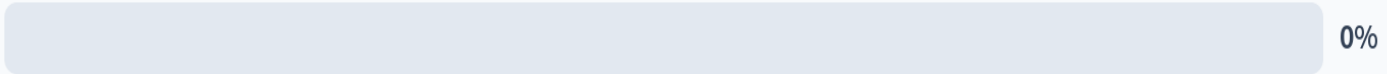
Not important

I'm not sure

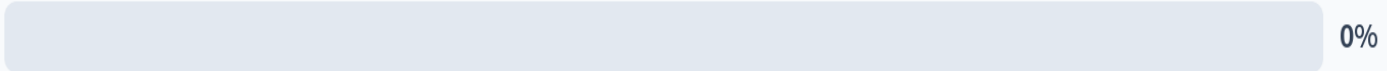
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

How important do you think it is for your agency to establish documented fraud, waste, and abuse policies?

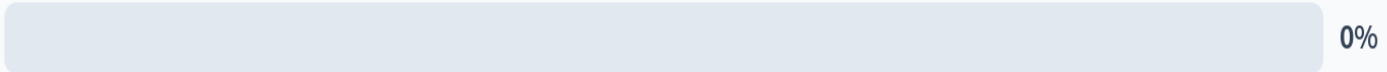
Very important



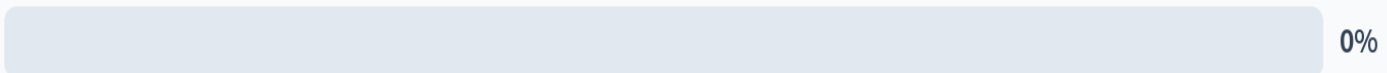
Somewhat important



Not important



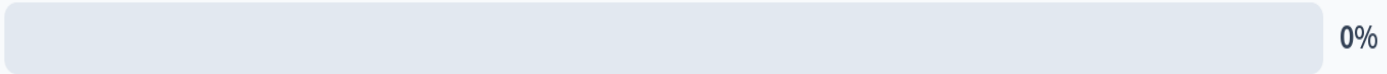
I'm not sure



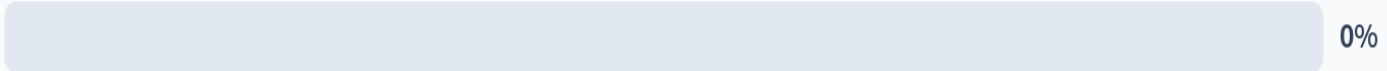
Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

How important do you think it is for your agency to establish documented fraud, waste, and abuse policies?

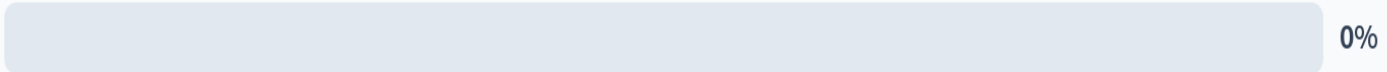
Very important



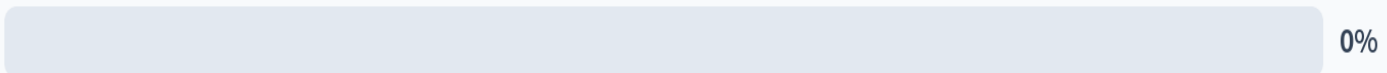
Somewhat important



Not important



I'm not sure



Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

How can employees be encouraged to report abuse without fear of retaliation?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

What steps do you think can be taken to reduce waste in your department?

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Questions & Answers



Check Out

0 surveys completed

0 surveys underway

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

Still have questions?

Contact the following individuals at the Office of the State Controller:

Stacey Alles

stacey.alles@state.co.us

303-866-4020

Gina Salazar-Love

gina.salazar@state.co.us

303-866-4289

Reference Documents



Reference Documents

2014



GAO issued the revised Standards for Internal Control in the Federal Government Requirement for federal managers to “**consider the potential for fraud** when identifying, analyzing, and responding to risks” (Principle 8)

2015



GAO issued A Framework for Managing Fraud Risks in Federal Programs ([GAO-15-593SP](#))

Detailed guide of **leading practices** to help agencies **strategically manage** their **fraud risks**

2016



Fraud Reduction and Data Analytics Act (FRDAA) enacted

2020



Payment Integrity Information Act (PIIA) enacted

Appendix



Cyber & Data (1 of 3)



Given the highly interconnected nature of the financial services sector and its dependencies on critical third-party service providers, all participants in the financial system must implement risk mitigation and resilience initiatives relative to both the frequency and impact of cyber threats.



Call to Action

- **Evolve identity and access programs to prevent takeover threats**
- **Use SOAR tools to augment cyber security resources**
- **Embed “privacy by design” throughout the data management lifecycle**



Evolving Regulatory

Effective access management and authentication controls

- Data access and authentication controls (FFIEC)

Cybersecurity disclosure

- Cyber incident disclosure requirements (FRB, OCC, FDIC)
- SEC disclosure for cyber risk governance issued in Q1 2022
- Focus on accurate disclosure of breach in addition to materiality
- Some states considering more stringent reporting and disclosures

Data & Privacy

- Rulemakings may address collection, portability, and use of consumer data (CFPB, FTC, SEC)
- CA CPRA adds business limitations, disclosure of AI models, cyber audits

Cyber & Data (2 of 3)



Challenges

Access management and authentication controls

- Growth in data collection and transfers has increased the number of attack vectors for bad actors
- Identification of a wide range of users
- Weak access and transaction controls facilitate malicious actors

Legal/regulatory compliance requirements

- Top FS risk; national security threat
- Increasing expectations for enhanced cybersecurity capabilities
- Timely cyber incident disclosure (moving toward any successful attempt/intrusion)

Customer data privacy and protection

- Customer data increasingly collected and used for predictive analytics, personalized marketing, and to introduce products/services
- Benefits to scale
- Customer desire to control collection and use

Cyber & Data (3 of 3)



Given the evolving cyber security risks which organizations are facing, Internal Audit can assist the organization with assessing the risk mitigation and resilience initiatives the organization has developed as they relate to the frequency and impact of cyber threats.

Risk Assessment



Ensure the organization's cybersecurity risk assessment, processes, and controls are in line with industry standards.

Data Security



Ensure appropriate controls are in place to prevent data leakage and / or security breaches.

Government Standards



Ensure adequate governance and oversight, monitoring of security operations and task action in regards to the IT risk management function.

Internal Audit Considerations



Training



Ensure awareness of cyber security concerns is sufficiently fostered and whether staff training has been updated considering changes to the working environment and IT infrastructure.

Technology Security Models



Ensure the appropriate implementation of revised technology security models, such as multilayered defenses, enhanced detection methods and encryption of data leaving the network

Share Knowledge



Ensure the organization has an appropriate understanding of cyber security risks and identify possible mitigation strategies to determine if cyber risks have been adequately managed.

Third Party & Cloud (1 of 3)



Financial services organizations are rapidly forming more numerous and complex relationships with third-party companies, including fintech-focused entities such as cloud service providers. These relationships offer advantages, but can reduce management's direct control of activities, which may introduce new risks or elevate existing risks.



Call to Action

- **Centralize and automate TPRM processes**
- **Execute dynamic TPRM risk assessments across the TPRM lifecycle**
- **Meet or exceed regulatory expectations across jurisdictions**
- **Build and use data sandboxes to strengthen cloud adoption/migration**
- **Build a “zero trust” security environment**



Evolving Regulatory

TPRM

- FRB, OCC, and FDIC proposed joint TPRM guidance
- FFIEC guidance on cloud computing

Security Systems and Authentication

- FFIEC guidance on systems authentication and access addresses many of the zero-trust architecture features, including multi-factor authentication, encryption, identity protection, and endpoint security

Third Party & Cloud (2 of 3)



Challenges

Centralization and automation third party risk management (TPRM)

- Allows for standardized, repeatable, scalable process
- Consistency in risk identification, prioritization
- Inventory and group vendors by risk assessments or risk categories

Third party risk assessments

- Comprehensive risk assessments should examine:
 - 3 lines of defense, enterprise-wide
 - Board reporting on risks, mitigation, and/or remediation
 - Criticality, prioritization
 - Multi-cloud, vendor duplicity strategies

Multiple jurisdictions/regulatory expectations

- Expectations differ across jurisdictions; FS ultimately responsible
- Clearly document responsibilities in contracts

Security Systems and Authentication

- Testing the impacts of changes to TPRM can provide opportunities to identify issues or vulnerabilities
- Regulatory attention on “zero-trust” security systems is building

Third Party & Cloud (3 of 3)



Internal Audit plays a key role in supporting the organization with their third-party service provider programs and ensuring appropriate compliance with regulatory requirements. The third-party relationships can reduce management's direct control of activities which may introduce new risks.

Cloud Security

Ensure the security and controls framework for cloud technologies is appropriate based on industry standards and frameworks. In addition, ensure that there are cloud-delivered security measures that align with the "Zero Trust" principle.

3rd Party Data Assessment

Ensure there is an enterprise-wide data privacy framework around third-party cloud solutions to ensure that the business practices are in alignment with privacy laws.

Accessibility & Availability Assessment

Ensure the third-party cloud solutions are accessible via various terminals and that the system downtime is minimized.

Internal Audit Considerations



SDLC Management

Ensure management is taking a sound and suitable system development lifecycle approach by conducting a risk-based implementation review.

Vendor Risk Management

Ensure there is a process in place for selecting, evaluating, and managing new providers and to continuously evaluate the compliance of contracts with key providers and solutions.

Vendor Duplicity Multi-Cloud Strategies

Ensure system configurations are standardized, the coordination is optimized, and software management is centralized across various vendor solutions.

Tech & Resiliency (1 of 3)



Recent events have clarified that significant disruptions are increasingly likely and can be interconnected. Though advances in technology have improved companies' ability to identify and recover from these disruptions, the frequency of them and potential for interconnectedness to augment risks underscore the need for operational resilience.



Call to Action

- **Set criticality standards and methodology**
- **Measure asset risk exposure**
- **Provide transparency to board / management**



Evolving Regulatory

Resilience practices and standards

- Regulators may consider governance, risk management, business continuity planning, TPRM, scenario analysis, etc. in supervisory examinations
- Methodology, controls, and other policies, processes, and procedures

Vulnerabilities and Remediation

- Regulators may focus on tools used for vulnerability discovery, prioritization of remediations, unremediated issues, internal controls, etc.

Transparency to boards and senior management

- Board review and approval of disruption “tolerances”; requirements to timely report cyber incidents

Consolidated Appropriations Act of 2022 (Cyber Incident Reporting Act)

- Organizations will need to swiftly report certain cyber incidents and ransomware payments to the Department of Homeland Security

Digital Operational Resilience Act (DORA)

- European Union legislation designed to improve the cybersecurity and operational resiliency of the financial services sector

Tech & Resiliency (2 of 3)



Challenges

Access management and authentication controls

- Growth in data collection and transfers has increased the number of attack vectors for bad actors
- Identification of a wide range of users
- Weak access and transaction controls facilitate malicious actors

Legal/regulatory compliance requirements

- Top FS risk; national security threat
- Increasing expectations for enhanced cybersecurity capabilities
- Timely cyber incident disclosure (moving toward any successful attempt/intrusion)

Customer data privacy and protection

- Customer data increasingly collected and used for predictive analytics, personalized marketing, and to introduce products/services
- Benefits to scale
- Customer desire to control collection and use

Tech & Resiliency (3 of 3)



Understanding the criticality, pervasiveness, and business-driven acceptable outage timeframes for all critical systems – and aligning that information to validated IT recovery capabilities – is key to building resilience. Organizations that are able to compare business expectations to live / real-time IT system data are inherently more resilient.

Recovery & Continuity Strategy

Ensure the appropriateness of key requirements for organizational resilience, strategies for risk reduction, and the organization's approach to managing service disruptions / outages.

Training

Ensure effective trainings are provided to key stakeholders and clearly provide guidance on response, recovery, and continuity strategies.

Internal Audit Considerations



Disruption Management

Ensure the ability to continue critical operations in the face of a business disruption, or an outage of critical systems.

Resilience Maturity

Ensure lessons learned from incidents, exercises, and other reviews of performance are implemented to support ongoing development in resilience maturity.

Building Resiliency

Ensure resiliency is facilitated through the use of technologies and agile auditing techniques, in response to new and emerging threats.

Ransomware and Cybercrimes

Ensure there are sufficient controls around ransomware and other cybercrimes to prevent account ID theft, bot attacks, synthetic ID frauds, etc.

Thank you!

