RED FLAGS- CONCEPTS AND TECHNIQUES

Presented by:

John Ekadah

Fraud: Introduction

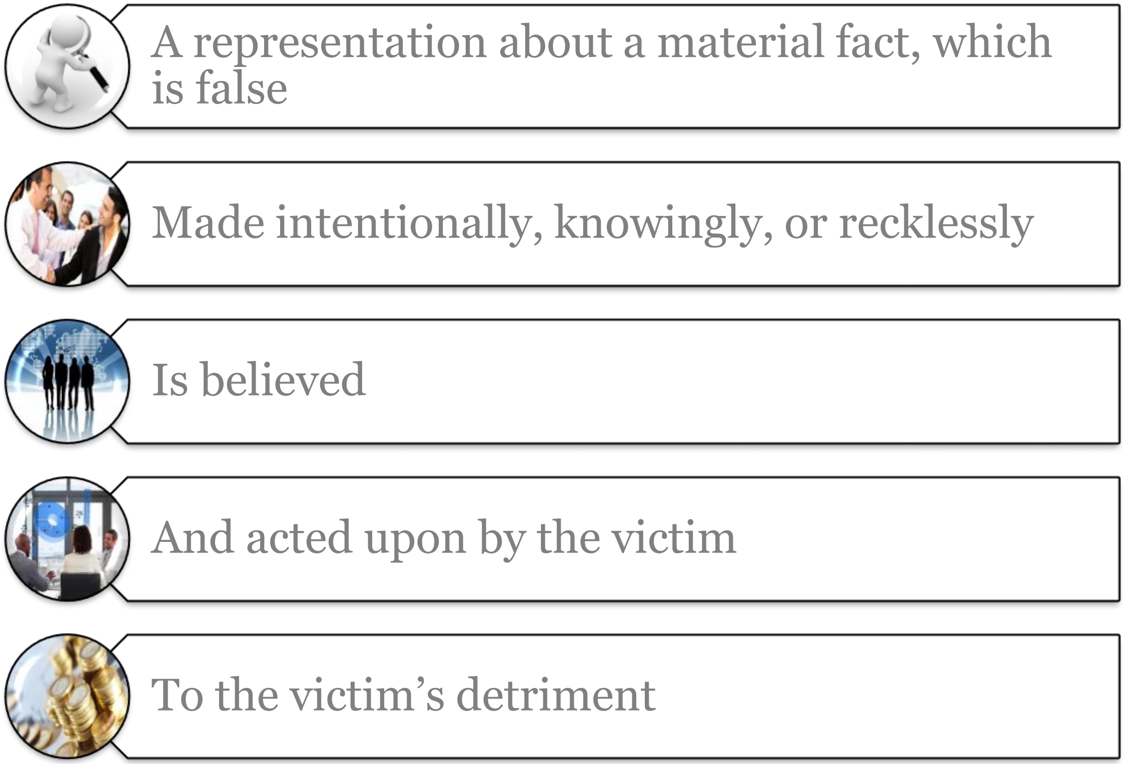
Definition of fraud

- A false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury.” *-Black’s Law Dictionary*
- Common classifications of fraud: corruption, asset misappropriation and fraudulent financial statements.

Corruption: Definition

- Corruption means any dishonest activity in which an organization's employee abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself or for another person or entity. Examples:
    - Conflict of interest which puts a person's interest ahead of the interest of the organization.
    - Inappropriate application of the tender and procurement process.
    - Accepting or seeking anything of value from any contractor, vendor or person providing services or materials to the organization.
    - Bribing, or attempting to bribe, any public official, vendor, customer or other person.

Elements of Fraud



- A representation about a material fact, which is false
- Made intentionally, knowingly, or recklessly
- Is believed
- And acted upon by the victim
- To the victim's detriment

What is Fraud in a Commercial Setting?

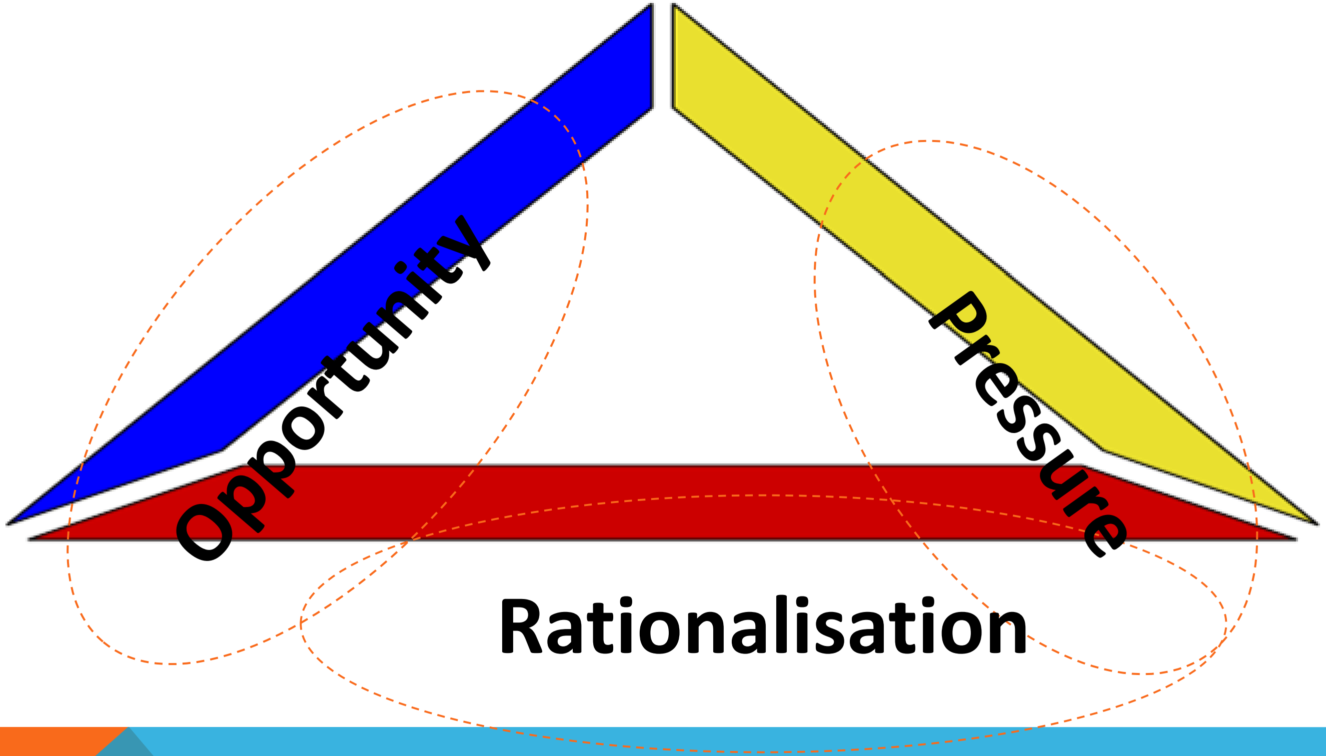
- Organizational Crime: that which is committed by businesses, particularly corporations and government.

- Occupational Fraud: offenses against the law by individuals in the course of their occupation.

Characteristics of Occupational Fraud

- Is clandestine or hidden;
- Violates the perpetrator's fiduciary duties to the victim organization;
- Is committed for the purpose of the direct or indirect financial benefit to the perpetrator;
- Costs the employee's organization assets, revenues or reserves; and
- Fraud is a global issue.

Why people commit fraud: Fraud Triangle



Why people commit fraud: Fraud Triangle

- Work Pressure
- Performance targets
- Poor financial performance
- Threat of job loss
- Personal pressure:
- Extravagant Life style
- To meet society's expectation
- To cover errors
- Intellectual challenge
- Financial problems
- Drugs or gambling
- Greed
- Medical bills

Opportunity

- Weak organizational policies and procedures
- Poor organizational corporate governance

Rationalization

Is justifying a behavior i.e. I stole

………….

- To save a family member who was sick or in jail.
- To save my home, car, etc. from being auctioned by the bank
- To reward myself because the organization does not pay me enough.

…A Typical Fraudster

Male

36 to 45 years

Commits fraud against employer

Finance or related function Fundraising,

Progra

Holds senior management position

Employed by Org. for over 10 years

Works in collusion with perpetrator

Fraud Risk Management Defined

- A Fraud Risk Assessment is a process that organizations utilize to determine their exposure to fraud, both internal and external. The assessment is a review of the operations and controls of an organization to determine where gaps exist that could allow fraud against the organization.

- The Fraud Risk Assessment looks at key areas to determine if actions have been taken that would alert management to risk or to effectively deter the execution of a fraud.

- Each risk assessment needs to be tailored for the organization and the specific risks faced by that organization

Fraud Risk Management – What, How, Why

- To mitigate the innumerable risks posed by fraud and misconduct.
- Achieved by identifying the risks and existing controls so as to develop an effective fraud risk management program.
- An effective fraud risk management framework will help achieve the following objectives:
  - Prevention – reduce the risk of fraud occurring;
  - Detection – discover fraud; and
  - Response – corrective action.

Sample Antifraud Program Elements

Prevention	Detection	Response
Board/audit committee oversight Executive and line management functions Internal audit, compliance, and monitoring functions		
❖ Fraud and misconduct risk assessment ❖ Code of conduct and related standards ❖ Employee and third-party due diligence ❖ Communication and training ❖ Process-specific fraud risk controls	❖ Hotlines and whistle-blower mechanisms ❖ Auditing and monitoring ❖ Proactive forensic data analysis	❖ Internal investigation protocols ❖ Enforcement and accountability protocols ❖ Disclosure protocols ❖ Remedial action protocols

Prevention

- Preventive controls are designed to reduce the risk of fraud and misconduct from occurring in the first place.
  - Leadership and Governance
    - ✓Board Audit Committee Oversight
    - ✓Senior Management Oversight
  - Internal Audit Function
  - Code of Conduct
  - Employee and Third-Party Due Diligence
  - Communication and Training
  - Fraud and Misconduct Risk Assessment

Prevention

Leadership and Governance

- Board/Audit Committee Oversight
  - May delegate principal oversight for fraud and misconduct risk management to a committee tasked with:
    - Reviewing and discussing issues raised during the entity's fraud and misconduct risk assessment
    - Reviewing and discussing with the internal and external auditors findings on the quality of the organisation's antifraud programs and controls
    - Establishing procedures for the receipt and treatment of questions or concerns regarding questionable accounting or auditing matters

Prevention

Leadership and Governance

- Senior Management Oversight
  - Chief Executive Officer can set the ethical tone and foster culture of high ethics and integrity
  - Chief Compliance Officer may chair committee of cross-functional managers who:
    - Coordinate the organisation’s risk assessment efforts
    - Establish policies and standards of acceptable business practice
    - Oversee the design and implementation of antifraud programs and controls
    - Report to the board and/or the audit committee on the results of the organisation’s fraud risk management activities

Prevention

Internal Audit Function

- Responsibilities include:
  - Planning and conducting the evaluation of design and operating effectiveness of antifraud controls
  - Assisting in the organisation’s fraud risk assessment and helping draw conclusions as to appropriate mitigation strategies
  - Reporting to the audit committee on internal control assessments, audits, investigations, and related activities

Prevention

Code of Conduct

- High-level endorsement from the organisation’s leadership
- Simple, concise, and positive language
- Topical guidance based on each of the company’s major policies or compliance risk areas
- Practical guidance on risks based on recognisable scenarios or hypothetical examples
- A visually inviting format
- Ethical decision-making tools
- A designation of reporting channels and viable mechanisms for reporting concerns and seeking advice

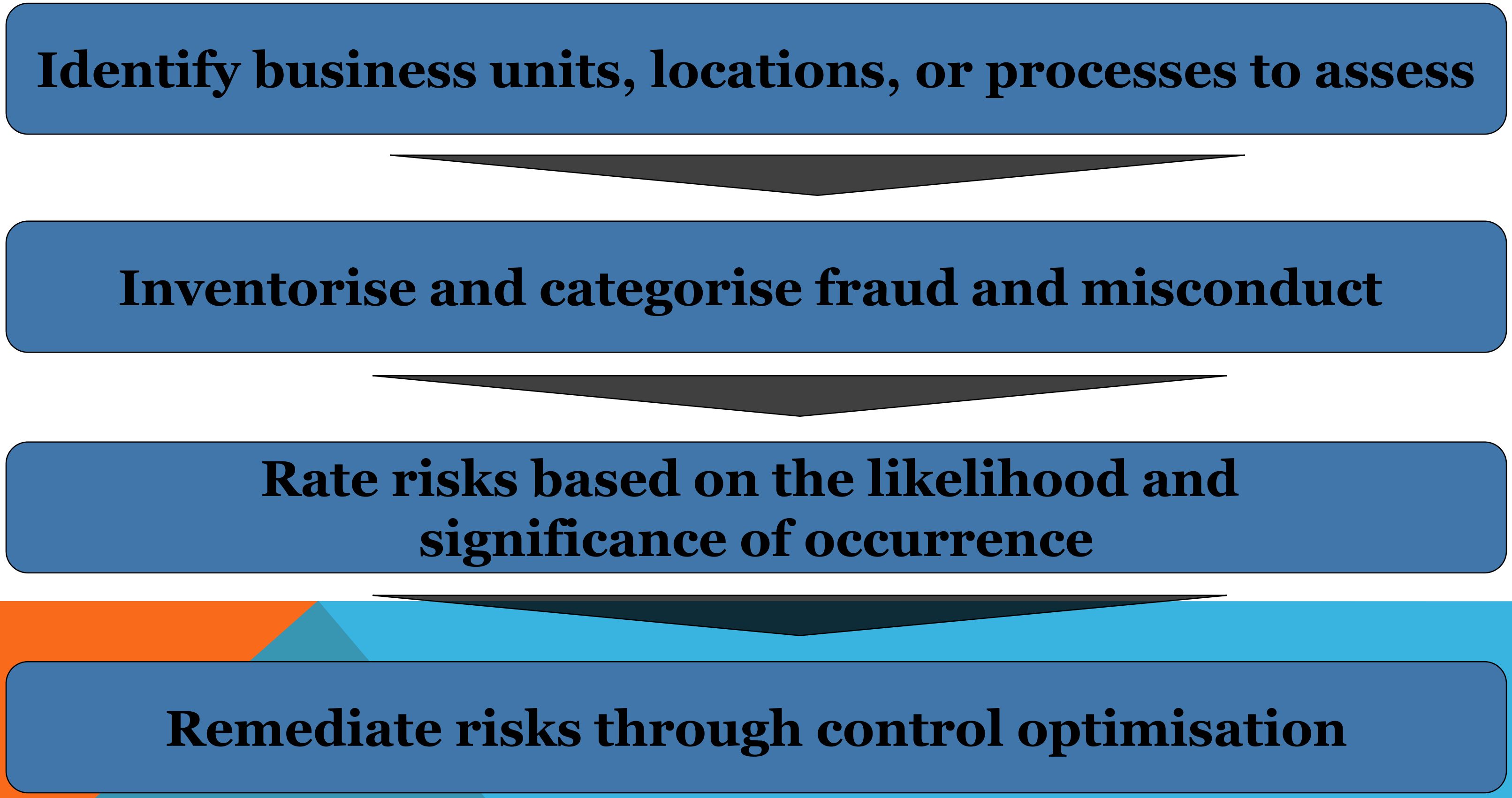
Prevention

Employee and Third-Party Due Diligence

- Used in hiring, retention and promotion of employees, agents, vendors and other third parties
- Scope and depth of due diligence varies based on organisation’s identified risk, individual’s job function/level of authority, and specific laws of the country in which organisation resides

Prevention

Fraud and Misconduct Risk Assessment Process



Identify business units, locations, or processes to assess

Inventorise and categorise fraud and misconduct

Rate risks based on the likelihood and significance of occurrence

Remediate risks through control optimisation

Detection

Detective controls are designed to uncover fraud and misconduct when it occurs.

- Mechanisms for Seeking Advice and Reporting Misconduct
- Auditing and Monitoring
- Proactive Data Analysis

Detection

Mechanisms for Seeking Advice and Reporting Misconduct

- Telephone hotlines provide a viable method whereby employees, and other third-parties, if applicable, are encouraged to:
  - Communicate concerns about potential fraud and misconduct
  - Seek advice before making decisions when the appropriate course of action is unclear

Detection

Auditing and Monitoring

- Performed in areas where:
  - There are specific concerns about a key procedure, account, or position
  - The company has a history of fraud and misconduct
  - There is high employee turnover or organisational change
  - Laws and regulations have changed significantly
  - Audits are legally required, or government agencies are targeting enforcement actions

Proactive Forensic Data Analysis

- Uses sophisticated analytical tools and techniques
- Computer-based cross-matching
- Non-obvious relationship identification to highlight potential fraud and misconduct
- Benefits include:
  - Identify hidden relationships between people, organisations and events
  - A means to analyse suspicious transactions
  - An ability to assess the effectiveness of internal controls intended to prevent or detect fraudulent activities
  - Potential to continually monitor fraud threats and vulnerabilities
  - Ability to consider and analyse thousands of transactions
  - Ability to consider a company's unique organisational and industry issues

Response

Response controls are designed to take corrective action and remedy the harm caused by fraud or misconduct.

- Investigations
- Enforcement and Accountability
- Corrective Action

Response

Investigations

- A well-designed process will typically include these attributes:
  - Oversight by the organisation’s audit committee, or special committee of the board
  - Direction by the outside counsel, selected by the audit committee
  - Vetting by organisation’s external auditor
  - A full-cooperation requirement
  - Reporting protocols

Response

Enforcement and Accountability

- A disciplinary process typically includes company wide guidelines that promote:
  - Progressive sanctions consistent with the nature and seriousness of the offense
  - Uniform and consistent application of discipline regardless of rank, tenure, job function

RESPONSE

Enforcement and Accountability

- Holding managers accountable is an important consideration
- Managers may be disciplined when they:
  - Knew, or should have known, that fraud and misconduct might occur
  - Directed or pressured others to violate company standards
  - Failed to ensure employees received adequate training or resources
  - Failed to set a positive example
  - Enforced company standards inconsistently or retaliated against others

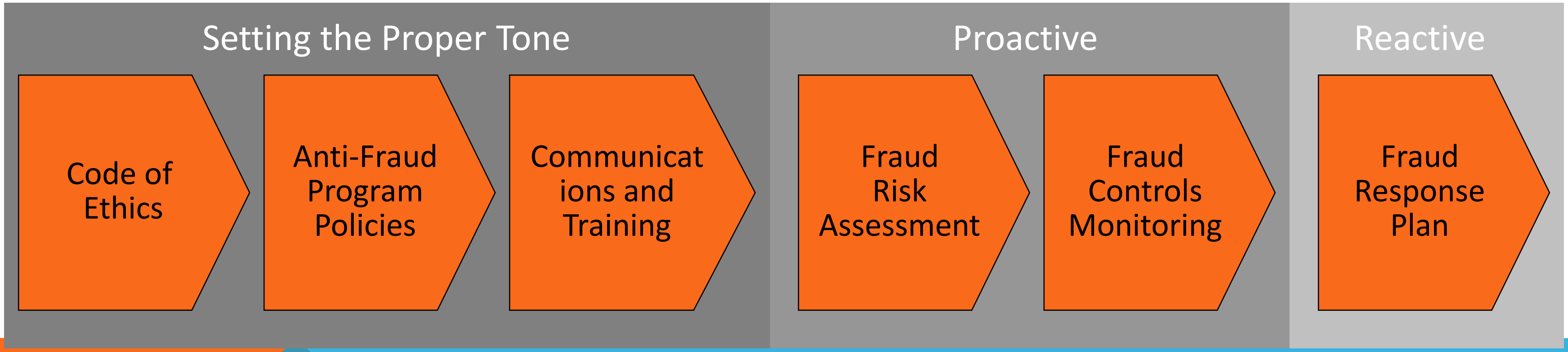
Response

Corrective Action

- Voluntarily disclosing the results of the investigation
- Remedying the harm caused
- Examining the root causes
- Administering discipline to those involved
- Communicating to the wider employee population

Anti-fraud Compliance Program

- An anti-fraud program demonstrates that management is setting the proper “tone at the top”
- An effective anti-fraud program should include each of the following elements:



Setting the Proper Tone

Code of Ethics

Anti-Fraud Program Policies

Communications and Training

Proactive

Fraud Risk Assessment

Fraud Controls Monitoring

Reactive

Fraud Response Plan

- An anti-fraud program will not provide absolute assurance against fraud, but it can help to mitigate the effects of fraud.

Fraud Risk Universe

(Example For Illustrative Purposes)

Financial Reporting

- Fictitious revenue (e.g. channel stuffing)
- Fictitious receivables
- Failure to write-off uncollectible amounts
- Manipulation of bad debt reserve assumptions
- Improper expense capitalization
- Manipulation of fixed asset depreciation schedules or assumptions
- Improperly accounting for leased equipment
- Improper inventory valuation
- Recording fictitious investments
- Misclassification of investments to postpone recognition of losses (e.g. bonds from trading to held-to-maturity)
- Failure to record impairments (goodwill, intangibles, fixed assets, or investments)
- Understatement / overstatement of accruals

  Failure to record contingencies
- Inappropriate "top-side" adjustments

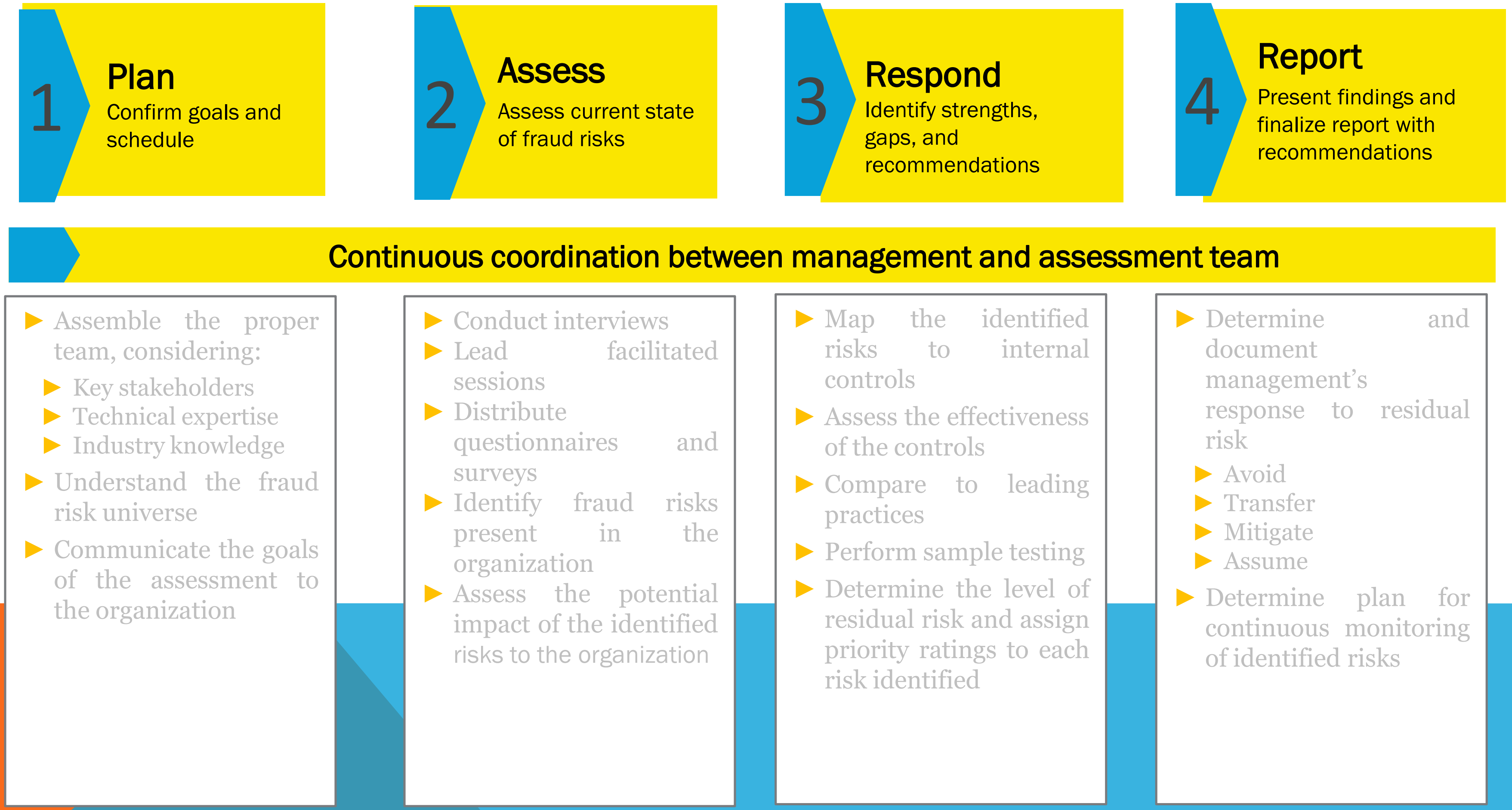
Corruption

- Bribery of government officials (e.g. direct payments, gifts, vacations, paying personal expenses, etc.)
- Bribes or kickbacks (e.g. company employees receiving compensation for favoring particular vendors)
- Extortion (soliciting payment from vendor to award business)
- Bid manipulation (procurement or sales)
- Inappropriate sole sourcing
- Conflicts of interest
- Product / equipment substitution
- Falsifying quality control documents
- Cost overcharging (excessive time or inflated / non-existent materials)
- Charging the same expense multiple times to different contracts
- Duplicate billing

Asset Misappropriation

- Theft of confidential information (proprietary business information or personally identifiable information)
- Payments to "phantom" employees
- Manipulation of pay rates or timecards
- Falsified commission calculations
- Worker's compensation fraud
- Payments to fictitious vendors or charities
- Check tampering (payee or endorsement forgery, amount manipulation, stolen check)
- Receivables lapping
- Unauthorized discounts / credit memos (kickbacks from customer or check diversion)
- Expense report fraud (fictitious or personal expenses, overstated expenses, duplicate submissions)
- Inappropriate personal use of company assets
- Corporate card abuse
- Embezzlement
- Petty cash theft
- Inventory theft

Stages of the Fraud Risk Assessment



1 **Plan**
Confirm goals and schedule

2 **Assess**
Assess current state of fraud risks

3 **Respond**
Identify strengths, gaps, and recommendations

4 **Report**
Present findings and finalize report with recommendations

Continuous coordination between management and assessment team

- Assemble the proper team, considering:
  - Key stakeholders
  - Technical expertise
  - Industry knowledge
- Understand the fraud risk universe
- Communicate the goals of the assessment to the organization

- Conduct interviews
- Lead facilitated sessions
- Distribute questionnaires and surveys
- Identify fraud risks present in the organization
- Assess the potential impact of the identified risks to the organization

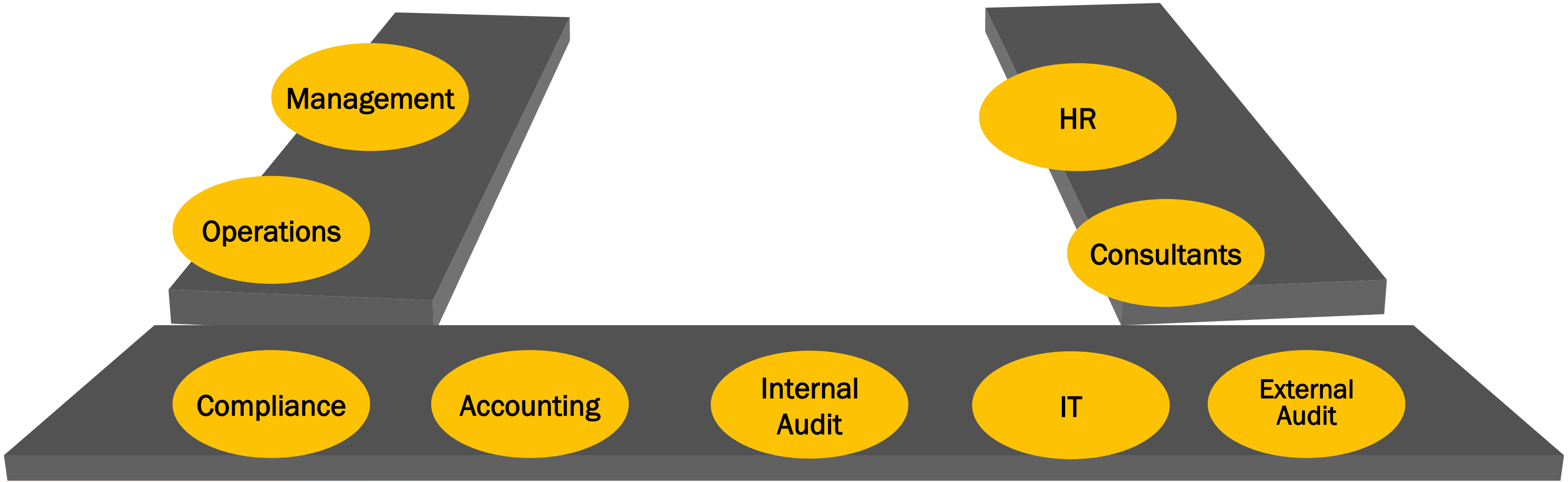
- Map the identified risks to internal controls
- Assess the effectiveness of the controls
- Compare to leading practices
- Perform sample testing
- Determine the level of residual risk and assign priority ratings to each risk identified

- Determine and document management's response to residual risk
  - Avoid
  - Transfer
  - Mitigate
  - Assume
- Determine plan for continuous monitoring of identified risks

Assemble the proper team

- Chose the right sponsor
- Ensure access to the entire organization
- Select team members with adequate technical skills
- Consider the independence/objectivity of the team members

Plan | Assess | Respond | Report



Management

Operations

HR

Consultants

Compliance

Accounting

Internal Audit

IT

External Audit

Understand organization risks

Plan | Assess | Respond | Report

Understand the types of risks present:

- **Inherent risk** – Present regardless of management's actions, based on the nature of the business.
- **Residual risk** – Remaining risk after management's actions, contingent upon what controls are in place

The ultimate goal of the Fraud Risk Assessment is to determine the residual risk present in the organization. However, during the planning stage, all risks should be considered.

Communicate goals

Plan | Assess | Respond | Report

- Management should set the tone of the assessment
- Employees should be encouraged to actively participate
- Information must be shared freely

Distribute questionnaires

Plan | Assess | Respond | Report

- Questionnaires allow access to large numbers of personnel, in an anonymous format

	Yes	No	Not Applicable
Do any employees have large personal debts or credit problems?			
Do any employees appear to be spending far more than they are earning?			
Do any employees gamble excessively?			
Do any employees use alcohol or drugs excessively?			
Do any employees resent their superiors?			
Do any employees have a close association with vendors or competitors?			
Do any employees have outside business interests that might conflict with their duties at the company?			
Is the company experiencing high employee turnover?			
Are employees required to take annual vacations?			

Hold focus groups

- Focus groups allow individuals from different parts of the organization to discuss and explore fraud issues in an open, controlled environment

- Skilled facilitators are crucial to ensure that the discussions stay on track and explore all relevant risks

- During the session, anonymous survey devices can be used to poll the participants on their opinions of certain fraud risks

Interview key employees

Plan | Assess | Respond | Report

- Interviews allow in-depth discussion of fraud risk with employees most knowledgeable of risks and controls

- The interviewers should be non-confrontational and clearly state the purpose of the interview

- Employees can be encouraged to think of hypothetical situations, such as “If you were promoted, how could someone who took your place commit fraud against the organization?”

Understand risk impact

- During the assessment phase, the team should make an effort to understand the potential impact to the organization posed by each risk

Simple example

Dollar impact of risk = $10,000,000

Likelihood of occurrence = 20%

Potential impact = $10,000,000 x 20% = $2,000,000

- Also consider non-financial impacts of fraud risks:
  - Reputational
  - Legal
  - Regulatory

Assess effectiveness of controls

Plan | Assess | Respond | Report

- Each risk should be mapped to its corresponding controls
- For key risks, the controls can be tested, through sample testing
- The team will assess whether the controls seem to be functioning as intended

Simple example

Control – All employee expense reports must be approved by manager

Test – Select a sample of expense reports and look for evidence of approval

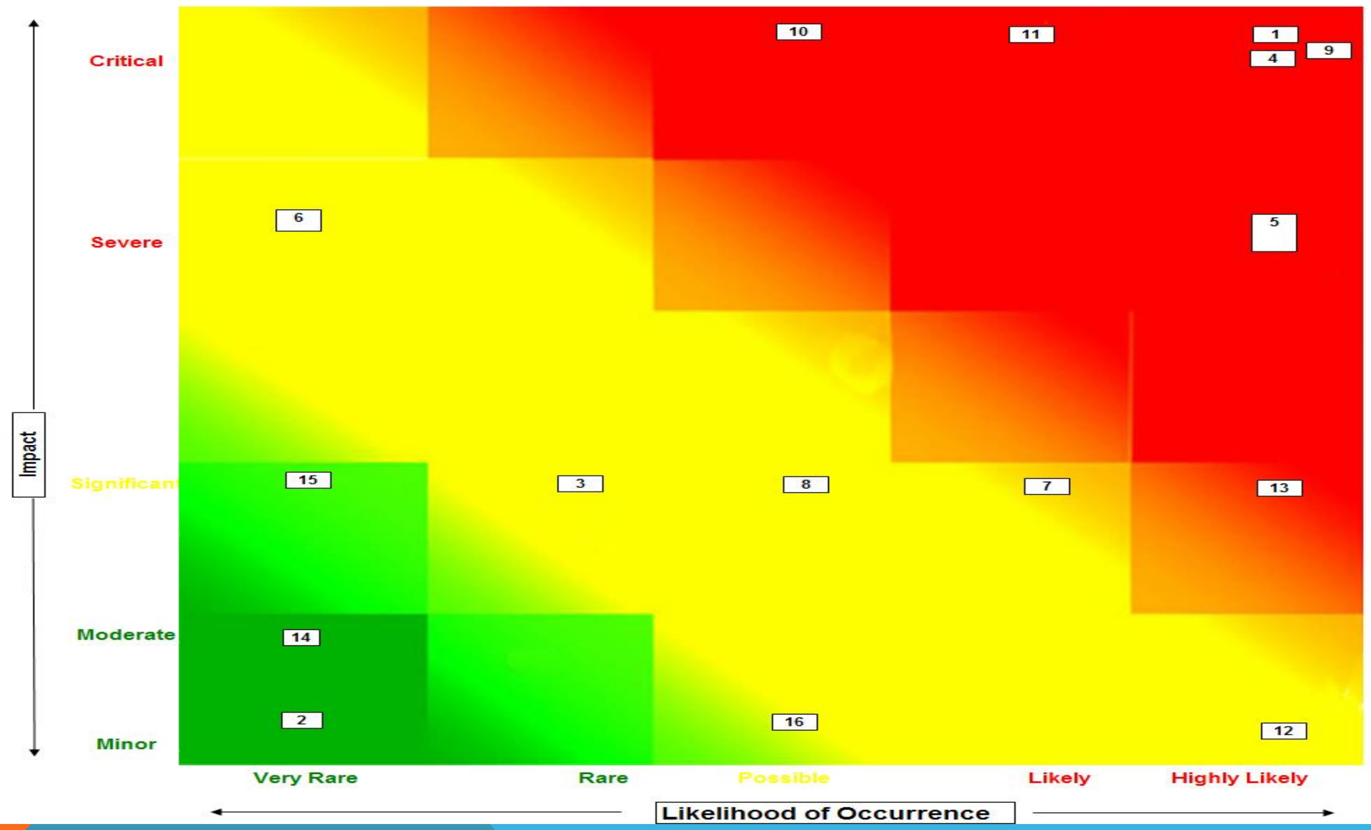
Result – If a significant percentage of the sample lacked approval, the control may not be functioning properly

Rank and prioritize risks – heat map

Plan | Assess | Respond | Report

- Risks should be tied to controls to understand and rank the residual risks

Fraud Risk Assessment - Overall Schemes



Legend

	Fraud Schemes	Impact	Likelihood
1	FCPA	Critical	Highly Likely
2	Bill and Hold Transactions	Minor	Very Rare
3	Trade Loading/ Channel Stuffing	Significant	Rare
4	Commercial Bribery	Critical	Highly Likely
5	Fraudulent Workers Comp Claims	Severe	Highly Likely
6	Customer Side Agreements	Severe	Very Rare
7	Fraudulent Inventory Capitalization	Significant	Likely
8	Fraudulent Overstatement of Trade Receivables	Significant	Possible
9	Conflicts of Interest	Critical	Highly Likely
10	Vendor Fraud	Critical	Possible
11	Benefit Fraud	Critical	Likely
12	Expense Reimbursement Fraud	Minor	Highly Likely
13	Procurement Fraud	Significant	Highly Likely
14	Cash Skimming	Moderate	Very Rare
15	Theft of Inventory	Significant	Very Rare
16	Sales and Marketing Fraud	Minor	Possible

Determine Managements Response

Plan Assess Respond Report

Management will decide on the organizational response to the residual risks identified

- **Avoid –** Management can avoid a risk by stopping the underlying activity all together
- **Transfer –** Management can transfer a risk by moving the potential impact elsewhere, such as by purchasing fraud insurance or asking a business partner to perform the underlying activity
- **Mitigate –** Management can mitigate a risk by adding additional controls which will reduce the residual risk to an acceptable level
- **Assume –** Management can assume a risk by determining that the currently present residual risk is already at an acceptable level when considered against the cost of additional controls, so no further action will be taken

Report Results

Plan | Assess | Respond | Report

- The report should be easy to understand and digest
- Format of the report is flexible, could be oral presentation or full written report
- All key information should be reported
- Management should sign-off on the report and the results communicated to the organization
- Periodically, key risks from the assessment should be revisited, with key controls continuously monitored