Fraud Risk Management

2021

Fighting fraud:
A never-ending battle

Our survey findings

When fraud strikes: **Incidents of fraud**

47%

told us **they had experienced fraud in the past 24 months.** This is the **second highest** reported level of incidents **in the past 20 years.**

6 incidents of fraud

On average, companies reportedly experienced 6 incidents **in the last 24 months.**

Top 4 types of fraud

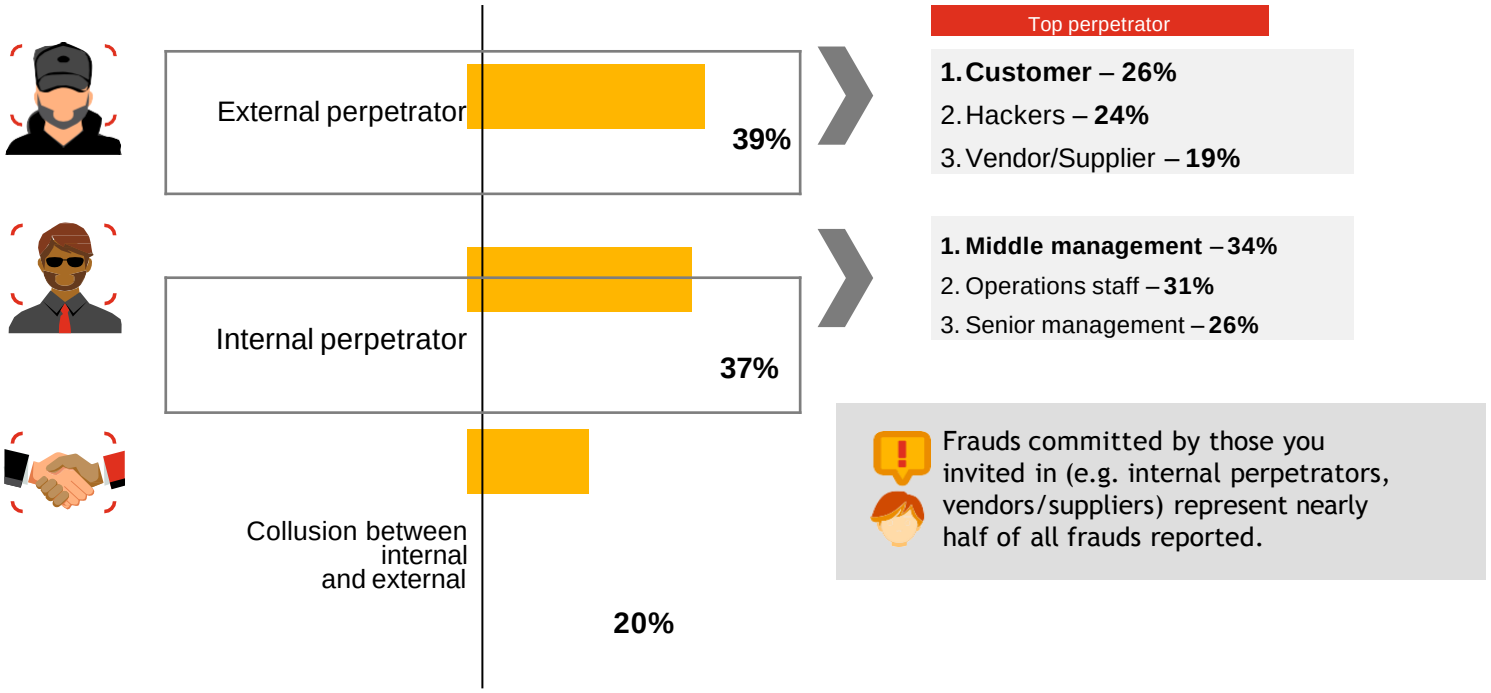
1. **Customer Fraud**
2. Cybercrime
3. Asset Misappropriation
4. Bribery and Corruption

Reported incidents of fraud committed by customers, accounting fraud, human resources fraud, and bribery and corruption — saw big increases this year.

The perpetrators: **Who's committing fraud**

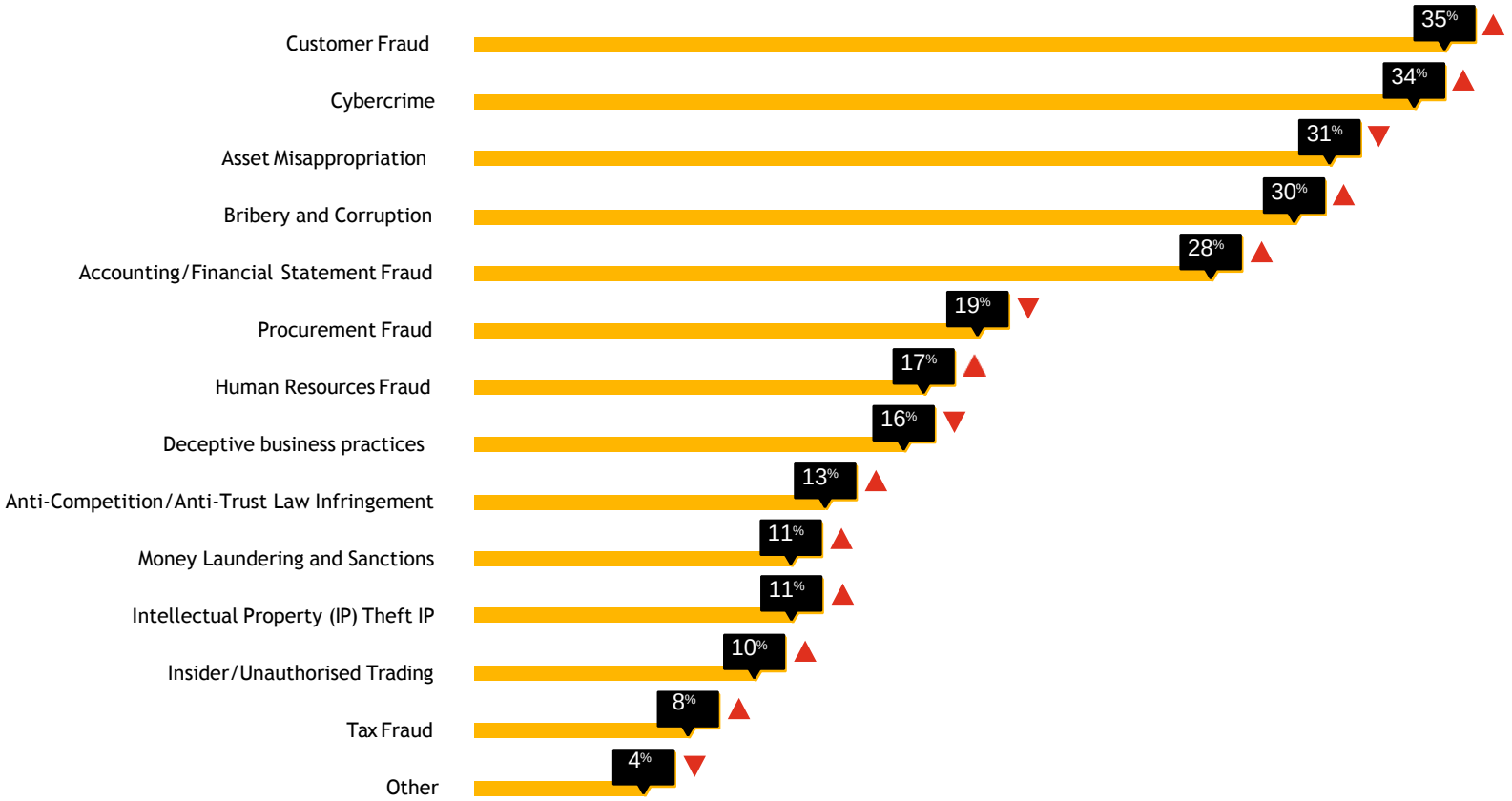
Fraud hits companies from all angles – the perpetrator could be internal, external, or in many instances there will have been collusion. Business partners remain a risk and fraud committed by management is trending upward.

Perpetrators: external, internal and collusion between them



Source: PwC's 2020 Global Economic Crime and Fraud Survey

Crimes: frequency of overall experience



Source: PwC's 2020 Global Economic Crime and Fraud Survey

Key Pressure Points we observe in the new environment that increase the risk of fraud

Fast tracking new suppliers and other business partners (customers, suppliers, agents, intermediaries or other advisors)

- The risk of onboarding third parties which are not fully vetted and screened may result in working with disreputable or even restricted parties;
- Working with new agents/intermediaries, due either to closure of existing agents or inability to deliver the volume needed;
- The pressure of bringing products very quickly to market.

Increased dealings with government officials

- Regulatory approvals, key IP issues, supply chain, financial aid: all of these are increasing the dealings employees have with government officials in higher risk jurisdictions, many of whom may not be trained for such interactions.

Shift of resources

- Business models are challenged and executives are more focused on operational measures than compliance and fighting fraud;
- The temporary transfer of staff into operations may leave prevention functions understaffed;
- Illness among the workforce and absences from work become an issue in terms of capacity and finding replacements to do the work;
- Ongoing investigations are halted due to lack of resources and focus;
- Budgets are reduced for any activity considered ‘non-essential’.

Significant job cuts

- In the current situation, every company is looking for savings, and one of the immediate measures is to cut jobs or reduce payments to employees. As experience has shown, for some employees this may create an incentive to commit fraud.

ILLUSTRATIVE FRAUD SCHEMES IN THE CONTEXT OF COVID-19

Asset Misappropriation

- Theft of cash;
- Larceny, e.g. warehouse theft;
- Misuse/theft of data: temptation for employees, in particular leavers, to copy sensitive data (customer lists, pricing calculations, IP theft);
- Payment of invoices without usual approvals.

Using third parties which were not fully vetted and screened:

- Collusion with disreputable third parties by some employees, for their personal benefit;
- Submitting duplicate invoices for work performed, which are not properly checked and verified by the company;
- Invoicing for work not done may not be discovered due to temporarily weakened controls;
- Paying bribes or being engaged in illegal activities on behalf of the company.

CONTROLS FAIL IN THE MAIN DUE TO A NUMBER OF (OFTEN NON-FRAUDULENT) REASONS, INCLUDING:

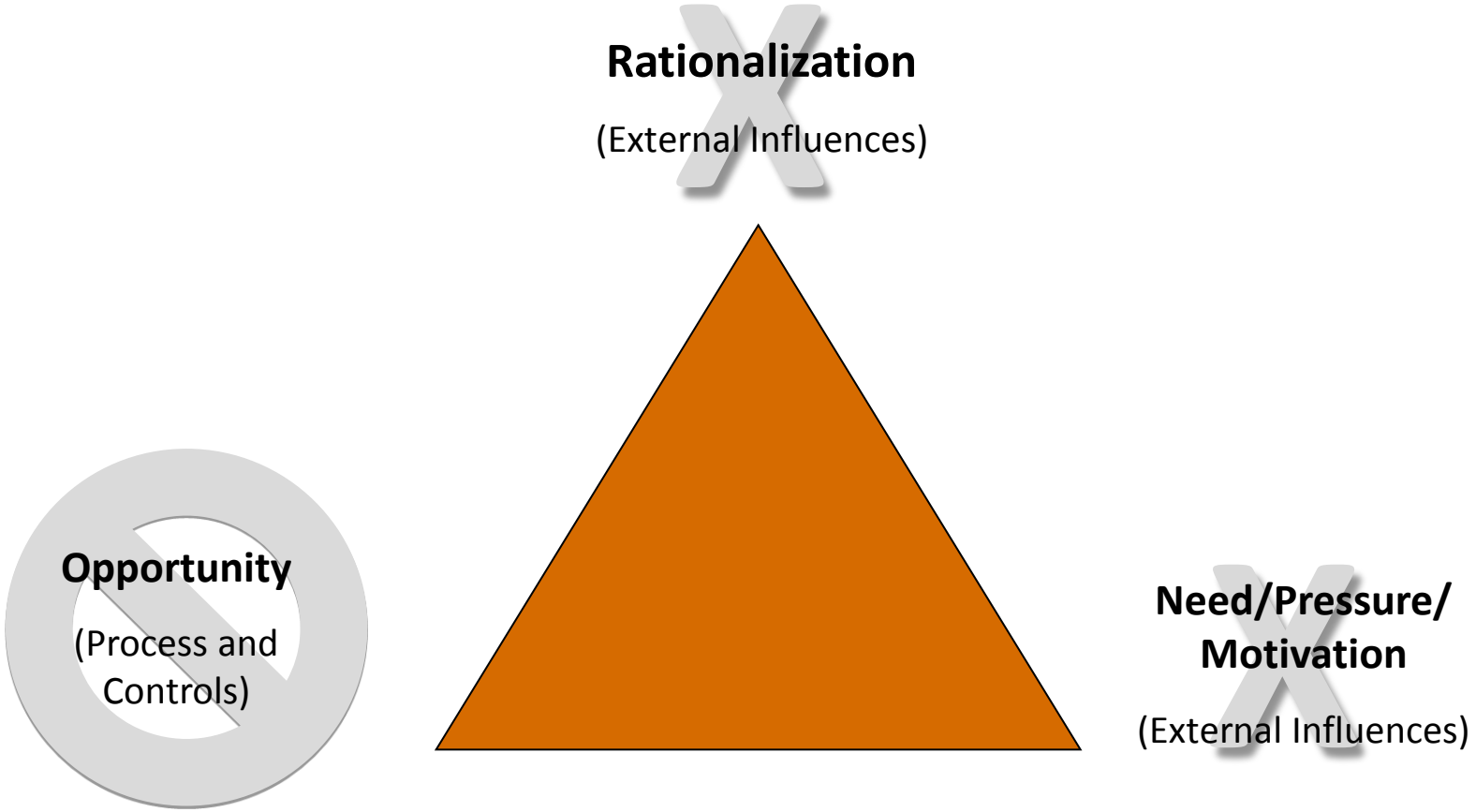
- Over-riding by management
- Poor application by staff and/or managers
- Lack of line management monitoring
- Assumptions that someone else had done it
- Indifference
- Lack of training.

Actions:

- Remind staff of their job descriptions and obligations, highlighting any controls for which they have responsibility.
- Remind staff of the need to maintain the highest levels of security while home-working. Open tabs on laptops and PCs should be closed down and laptops switched off and stored securely when not in use.
- Be cautious in dealings via email and telephone, remembering that fraudsters can hijack communications in convincing ways.
- Ensure new staff (or staff deployed to new tasks) receive the proper levels of training in applying controls and conducting checks.
- Seek corroboration and additional supporting documentation where appropriate.

Fraud Triangle

The fraud triangle is a common pictorial of the three factors that drive fraud.



Fraud Opportunity

When an organization's primary focus is on cost reduction and speed/convenience of conducting business, an environment conducive for fraud many times arises due to the combining of sensitive responsibilities and authorities within job functions.

Employee's years of service

X

Number of key responsibilities residing with the employee

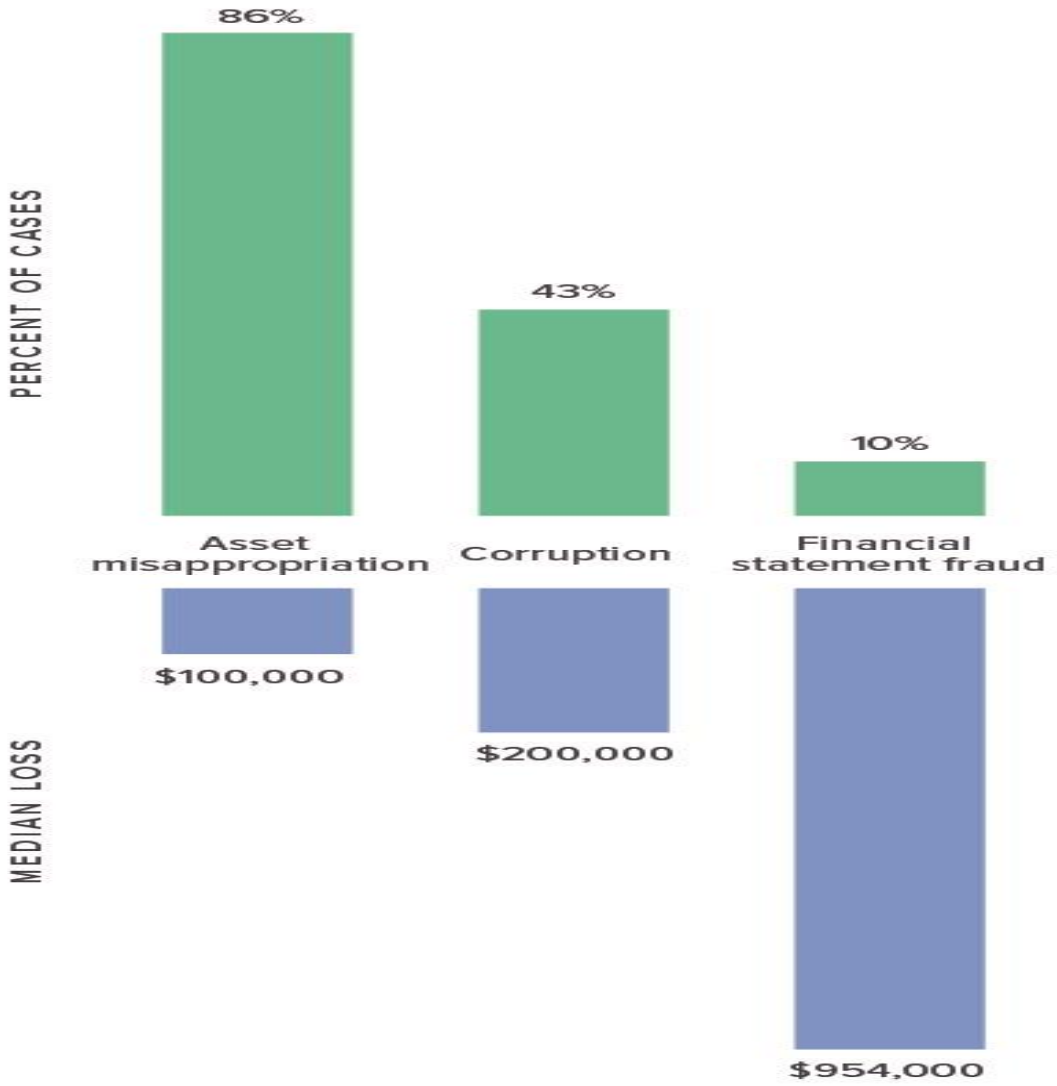
X

Organization's complacency level with respect to validating controls and monitoring activities

=

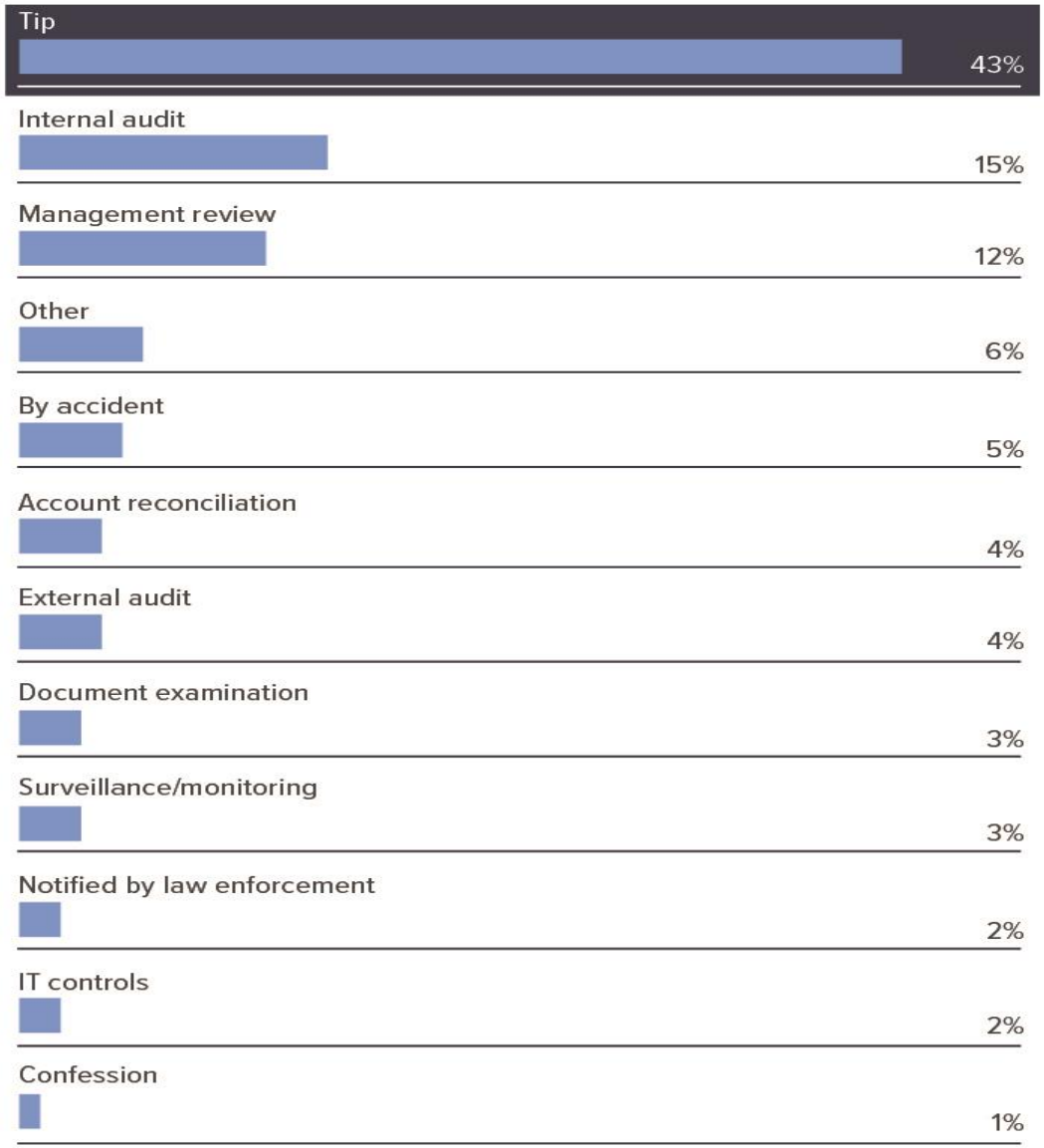
Potential for fraud to be committed

FIG. 2 **How is occupational fraud committed?**



2020 Report to the Nations

FIG. 9 **How is occupational fraud initially detected?**



2020 Report to the Nations

FIG. 27 **How does the perpetrator's level of authority relate to occupational fraud?**

2020 Report to the Nations

Fraud Risk

An organization CANNOT control individuals'

- Needs/pressures/motivations
- Rationalization

However, an organization CAN control

- **Opportunities** for fraud to be perpetrated by having the necessary **controls** and **monitoring activities** to effectively limit and/or remove opportunities

Fraud Risk Management Program Overview

Principle 1	**As part of an organization's governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the expectations of the Board of Directors and senior management regarding managing fraud risk.**
Principle 2	**Fraud risk exposure should be assessed periodically by the organization to identify specific potential schemes and events that the organization needs to mitigate.**
Principle 3	**Prevention techniques to avoid potential key fraud risk events should be established, where feasible, to mitigate possible impacts on the organization.**
Principle 4	**Detection techniques should be established to uncover fraud events when preventive measures fail or unmitigated risks are realized.**
Principle 5	**A reporting process should be in place to solicit input on potential fraud, and a coordinated approach to investigation and corrective action should be used to help ensure potential fraud is addressed appropriately and timely.**

FRM Program Components

- Commitment
- Fraud awareness training
- Affirmation process
- Conflict disclosure
- Fraud risk assessment

FRM Program Components

- Reporting procedures and whistleblower protection
- Investigation process
- Corrective action
- Process evaluation and improvement
- Continuous monitoring

Steps in Developing a Fraud Risk Management Program

1. Define program objectives.
2. Assess fraud risks.
3. Design program components.
4. Implement program components.
5. Communicate expectations
6. Ensure compliance.
7. Identify and investigate frauds
8. Measure, evaluate, and report program effectiveness

Principle 1 - Fraud Risk Program

Key Components of a Fraud Risk Program*

- Board ownership of agendas and information flow.
- Access to multiple layers of management and effective control of a whistleblower hotline.
- Independent nomination processes.
- Effective senior management team (including chief executive officer (CEO), chief financial officer, and chief operating officer) evaluations, performance management, compensation, and succession planning.
- A code of conduct specific for senior management, in addition to the organization's code of conduct.
- Strong emphasis on the board's own independent effectiveness and process through board evaluations, executive sessions, and active participation in oversight of strategic and risk mitigation efforts.

Define Program Objectives

- Tailor objectives to the organization's specific needs and goals.
- Include a clear, explicit definition of what the organization intends to accomplish.
- Weigh:
  - Management's risk appetite
  - Investment in anti-fraud controls
  - Prevention of material frauds

Every company has a different risk appetite.

- Management needs to address risk appetite in relation to fraud

Design Program Components

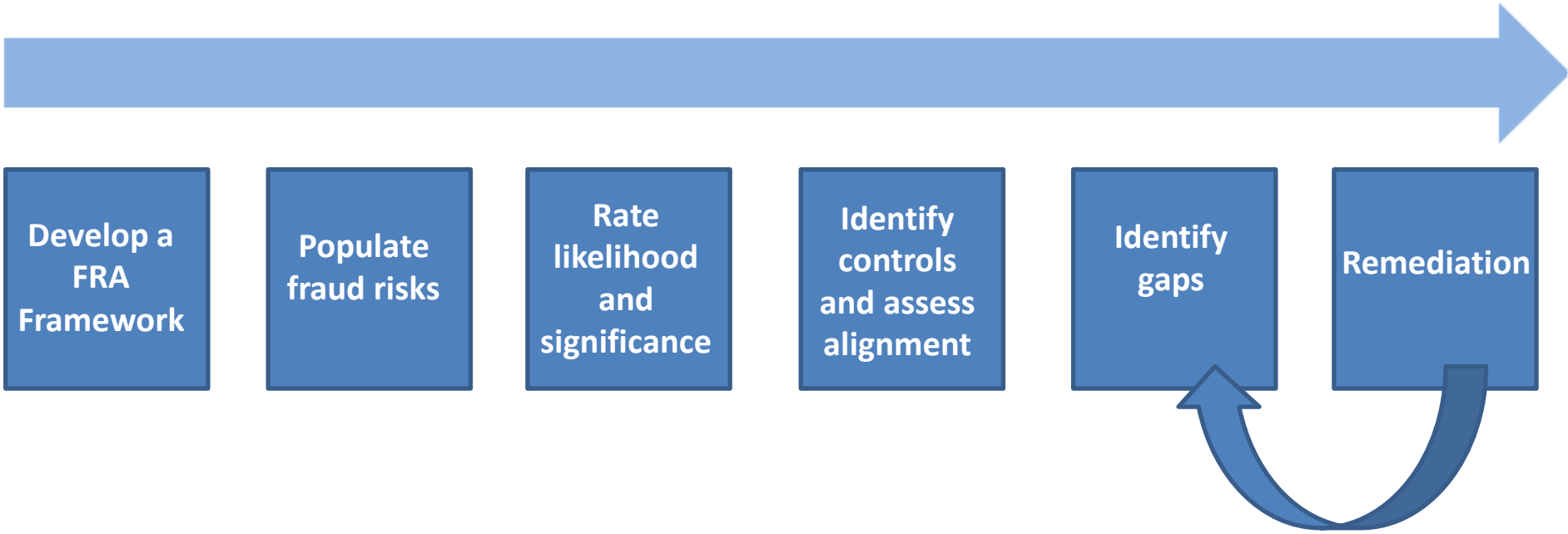
- Initiatives to increase the anti-fraud culture and tone of the organization
- Fraud prevention controls
- Fraud detection controls
- Policies, processes, and procedures for investigating and responding to fraud.

Principle 2 - Fraud Risk Assessment

Three Key Elements of a Fraud Risk Assessment*

- Identify inherent fraud risk — Gather information to obtain the population of fraud risks that could apply to the organization.
- Assess likelihood and significance of inherent fraud risk — Assess the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with staff, including business process owners.
- Respond to reasonably likely and significant inherent and residual fraud risks
- Perform a cost-benefit analysis to decide what the response should be to address the identified risks and.

Fraud Risk Assessment



Capturing Fraud Risks and Controls

Entity Level Controls

(Code of Conduct, Hiring Practices, Whistleblower Procedures)

Institutional Approach

Fraud Risks

↓

Susceptible Processes and Apps

↓

Risk Probability and Severity

↓

Controls/ Deterrents

↓

Control Gaps

↓

Remediation

Financial Statement Approach

Chart of Accounts

↓

Fraud Risks

↓

Risk Probability and Severity

↓

Susceptible Processes and Apps

↓

Controls/Deterrents

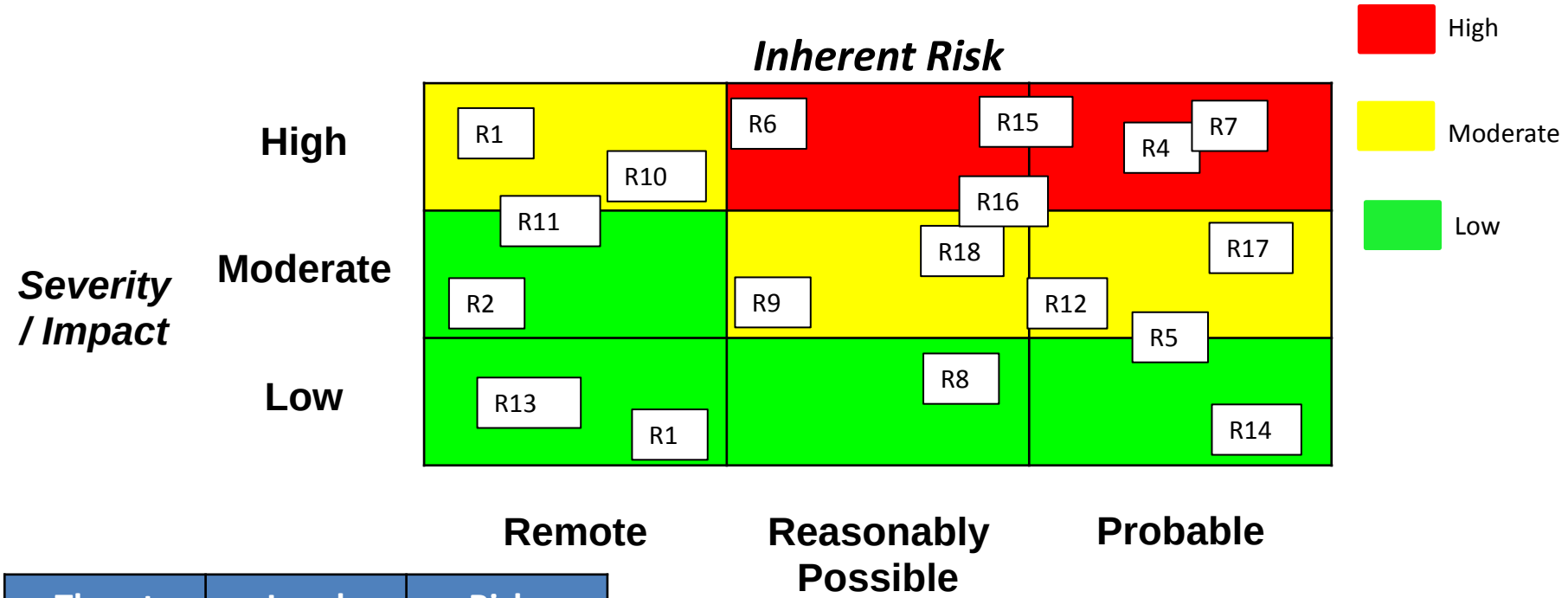
↓

Control Gaps

↓

Remediation

Fraud Risk Assessment Simplified Heat Map



Threat	Level	Risks
High		5
Moderate		8
Low		5

Activity Name	Fraud Risk Assessment
Preparer	XXXX
Preparation Date	X/X/20XX
Updated by	XXXX
Last Revision Date	X/X/20XX

Potential Fraud Risk	Examples	Susceptible Process	Fraud Type	Potential Impact/ Severity (H,M,L)	Probability of Fraud Occurrence (H,M,L)	Inherent Fraud Risk (H,M,L)	Controls to Mitigate Inherent Risk	WP REF	Residual Fraud Risk (H,M,L)	Comment / Control Gap
Improper application of GAAP	Secure credit based upon improper accounting (falsify meeting the debt	Financial Reporting	Fraudulent Financial Reporting	H	M	H	Insert Control 1 Insert Control 2		H	
Inappropriate top-sided journal entries	Manipulation of financial performance	Financial Reporting	Fraudulent Financial Reporting	H	H	H	Insert Control 1 Insert Control 2		L	
Willfully miscalculating tax liabilities	Understating tax liabilities	Financial Reporting/Procurement/ Tax	Fraudulent Financial Reporting/Corruption	H	L	L	Insert Control 1		L	
Theft fixed assets	Taking of inventory without authorization, improper disposal of fixed assets	Fixed Asset Management/Financial Reporting	Fraudulent Financial Reporting/ Misappropriation of Assets	H	L	L	Insert Control 1 Insert Control 2 Insert Control 3 Insert Control 4 Insert Control 5		L	
Embezzlement	Check kiting; forgery	Procurement	Misappropriation of Assets	M	M	M	Insert Control 1 Insert Control 2 Insert Control 3		L	
Vendor abuse	Bribery, related-party collusion, extortion, kickbacks, preferential treatment, skimming, fictitious vendor billings	Procurement/Legal	Corruption/Misappropriation of Assets	H	L	M	Insert Control 1 Insert Control 2 Insert Control 3		L	
Related party transactions	Transactions not at "arms-length"	Procurement/Legal	Corruption	H	L	L	Insert Control 1		L	
Theft of proprietary confidential information	Trade secrets and customer lists sold to a competitor	Sales Management, Production	Theft of Sensitive Data	M	H	M	Insert Control 1 Insert Control 2 Insert Control 3		L	
Use of company assets for personal gain	Using company vehicles at side-business	Fixed Asset Management	Misappropriation of Assets	M	L	L	Insert Control 1		L	
Theft from company's operating account	Fraudulent disbursements to fictitious vendors	Cash and Treasury Management/ Accounts Payable	Fraudulent Financial Reporting	H	H	H	Insert Control 1		M	
Intentional manipulation, corruption and/or destruction of data	Destruction of customer records	Data Processing	Theft of Sensitive Data	H	M	H	Insert Control 1		M	

Principle 3-4 - Prevention and Detection

Fraud Controls Types

Preventive – Intended to reduce the risk of fraud occurring to an acceptable level

Detective – Intended to flag potential risk that a fraud occurred in a timely Manner

Corrective – remedial action taken

Principle 5 - Investigation and Corrective Action

Key Components of Investigation and Response*

- Categorizing issues.
- Confirming the validity of the allegation.
- Defining the severity of the allegation.
- Escalating the issue or investigation when appropriate.
- Referring issues outside the scope of the program.
- Conducting the investigation and fact-finding.
- Resolving or closing the investigation.
- Listing types of information that should be kept confidential.
- Defining how the investigation will be documented.
- Managing and retaining documents and information.

Ensure Compliance

- Include mechanisms that monitor, identify, and address breaches in compliance.
- Designate an individual or team to monitor compliance and address noncompliance.
- Formal sanctions for intentional noncompliance must be well publicized, consistent, and firm.

Fraud Risk Management Monitoring Points of Focus

Considers a mix of ongoing and separate evaluations

Consider factors for setting the scope and frequency of evaluations

Establishes appropriate measurement criteria

Considers known fraud schemes and new cases

Evaluates, communicates, and remediates deficiencies