Conducting a fraud risk scenario assessment

Fraud Risk Scenario Assessment

In this session, we will:

- Examine a practical application of how to conduct a fraud risk scenario assessment in your business.
- Focus of assessment and approach-learn assessment methodology
- Explore areas vulnerable to fraud risk.
- Review next steps in developing an anti-fraud program.

Purpose of FRSA

- The FRSA helps management understand:-

- risks unique to its business activities
- Gaps and identify weaknesses in controls
- priorities of controls to manage those risks
- how to develop a realistic plan for targeting the right resources and controls to reduce fraud risks.

Role of Internal Audit in Fraud Risk Assessment

- IIA Performance Standard 2120

"The Internal Audit activity must evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk

(IIA Standard 2120.A2)

Role of Internal Audit in FRA

- Internal audit historically has been viewed as a controls monitoring role
- Internal audit is, however, well-placed to play a much broader and important role in all aspects of Fraud Risk management due to

❖ Audit skillsets

❖ Insights across the company

❖ Independent viewpoint

Management's role - Establish, Maintain and Evaluate Antifraud programs and controls:

1. Perform fraud risk assessment: Consider risks and vulnerabilities in their process areas
2. Create a control environment & design and implement antifraud programs and controls: programs and controls need to address both pervasive and specific risks due to fraud
3. Communicate and provide information related to antifraud programs and controls
4. Monitor the effectiveness of antifraud programs and controls:

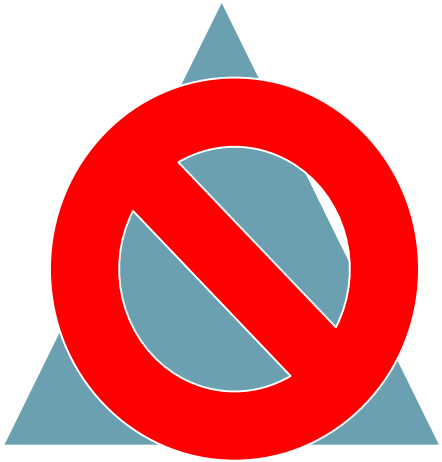
a. Test the design, implementation and operating effectiveness of antifraud programs and controls

b. Evaluate and disclose the significance of deficiencies found in testing antifraud programs and controls

c. Address identified deficiencies

Donald Cressy's Fraud Triangle

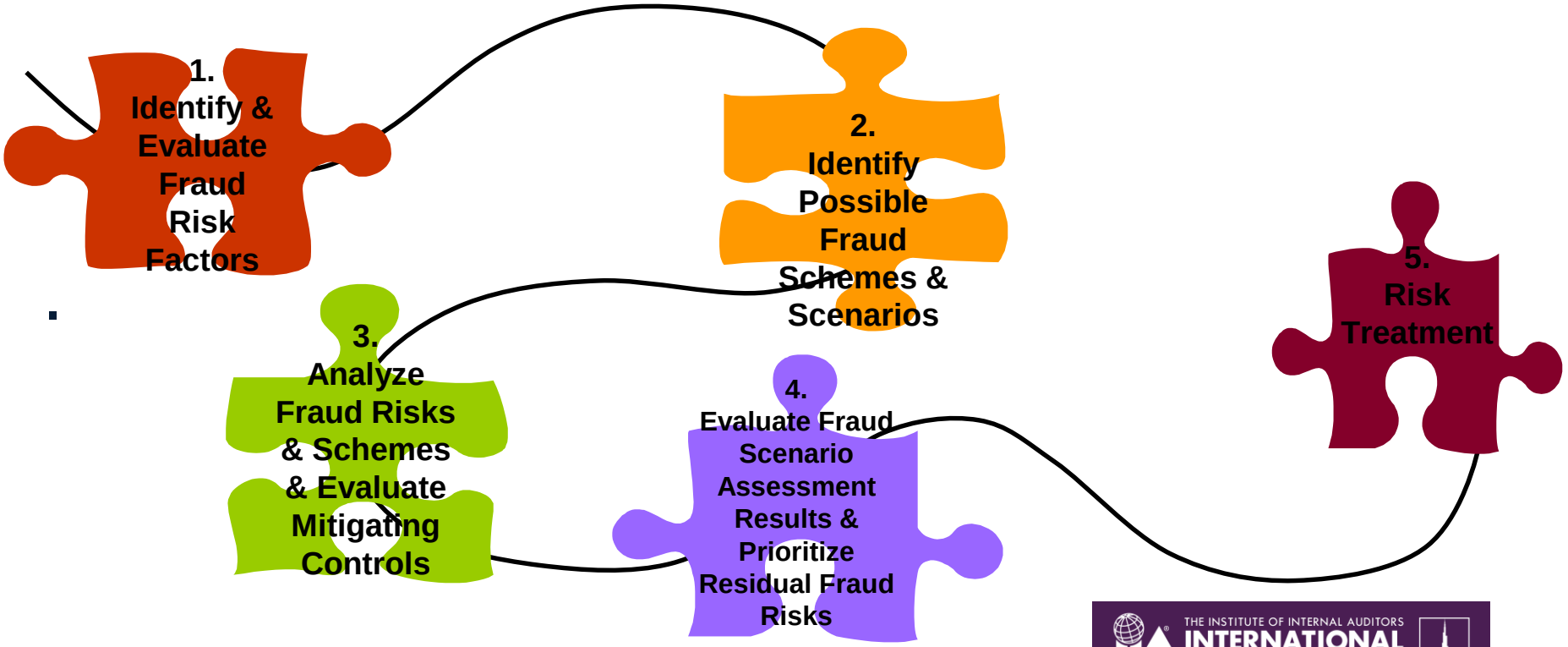
Pressure



Rationalisation

Opportunity

Methodology



1. Establish Context

- Apply top-down approach
- Assemble the right team
- Threats posing greatest fraud risk receive most attention
- Mitigate unacceptable vulnerabilities to ensure identified fraud risk do not exceed risk appetite

Phase 1 – Establish the context and identify and evaluate fraud risk factors

- Kick-off presentation with the Leadership of the organisation to appraise them of the process steps that will be conducted as part of the FRSA
- Prepare pre-read materials for Interviews and Group discussion sessions
- Conduct the Interviews with key Executives and Group Discussion Sessions
- Document interview observations and findings after each interview

2. Identify possible scenarios

- Educate the employees and openly promote the process
- Pre-book meetings with all Heads of departments within a specific timescale
- In advance of meetings, consider risks from a perspective of a fraudster !
- Have a consistent script but needs an expert ‘steer’ to ensure elicit all relevant risks and controls

Phase 2 – Identify Fraud Risk and Potential Scenarios and Schemes

- Identify and catalogue possible fraud scenarios and schemes
- Facilitate Group discussion sessions and document observations and findings
- Distribute FRSA Survey and evaluate results
- Share results with management

Conducting the exercise

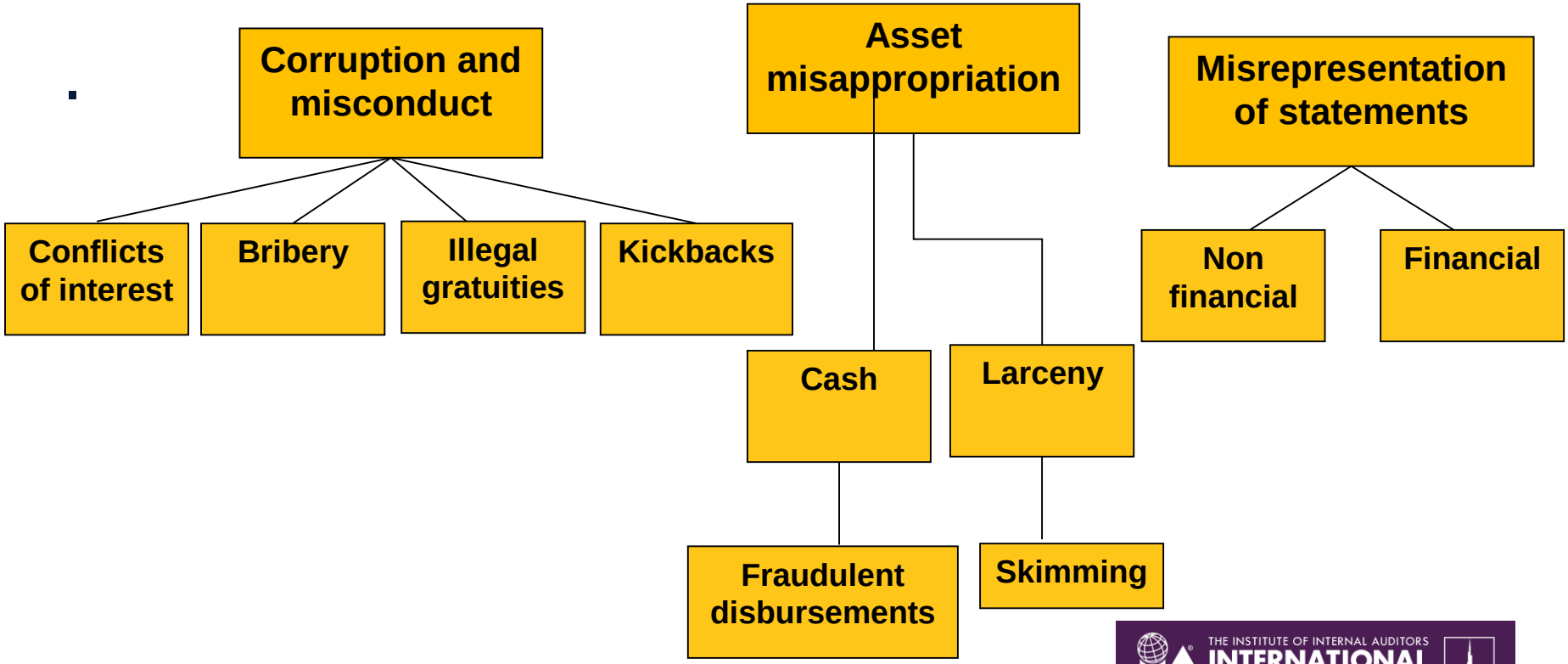
Break the business down in manageable chunks

- Process Map
- Identify Risks
- Identify Controls
- Walkthroughs
- Control Absences

Sample fraud risk assessment template

Dept	Type	Ref	Fraud Risk	Fraud Scenario	Inherent Risk- HML	Actual control/ s	Control Risk Rating	Net Rating HML

Types of fraud



Asset Misappropriation

Schemes	Potential Scenarios
Expenses	•Reimbursement for ‘lost receipts’ expenses •Reimbursement for luxury accommodation / meals •Reimbursement for travel expenses of family members
Inventory	•Theft of inventory items •Consistent shrinkage of items
Credit cards	•Reimbursement for personal expenses •Use card to circumvent competitive bid requirements
Procurement	•Payments to phantom vendors, shell companies •Manipulation of tender evaluation results
Payroll	•Payment to fictitious employee •Payment to terminated employee •Overpayment to existing employees
Information	•Confidential information theft

Bribery or corruption

Schemes	Potential Scenarios
Kickbacks	•Cash or non-cash gifts from vendors for favourable treatment •Awarding contracts based on side agreements
Competitive Bid Rigging	•Establishing criteria that gives selected vendors an unfair advantage •Purchasing in small increments to avoid the bidding process
Bribery	•Domestic or foreign bribes to avoid the bidding process •Failure to adhere to FCPA
Conflicts of interest	•Awarding contracts to parties related to individuals involved in the decision making process
Forgery or falsification of documents	•Falsification of shipping dates, contract terms, operating results •Altering or creating documents with the intent to defraud •Destruction or disappearance of records

Financial statement fraud

Schemes	Potential Scenarios
Fictitious Revenue	•Improper or early revenue recognition, Falsifying revenue •Recording pending transactions as completed transactions
Overstating assets	•Improper valuation of inventories, fixed assets
Understating liabilities and expenses	•Reclassifying (capitalizing) expenses as assets •Hiding losses in future reporting periods
Non financial	•Falsifying external documents to suppliers •Internal memorandums give misleading information •Publicly announced information provides unsubstantiated favourable results
Improper Note disclosure	•Omission of material contingencies or subsequent events
Management estimates	•Manipulation of management estimates for receivables, goodwill or depreciation

Phase 3 – Analyse of Fraud Risk and Potential Scenarios and Schemes

- Link fraud scenarios and schemes to risks and mitigating controls
- Evaluate (rate) actual control design and implementation
- Share results with management and finalize results of this phase

Likelihood

Rating	Description
1	Low probability of fraud, could occur at some point every 10 years
2	Medium probability of fraud, Might occur at some point every five years
3	High probability of fraud, expected to occur in most circumstances within the next 1 to 2 months

Consider:-

- Known instances / allegations
- Previous history
- Pervasiveness of risk across organisation

Impact

Score	Description	Examples
1	Minor consequence	Minor impact on strategy Short delay to attain key performance targets Some reputational sensitivity
2	Moderate consequence	Moderate impact on strategy Failure to attain key performance target Major reputational sensitivity Regulatory intervention/probation Resignation or dismissal or departmental manager Regional/trades media attention
3	Major consequence	Major impact on strategy Suspending key performance targets Major reputational sensitivity, service downgraded Complex litigation Criminal investigation

Identifying controls

Examples of Company wide Level Controls	Examples of Process Level Controls
Fraud Control Policy	Segregation of controls
Code of Conduct	Documents verification
Fraud Awareness Program	Access controls (financial systems / confidential data)

Control Risk Rating

1- **Control design**

- How well have the controls been designed to mitigate the Fraud Risk and Scenario?

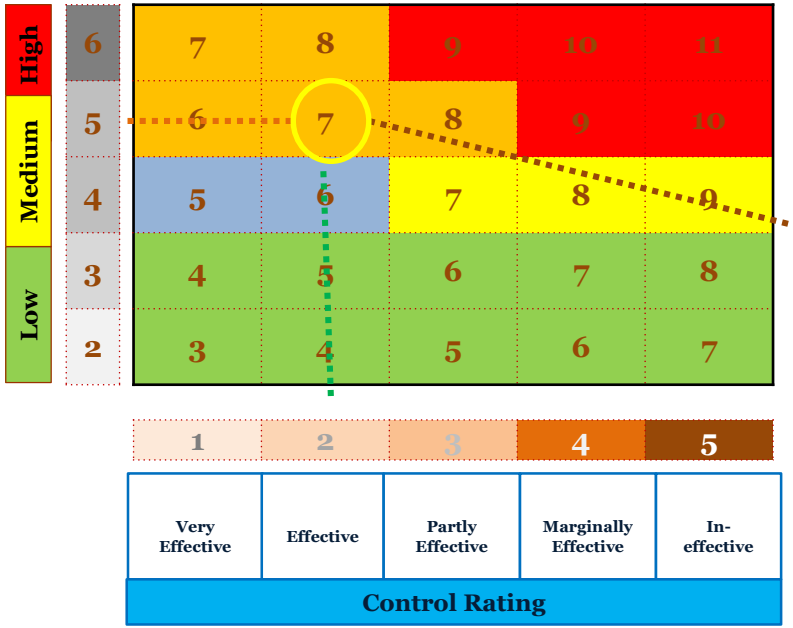
2- **Control effectiveness**

- How effective are the controls in mitigating the Fraud Risk and Scenario?

Control risk rating	Description
1	Very effective “reduces 81-100% of the risk”
2	Effective “reduces 61-80% of the risk”
3	Partly effective “reduces 41-60% of the risk”
4	Marginally effective “reduces 21-40% of the risk”
5	Not effective or no control “reduces 0-20% of the risk”

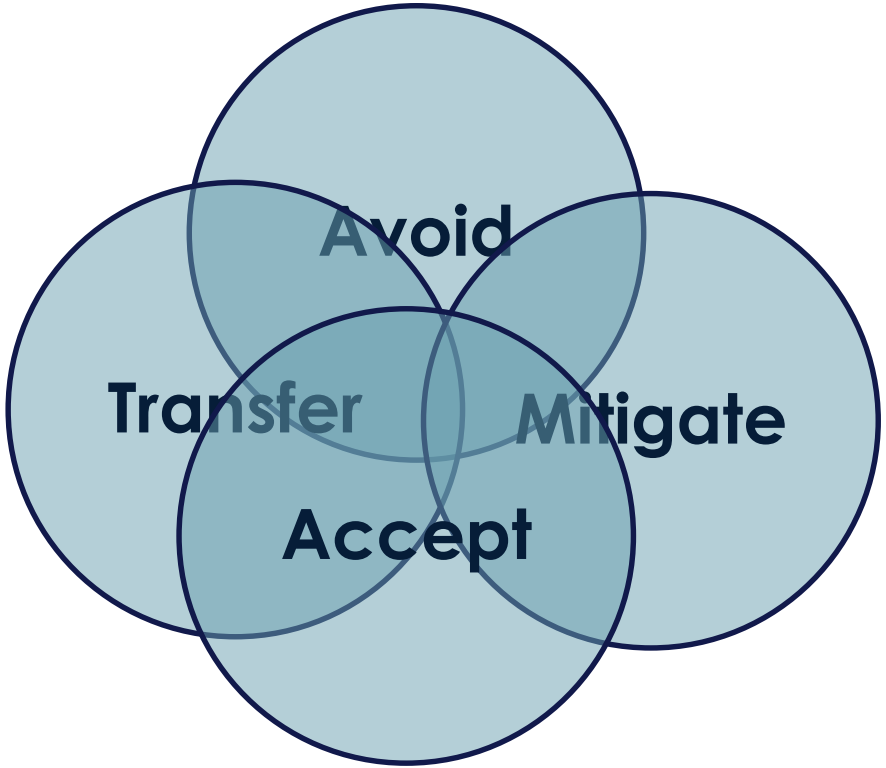
Sample assessment results matrix

Ratings shown are for EXAMPLE purposes ONLY and do not constitute results of the final assessment.



Area 1	Immediate Action Required
Area 2	Continuous Monitoring
Area 3	Action Required
Area 4	Periodic Monitoring
Area 5	No Action Required

Response to residual risks



Phase 5 – Develop Action Plan

- Upon completion of the FRSA report, the Assessment team should deliver a copy to the Audit Committee
- The Audit Committee is required to communicate to Management the areas of vulnerabilities identified
- Each business unit or department should be aware of their vulnerabilities and responsible for mitigating the respective Fraud Risks and scenarios highlighted in the FRSA report

A Robust Anti-fraud Program

- Key elements consist of:
- Code of ethics (including conflict of interest declaration and gifts declaration)
- Fraud control policy
- Whistle-blowing policy and mechanism
- Fraud risk scenario assessment
- Delegation of authority (matrix)
- Business expense policy
- Human resource policy

Benefits of Fraud Risk Scenario Assessment

- Provides a snapshot of where fraud risk may occur
- Providing structure to address the potential of fraud in a proactive manner
- Reduce exposure from fraud risk, and associated potential impact on bottom line (i.e. Financial Impact)
- Supplement the internal controls environment by helping to prevent, detect and deter fraud
- Identifies and reviews the effectiveness of key policies, guidelines and other controls used to minimise fraud in the workplace
- Help address areas of exposure in an organization where the internal controls environment may have limitations, such as collusion
- Increases the degree of employee awareness of fraud prevention risks and controls across the entity

Questions?