FRAUD RISK ASSESSMENT
GOVERNANCE, RISK AND CONTROL
CONFERENCE —
29 August 2014, Lusaka, Zambia

Nchimunya Chisuta  CFE, FCCA, FZICA
Regional Audit Director – Southern Africa, World Vision Int.
Agenda

✓ Fraud Risk Assessment
- Process of Identifying and Analysing Risks (Sample Fraud Risk Assessment tool)
- Brief background of what constitutes fraud
- Share Resources tools to utilise in fraud risk management
- Common challenges in Effective Fraud Risk Assessment

✓ Fraud Risk Exposure
IMPORTANCE OF THIS SESSION

• Effective risk assessment is increasingly Important to the success of any business

• Relationship of Fraud Risk assessment with enterprise risk management program

• Training received is a very good basis for implementing an anti-fraud programme. A trained leader/staff/Entrepreneur is an important asset

• The environment and business world we operate requires responsible persons in positions of authority to lead the way with knowledge on fraud and set the tone at the top. Examples of current statistics:
Awareness on Global Trends

Source: Global Corruption Barometer 2013

Key findings from 114,000 respondents in 107 countries:

• **Bribes:** Overall, more than one in four people (27%) report having paid a bribe in the last 12 months when interacting with key public institutions and services.

• The **police and the judiciary** are seen as the two most bribery prone. An estimated 31 per cent of people who came into contact with the police report having paid a bribe. 27% with Judiciary

• Governments are not thought to be doing enough to hold the corrupt to account

• The democratic pillars of societies are viewed as the most corrupt around the world, political parties, the driving force of democracies, are perceived to be the most corrupt institution.
Awareness on Global Trends

Source: Global Corruption Barometer 2013

- **Powerful groups** rather than the public are judged to be driving government actions. More than one in two people (54 per cent) think their government is largely or entirely run by groups acting in their own interests rather than for the benefit of the citizens.
- People state they are ready to change this status-quo in the fight against fraud. Nearly 9 in 10 surveyed say they would act against corruption.
- 53 per cent of people surveyed think that corruption has increased or increased a lot over the last two years. This was the case in Algeria, Lebanon, Portugal, Tunisia, Vanuatu and Zimbabwe, where people indicate that corruption has gotten much worse, with three out of four indicating an increase in corruption.
Awareness on Global Trends

- ACFE reports that the average total cost of fraud in a corporate org. is equivalent to 7% of the annual revenues. Failing to address these issues places an org/company at a competitive disadvantage when fraud becomes a cost of doing business.
FRAUD RISK ASSESSMENT - RESOURCES TO SHARE (www.acfe.com)

Fraud Control Policy
Fraud Risk Assessment Framework
Fraud Questionnaires
Fraud Surveys
Fraud Assessment Checklist
Fraud Risk Self Assessment Tool

NOTE: These appendix are samples. The information may or may not agree with all the concepts noted within this presentation. The material is being provided as an example that may be a used as a tool, reference, or starting point.
FRAUD RISK ASSESSMENT – What is Fraud?

• Legal Definition: A false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of what should be disclosed, that deceives and is intended to deceive so that the individual will act upon it to her or his legal injury.

• Fraud is a type of criminal activity in simple words ‘the abuse of entrusted power for gain’.

• Fraud, by definition, entails intentional misconduct, designed to evade detection. As such, a fraud risk assessment team should engage in strategic reasoning to anticipate the behaviour of a potential fraud perpetrator. ...

• Fraud falls into these 3 main categories:

***Using Game Theory and Strategic Reasoning Concepts to Prevent and Detect Fraud,” Accounting Horizons, Volume 18
Purpose of Risk Assessment

Risk assessment is intended to provide management with a view of events that could impact the achievement of objectives. It is best integrated into existing management processes and should be conducted using a top-down approach that is complemented by a bottom-up assessment process. Boards of directors—and particularly board audit committees—often request enterprise-wide risk assessments to ensure that key risks are identified and duly addressed. Such risk assessments should not be disconnected from other assessments performed within the organization. The internal audit function, for instance, may be assessing risks to plan its audits for the year. The finance function may look at similar information to perform its risk-based scoping. Business units may also be assessing risks from a business planning or performance management perspective. These individual assessments should be aligned (e.g., using common terminology, risk categories, and congruent outcomes), to cover key objectives, and be integrated to contribute to an enterprise-wide risk assessment.
Types of Risk Assessments

- **Strategic risk assessment.** Evaluation of risks relating to the organization’s mission and strategic objectives, typically performed by senior management teams in strategic planning meetings, with varying degrees of formality.

- **Operational risk assessment.** Evaluation of the risk of loss (including risks to financial performance and condition) resulting from inadequate or failed internal processes, people, and systems, or from external events.

- **Compliance risk assessment.** Evaluation of risk factors relative to the organization’s compliance obligations, considering laws and regulations, policies and procedures, ethics and business conduct standards, and contracts, as well as strategic voluntary standards and best practices to which the organization has committed. This assessment is typically performed by the compliance function with input from business areas.

- **Financial statement risk assessment.** Evaluation of risks related to a material misstatement of the organization’s financial statements through input from various parties such as the controller, internal audit, and operations.
Types of Risk Assessments - continued

- **Internal audit risk assessment.** Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives. This top-down approach enables the coverage of internal audit activities to be driven by issues that directly impact shareholder and customer value, with clear and explicit linkage to strategic drivers for the organization.

- **Market risk assessment.** Evaluation of market movements that could affect the organization’s performance or risk exposure, considering interest rate risk, currency risk, option risk, and commodity risk. This is performed by market risk specialists.

- **Credit risk assessment.** Evaluation of the potential that a borrower or counterparty will fail to meet its obligations in accordance with agreed terms. This considers credit risk inherent to the entire portfolio as well as the risk in individual credits or transactions. Conducted typically by credit analysts.
Types of Risk Assessments - Continued

• **Customer risk assessment.** Evaluation of the risk profile of customers that could potentially impact the organization’s reputation and financial position. This assessment weighs the customer’s intent, creditworthiness, affiliations, and other relevant factors. This is typically performed by account managers, using a common set of criteria and a central repository for the assessment data.

• **Product risk assessment.** Evaluation of the risk factors associated with an organization’s product, from design and development through manufacturing, distribution, use, and disposal. This assessment aims to understand not only the revenue or cost impact, but also the impact on the brand, interrelationships with other products, dependency on third parties, and other relevant factors. This type of assessment is typically performed by product management groups.
Types of Risk Assessments - Continued

• **Security risk assessment.** Evaluation of potential breaches in an organization’s physical assets and information protection and security. This considers infrastructure, applications, operations, and people, and is typically performed by an organization’s information security function.

• **Information technology risk assessment.** Evaluation of potential for technology system failures and the organization’s return on information technology investments. This assessment would consider such factors as processing capacity, access control, data protection, and cyber crime. This is typically performed by an organization’s information technology risk and governance specialists.

• **Project risk assessment.** Evaluation of the risk factors associated with the delivery or implementation of a project, considering stakeholders, dependencies, timelines, cost, and other key considerations. This is typically performed by project management teams.
What is Fraud Risk Assessment?

Fraud risk assessment is the evaluation of potential instances of fraud that could impact the organization’s ethics and compliance standards, business practice requirements, financial reporting integrity, and other objectives. This is typically performed as part of a broader organization-wide risk assessment, and involves subject matter experts from key business functions where fraud could occur (e.g., procurement, accounting, and sales) as well as forensic specialists e.g. Certified Fraud Examiners (CFEs).
FRAUD RISK ASSESSMENT

The foundation of an effective fraud risk management program should be seen as a component of a larger enterprise risk management (ERM) effort and is rooted in a risk assessment that identifies where fraud may occur and who the perpetrators might be.
FRAUD RISK ASSESSMENT

Involves asking questions such as:

• How might a fraud perpetrator exploit weaknesses in the system of controls?
• How could a perpetrator override or circumvent controls?
• What could a perpetrator do to conceal the fraud?
• What has happened in the past?
• Can we prevent it?
• Can we catch it right away?
• Can we handle it?
FRAUD RISK ASSESSMENT

Involves asking questions such as, where is fraud inherently high:

• By functional area
• By position
• By Relationship
FRAUD RISK ASSESSMENT

• The initial assessment of fraud risk should consider the inherent risk of particular frauds occurring in the absence of internal controls. After all relevant fraud risks have been identified, internal controls are mapped to the identified risks. Fraud risks that remain unaddressed by appropriate controls comprise the population of residual fraud risks.

Following this statement, note there are 3 KEY STEPS:

1. **Identify inherent fraud risk** — Gather information to obtain the population of fraud risks that could apply to the organization. Included in this process is the explicit consideration of all types of fraud schemes and scenarios; incentives, pressures, and opportunities to commit fraud; and IT fraud risks specific to the organization.
FRAUD RISK ASSESSMENT

2. 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.

3. Respond to reasonably likely and significant inherent and residual fraud risks — Decide what the response should be to address the identified risks and perform a cost-benefit analysis of fraud risks over which the organization wants to implement controls or specific fraud detection procedures.
FRAUD RISK ASSESSMENT – Framework Illustration

The framework below illustrates how the elements of fraud risk identification, assessment, and response are applied in a rational, structured approach;
## FRAUD RISK ASSESSMENT – Framework Illustration

<table>
<thead>
<tr>
<th>Identified Fraud Risk</th>
<th>Likelihood</th>
<th>Significance</th>
<th>People /Dept.</th>
<th>Existing Anti-Fraud Control</th>
<th>Control Effectiveness</th>
<th>Residual Risks</th>
<th>Fraud Risk Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inappropriate journal entries</td>
<td>Reasonably possible</td>
<td>Material</td>
<td>Finance</td>
<td>Standard monthly and quarterly journal entry log maintained. Review process in place for standard entries, and nonstandard entries subject to two levels of review</td>
<td>Tested by IA</td>
<td>Risk of override</td>
<td>Unusual Dr/CR combinations</td>
</tr>
</tbody>
</table>
## FRAUD RISK ASSESSMENT – Framework Illustration

<table>
<thead>
<tr>
<th>Identified Fraud Risk</th>
<th>Likelihood</th>
<th>Significance</th>
<th>People /Dept.</th>
<th>Existing Anti-Fraud Control</th>
<th>Control Effectiveness</th>
<th>Residual Risks</th>
<th>Fraud Risk Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intruders gaining access to the systems using default or weak passwords or stolen and reused credentials.</td>
<td>Reasonably possible</td>
<td>Material</td>
<td>ICT/All</td>
<td>Cobit 5 regular mgmt review of all password protected accounts and related privileges and ensure that all users on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable. Define and implement procedures to grant, limit and revoke access to systems, premises, buildings and restricted areas.</td>
<td>Tested by IA</td>
<td>Weak logical access control in place</td>
<td>Unauthorised access to key info</td>
</tr>
</tbody>
</table>
# FRAUD RISK ASSESSMENT – Framework Illustration

<table>
<thead>
<tr>
<th>Identified Fraud Risk</th>
<th>Likelihood</th>
<th>Significance</th>
<th>People /Dept.</th>
<th>Existing Anti-Fraud Control</th>
<th>Control Effectiveness</th>
<th>Residual Risks</th>
<th>Fraud Risk Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domineering Board members - Conflicts of interest -</td>
<td>moderate</td>
<td>Significant</td>
<td>General mgt</td>
<td>Annual conflict of interest disclosure Stringent board recruitment and selection policy and processes</td>
<td>Tested by external auditors</td>
<td>Undeclared conflict of interest Inadequate understanding of the roles of the some AC members</td>
<td>Lack of Established protocol for disclosure of potential conflicts of interest Poor tone at the top</td>
</tr>
</tbody>
</table>


Fraud Risk Assessment - Common Challenges

• Not using an Expert (in your group) to help analyse the fraud risk

  Solution: *for fraud risks by area, use subject matter experts*

• Fraud Risk Assessment Viewed as a one off episodic event with no value addition (only conducted for 2-3 years Strategic Plans)

  Solution: *Conduct and update when need arises, but at a minimum twice a year*

• Information and data is hard to use and interpret

  Solution: *Use simple, understandable terms. Review for reasonableness of implementing recommended actions for addressing residual fraud exposure*
Fraud Risk Assessment - Common Challenges

• Results of fraud risk assessment are not acted upon

**Solution:** Hold staff/process owner accountable with action plans/deadline for implementation

• Leaving the role to Risk Mgt and Compliance Unit

  **Solution:** Solicit heightened interest from all stakeholders: awareness, training, JDs

• Risk being over controlled

  **Solution:** Prioritise which controls to invest in
Fraud Risk Assessment - Common Challenges

• Too many different risk assessments are performed across the organization

• Solution: Adopt consistency approach
Fraud Risk Management Program

- Fraud risk assessment.
- Roles and responsibilities.
- Commitment.
- Fraud awareness.
- Conflict disclosure.
- Reporting & whistleblower protection.
- Investigation process.
- Corrective action.
- Continuous monitoring.

2012 Report to the Nations on Occupational Fraud and Abuse, ACFE
EFFECTIVE FRAUD RISK ASSESSMENT - AS A DITERRENT

THE LARGEST DITERRENT TO FRAUDSTERS:
Belief that they will be caught
Perception of Detection

A major reason why people commit fraud is because they are allowed to do so. The threat of fraud can come from inside or outside the organisation, but the likelihood that a fraud will be committed is greatly decreased if the potential fraudster believes that the rewards will be modest, that they will be detected or that the potential punishment will be unacceptably high.
COMPRENSIVE FRAUD EXPOSURE ANALYSIS
EFFECTIVE FRAUD HANDLING

• Response Mechanism
• Investigation
• Loss Recovery
• Effective Reporting to the Board
• External Authorities
• Publicity
• Morale and HR Concerns
INVESTIGATIVE RESOURCES

• Experienced investigators
• Forensic accounting
• Computer forensics specialists
Based on a survey by the Association of Certified Fraud Examiners (ACFE) Fraud starts small and just gets bigger and bigger, until something becomes noticeably different or unusual.
NOT ADDRESSING FRAUD

• From the pictures, it is clear that someone “responsible” is not doing his job
• Fraud starts small then grows like a cancer if left unchecked
Coachroach Theory

When you discover one coachroach, be rest assured......
...there more coach roaches hiding!
IMPACT OF SOCIAL MEDIA, EMAILS

• Need for Employers to monitor employees emails to review extent of potential to fraud/reputational risk issues; Remember all materials are sent and received via emails and ICT media using company assets;
• Defamatory materials
• Scandalous material
• Vicarious liability
• online chat rooms, social networking sites, hoax websites, fake ads etc
Syndicates

In addition to individual fraudsters, there has also been an increase in the last decade in cyber fraud being committed by gangs of organised criminals. Examples include false or stolen identities being used to defraud banks, and forms of e-fraud exploiting the use of internet by commercial businesses.

These complex syndicates have established structures (need to know basis meetings), business plans, long term vision statements, funding etc.

1. Leaders
2. Hard core established criminals
3. Organisers
4. Mules
Detection of Syndicate Crime & ID fraud

Most vulnerable departments are:

- Back office, voucher processing, ICT
- ICT department
- Globally now targeting telecoms
- Phishing emails
- Sim Swops
- Using former employees
- Reaching out to insider staff with addiction problems (loan sharks, tribal connections)
- Using applications like team viewer
- Watch out for use of Key loggers
Key loggers
“THE FUTURE DEPENDS ON WHAT WE DO IN THE PRESENT.”

- Mahatma Gandhi
QUESTIONS ?
CONTACT DETAILS

Mr. Nchimunya Chisuta

Cell: 0979-921779
Skype: nchisuta1
Email: nchisuta@yahoo.com or nchisuta1@gmail.com or nchimunya_chisuta@wvi.org