

Fraud Assessment in an Automated World

Gerry Koreman, Internal Audit, Manitoba Hydro

Geoffrey Smith, Internal Audit, Air Canada

Miguel Rueda, Fraud and Ethics Manager, Air Canada

Agenda

- Round Table Assessment and Questions
- What is Fraud?
- Fraud Statistics
- Our Obligation
- Fraud Governance and Risk Assessment
- IT Fraud Risk Assessment
- Fraud Detection Using Data Analysis
- Air Canada's Fraud and Ethics Program

Round Table Exercise

- How many have performed a formal Fraud Risk Assessment?
- Is the Fraud Risk Assessment a formal part of the annual audit plan or is fraud inherently assessed within each of audit's assigned?
- How significant is fraud considered in your organization? Preventative or Corrective?
- Who is responsible for handling fraud cases?
- Who is responsible for your whistleblower program?

What is Fraud?

“... any illegal act characterized by deceit, concealment or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage.”

Institute of Internal Auditors

ISACA'S VIEWPOINT

ISACA has a more broad definition; fraud activities are rolled under Guideline #9 – Audit Consideration for irregularities.

Not all irregularities should be considered fraudulent activities.

The determination of fraudulent activities depends on the legal definition of fraud in the jurisdiction pertaining to the audit.

Irregularities include, but are not limited to:

- deliberate circumvention of controls with the intent to conceal the perpetuation of fraud,
- unauthorised use of assets or services, and abetting or helping to conceal these types of activities.

Examples of Irregularities

- Intentional violations of established management policy
- Intentional violations of regulatory requirements
- Deliberate misstatements or omissions of information concerning the area under audit or the organisation as a whole
- Gross negligence
- Unintentional illegal acts

Fraud involves the use of deception to obtain unjust or illegal financial advantage.

Fraud Statistics

- Based on the 1,843 Certified Fraud Examiners who responded to the survey, the median response was that the average organization annually loses 5% of its revenues to fraud.
- The median loss from the 1,822 who responded to the total dollar amount lost due to fraud was \$160,000.
- 23.7% of the respondents lost \$1,000,000 and above.
- Three primary categories: Asset Misappropriation, Corruption, Financial Statement Fraud.

Association of Certified Fraud Examiners 2010 Report to the Nations

- Many of the non-profit organizations I have been involved with have been involved with at least one fraud over the years.

Our Obligation - ISACA

- ISACA Standard #9 Irregularities and Illegal Acts
- 03 – when planning and performing an audit, the auditor should consider the risk of irregularities and illegal acts.
- 04 - maintain an attitude of professional scepticism during the audit.
- 05 - When performing audit procedures the auditor should consider unusual or unexpected relationships that may indicate a risk of material misstatements.
- 11 - Auditor should communicate these matters to the appropriate level of management in a timely manner.
- 12 - If the auditor has identified a material irregularity or illegal act involving management or employees who have significant roles in internal control, the auditor should communicate these matters in a timely manner to those charged with governance.

Our Obligation

Institute of Internal Auditors

International Professional Practices Framework (IPPF):

1220.A2 – Must have sufficient knowledge to evaluate risk of fraud but are not expected expertise.

1220.A1 – Must exercise due professional care.

2060 – Chief Audit Executive must report periodically to senior management and the board. Reporting must include significant risk and exposures and control issues, including fraud risks.

2060.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and the manner in which the organization manages fraud risk.

2210.A2 – The internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

Fraud Governance and Risk Assessment

Key Principles for proactively establishing an environment to effectively manage an organization's fraud risk:

Principle 1 – Fraud risk management program, including written policy to convey expectations of the board of directors and senior management regarding managing fraud risk.

Principle 2 – Fraud risk exposure should be assessed periodically to identify specific schemes and events that the organization needs to mitigate.

Principle 3 – Prevention techniques to avoid potential key fraud risk events where feasible.

Principle 4 – Detection techniques should be established to uncover fraud events when preventative measures fail.

Principle 5 – 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 ensure potential fraud is addressed appropriately and timely.

Fraud Risk Assessment



An organization should understand fraud risk and the specific risks that directly or indirectly apply to the organization. A structured fraud risk assessment should be performed and updated periodically.

The assessment may be integrated with an overall organizational risk assessment or performed as a stand alone exercise, but should, at minimum, include risk identification, risk likelihood and significance and risk response.

Foundation of an Effective Fraud Risk Assessment



An effective fraud risk assessment program should be seen as a component of a larger enterprise risk management effort and is rooted in a risk assessment that identifies where fraud may occur and who the perpetrators might be.

Fraud Risk Assessment



Key Elements:

1. Identify Inherent Fraud Risk:

Gather information to obtain population of fraud risks and explicit consideration of all types of fraud schemes and scenarios.

This should be a brainstorming activity to identify an organization's fraud risks including an Analysis of the *Fraud Triangle*:

- **Incentive/Pressure**
- **Fraud Risk**
- **Opportunity Attitude/Rationalization**

Also consider the potential for management override of controls.

IT risks should be incorporated into an organization's overall fraud risk assessment.

Fraud Risk Assessment



Key Elements:

2. Assess likelihood and significance of inherent fraud risk

Assess the relative likelihood and potential significance of identified fraud risks.

This will be a subjective process, all fraud risks are not equally likely, nor will all frauds have a significant impact on every organization.

Consider fraud risks to the business on an inherent basis, or without consideration of known controls.

Then map to relevant controls and evaluate the significance of those residual risks and decide on the nature and extent of the preventative and detective controls and procedures to address such risks.

Fraud Risk Assessment



Key Elements:

3. Respond to Reasonably likely and significant inherent and residual fraud risks

Address the identified risks and ***perform a cost-benefit analysis of fraud risks*** where controls or specific fraud detection procedures should be placed.

The key is to be selective and efficient. There are thousands of potential controls that could be put in place.

The goal is a structured approach and efficient controls that deliver the most benefit for the cost of resources where benefits exceed the cost.

Fraud Risk Assessment Framework



See example

Improving the Flow of Information

Do not fixate on building a perfect framework. There is a substantial amount of risk information that is lost, stuck, or siloed.

- ▣ Compliance and ethics officers only receive 6% of available employee information about top risks.
- ▣ 21% - reported information relevant to top risks sits in different corporate functions.
- ▣ 60% - information reported to managers by employees likely never leave the business.
- ▣ 50% - of observed business misconduct is never reported by employees.

What I have Learned

- ▣ Discuss with Corporate Risk Manager. Where does our fraud risks lie within the Corporate Risk Map?

Should fraud be rated higher or lower within the annual audit plan?

- ▣ Discuss or survey entry level to business process owners about the likelihood and significance of fraud during the planning phase.

Do not just rely on existing audit programs.

- ▣ Document the process for re-use when we review or follow-up on audit recommendations.

IT Fraud Risks

- Access to systems or data for personal gain
- Changes to system programs or data for personal gain
- Fraudulent activity by an independent contractor or off-shore programmer
- Conflicts of interest with suppliers or third parties
- Copyright infringement

Independent Contractor Fraud

Scenario	Fraud
<p>An IT consultant under contract illegally accesses the company's computer systems .</p> <p>Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section</p>	<p>After the company declined to offer an IT contractor permanent employment, he illegally accessed the company's computer systems and caused damage by impairing the integrity and availability of data. He was indicted on federal charges, a charge that carries a maximum statutory penalty of 10 years in federal prison.</p>

Access to systems or data for personal gain

Scenario	Fraud
<p>A database analyst for a major check authorization and credit card processing company, exceeds his authorized computer access .</p> <p>Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section</p>	<p>The employee uses his computer access to unlawfully steal consumer information of 8.4 million individuals. The information stolen included names and addresses, bank account information , and credit and debit card information. He sold the data to telemarketers over a five year period. A U.S. District Judge sentenced him to 57 months' imprisonment and a \$3.2 million in restitution for conspiracy and computer fraud</p>

Access to systems or data for personal gain

Scenario	Fraud
<p>An employee in the payroll department moved to a new position. Upon switching positions, the employee's access rights were left unchanged.</p> <p>•Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI</p>	<p>Using the retained privileged access rights, the employee provided an associate with confidential information for 1,500 of the firm's employees, including 401k account numbers, credit card account numbers, and social security numbers, which was then used to commit over 100 cases of identity theft. The insider's actions caused over \$1 million in damage to the company and its employees.</p>

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
Requirements Definition	195 illegitimate drivers' licenses were created and sold by a police communications officer who accidentally discovers she can create them.	Ill-defined authentication and role-based access control requirements. Ill-defined security requirements for automated business processes. Lack of segregation of duties.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
System Design	An employee realizes there is no oversight in his company's system and business processes, so he works with organized crime to enter and profit from \$20 million in fake health insurance claims.	Insufficient attention to security details in automated workflow processes. Lack of consideration for security vulnerabilities posed by authorized system overrides.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
System Implementation	An 18-year-old former Web developer uses backdoors he inserted into his code to access his former company's network, spam its customers, alter its applications, and ultimately put the company out of business.	Lack of code reviews.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
System Maintenance	A foreign currency trader covers up losses of \$691 million over a five-year period by making unauthorized changes to the source code.	Lack of code reviews. End-user access to source code.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

IT Fraud Risk Assessment Key Elements

- Types of frauds
- Inherent risk of fraud
- Existing controls
- Control gaps
- Likelihood
- Business impact

IT Fraud Risk Assessment - Example

Business Owner-	Fraud Risks	Controls	Preventive or Detective	Monitoring	Likelihood	Impact
IT - CIO	<p>Access to systems or data for personal gain. (Logical Access)</p> <p>Access to customers' or employees' personal information (e.g., credit card information, payroll information)</p> <p>Access to confidential company information (e.g., financial reporting, supplier data, strategic plans)</p> <p>Copying and use of software or data for distribution</p>	<p>Identity management (e.g. individual user IDs, automated password complexity rules, password rotation)</p> <p>Access controls</p> <p>Authentication controls</p> <p>Authorization controls</p> <p>Access control lists</p> <p>Network controls</p> <p>Anti-virus and patch management</p> <p>Restricted access to software code</p>	Both	<p>Information security</p> <p>System administrators</p> <p>Business owners</p> <p>Internal auditing</p>	Medium	High

Fraud Detection Using Data Analytics

- **Why use data analysis?**
- **Analytical techniques**
- **Types of fraud tests**
- **Analyzing full data populations**
- **Fraud detection program strategies**
- **Fraud audit program components**

Why Data Analytics?

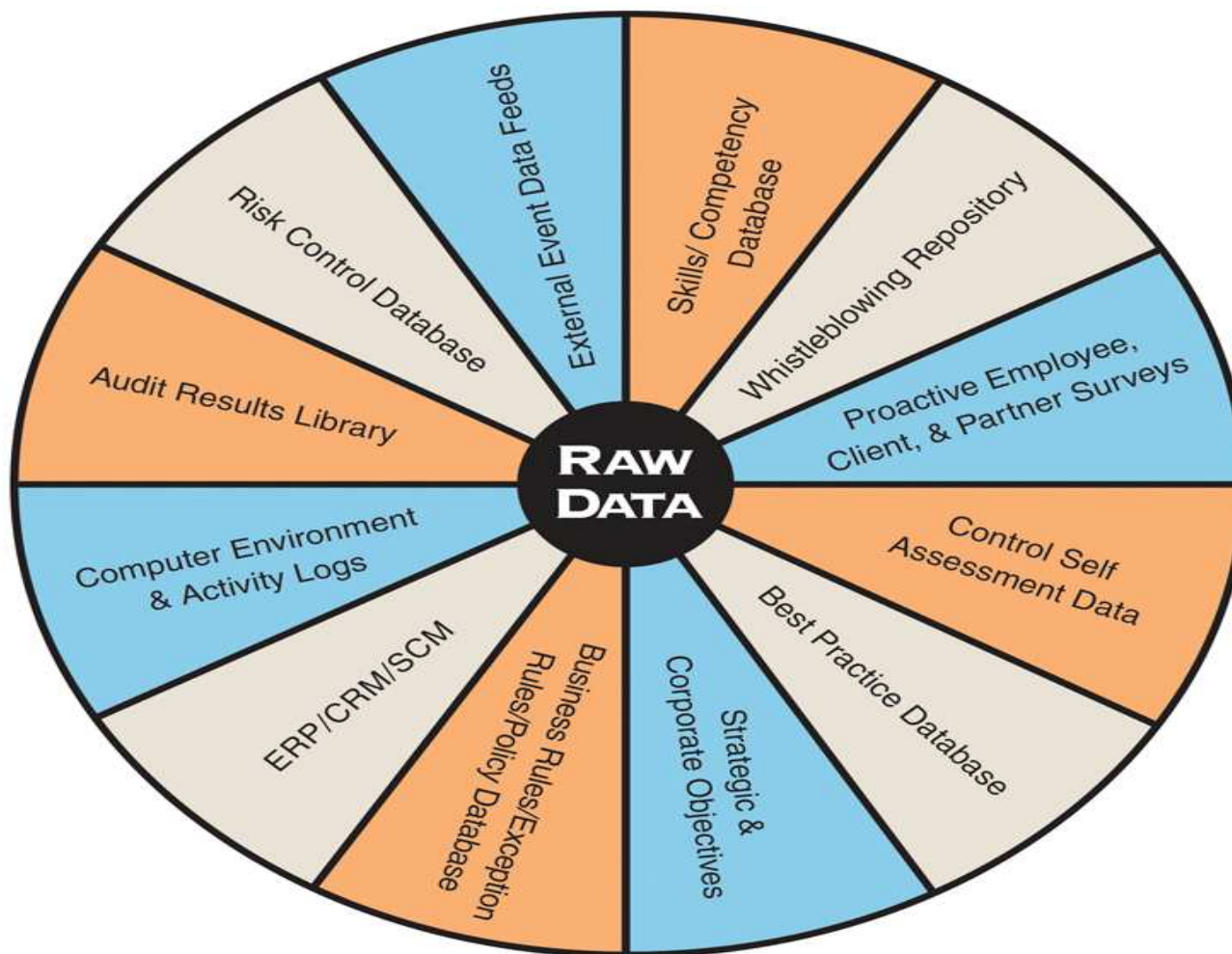
- Internal control system weaknesses
- Examine 100% of transactions
- Compare data from different applications
- Perform tests designed for fraud detection and control verification
- Automate tests in high-risk areas
- Maintain logs of analytics performed

Fraud Audit Program Components

- **Profile of potential fraud**
- **Test transactional data**
- **Implement continuous auditing and/or monitoring**
- **Review results of data testing**
- **Respond with recommendations**

IT Fraud Risk Assessments

Diversified Data Sources



IT Fraud Risk Assessments

Analytical techniques

- **Calculate statistical parameters**
- **Classify to find patterns**
- **Stratify to identify unusual values**
- **Digital analysis, to identify unlikely occurrences**
- **Joining or matching data between systems**
- **Duplicates testing**
- **Gaps testing to identify missing data**
- **Summing and totaling to check control totals that may be falsified**
- **Graphing to provide visual identification of anomalous transactions**

Application of Data Analytics in Fraud Detection

- **Accounts Payable**
- **Accounts Receivable**
- **Cash Disbursements**
- **Conflict of Interest**
- **Credit Card Management**
- **Deposits**
- **General Ledger**
- **Kickbacks**
- **Insurance claims**
- **Loans**
- **Materials**
- **Management**
- **Inventory Control**
- **Purchase Order**
- **Management**
- **Loans**
- **Salaries and Payroll**
- **Claims**
- **Vendor Management**

Types of Fraud Tests - Examples

Type	Tests used
Fictitious vendors	Run checks to uncover post office boxes used as addresses and to find any matches between vendor and employee addresses and/or phone numbers.
Altered invoices	Search for duplicates. Check for invoice amounts not matching contracts or purchase order amounts.
Duplicate invoices	Review for duplicate invoice numbers, duplicate dates, and duplicate invoice amounts.
Duplicate payments	Search for identical invoice numbers and payment amounts.
Payroll fraud	Check whether a terminated employee is still on payroll by comparing the date of termination with the pay period covered by the paycheck, and extract all pay transactions for departure date less than the date of the current pay period.

Key considerations when testing for fraud

1. **Build** a profile of potential frauds to be tested
2. **Analyze** data for possible indicators of fraud
3. **Automate** the detection process through continuous auditing/monitoring of high-risk business functions to improve controls
4. **Investigate** and drill down into emerging patterns
5. **Expand** scope and repeat as necessary
6. **Report**

Air Canada Fraud & Ethics Program

Governance

- Fraud & ethics committee
- Fraud policy
- Code of conduct
 - Definition of fraudulent activities
 - Other code violations
 - Hotline
- Air Canada Corporate Security involvement
 - Risk assessment
 - Operations & Investigations
 - Compliance & Security Management System
 - Consultation & Support
 - Liaison with government agencies

Air Canada Fraud & Ethics Program

Exposures (In order of magnitude)

- Ticketing fraud
 - Automated tool
 - Dedicated team
 - Dedicated ticket fraud email address
- Vendor fraud
- Occupational (Employee-related) fraud
- Foreign location-related fraud

Air Canada Fraud & Ethics Program

Response

- Fraud awareness
 - Acknowledgement of Code of Conduct
- Dedicated investigative corporate security team, including commercial fraud
- Coordination of fraud responses through the Fraud & Ethics committee
- Hotline
 - Use as a repository for all fraud activity
- Quarterly reporting to the Audit Committee