Deloitte.

Rebuilding trust after fraud

First 90 days

Dailene Kells

October 2, 2014 – AFOA Conference

Restoring trust when it is lost

- Some say trust can never be restored, but it can be
- Harder to overcome a loss of trust based on a violation of character than competence

Understanding different types of trust

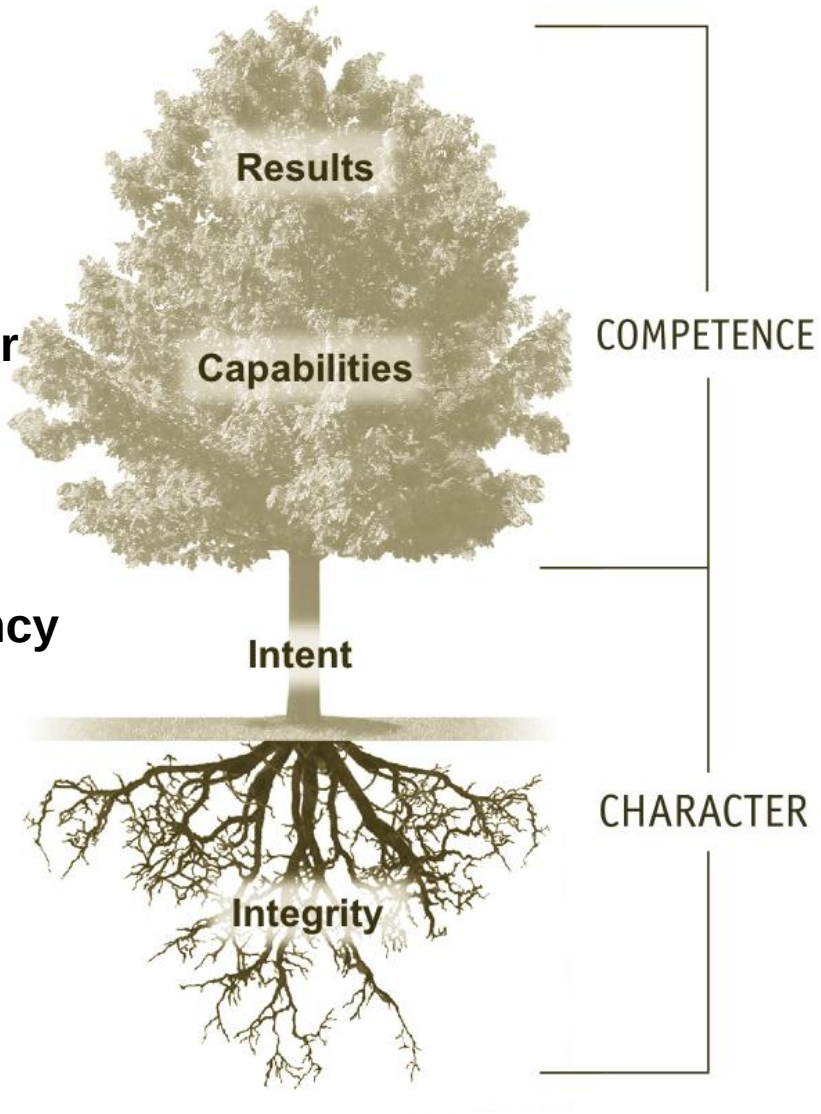
1. Self trust
2. Relationship trust
3. Inspiring trust
4. Stakeholders trust

Self trust – the individual or organization

1. Integrity
   - act according to your values?
2. Intent
   - what is your agenda?
3. Capabilities
   - are you relevant?
4. Results
   - what is your track record?

Character

Competency



Relationship trust

- Talk straight
- Demonstrate respect
- Create transparency
- Right wrongs
- Show loyalty
- Deliver results
- Get better

- Confront reality
- Clarify expectations
- Practice accountability
- Listen first
- Keep commitments
- Extend trust

Stakeholders trust

- Organizational trust – the principle of alignment
- Market trust – the principle of reputation
- Societal trust – the principle of contribution

Inspiring trust

- Extend smart trust
- Restoring trust when lost
- A propensity to trust

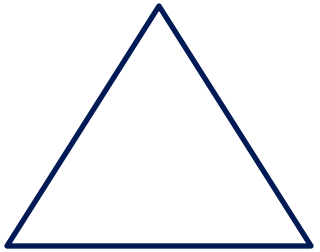
Context

What happened?

What is fraud?

Fraud is generally described in three categories:

1. Asset misappropriation
2. Fraudulent accounting and financial reporting
3. Corruption



Fraud is a behaviour that is deceptive, dishonest, corrupt or unethical. For fraud to exist there needs to be an offender, a victim and an absence of control or safeguards

Impact of fraud

- Staff morale – sense of betrayal
- Good employees do not want to work for an organization where fraud is widespread, not investigated or not acted upon
- Reputation can be damaged
- Become overly focused on the response to a fraud
- Supervisors of fraudster reputation is impacted negatively

Examples of fraud

- Ghost employees or not deleting old employees and redirecting the salary to the fraudster's bank account
- Bogus suppliers – payment going to fraudster's bank account
- Bogus purchase orders of a bona fide supplier and substitute bank account details
- Kickbacks or bribes from suppliers or contractors
- Friends of the fraudster provide services at an inflated price
- Personal use of business resources (e.g. vehicles) or personal purchases on corporate credit card
- Inflated or bogus expense claims
- Falsify time sheets (e.g. claim over time although not worked)
- Manipulate financial data to receive performance based bonuses

Start rebuilding

Move forward

Minimize the risk of fraud

- Design and implement internal controls that prevent, detect and deter most fraudulent behaviour
- Tone at the top – adhere to policies and procedures
- Have controls that are visible – built into the day to day activities – and staff are held accountable for their actions (e.g. require receipts & details) for expense claims

Move forward

- Learn from what happened
- Put in stop gaps and reduce your risks
- Communicate changes
- Be consistent
- Monitor that new processes are being followed
- Communicate to stakeholders – members, Chief & Council, staff

Move forward cont’d

Mitigating Strategies

Lead by example

- Tone at the top
- Adhere to policies and procedures
- Hold people accountable for their actions

Create a positive work environment

- Happy people – happy place
- Positive work environment encourages people to want to act in the best interests of the organization
- Positive employee recognition
- Treat staff fairly
- Have clarity in roles and responsibilities
- Clear lines of communication between management and staff

Policies and procedures

- Finalize “backbone” policies and have them approved by Chief & Council
  - Procurement (including contracts)
  - Delegation of authorities – authorized to act on behalf of the organization
  - Travel expenses
  - Human resources – hiring and dismissal (verify qualifications, reference checks, credit checks, social media scans)
  - Capital assets

- Define and communicate procedures to be followed by staff
- Should be zero tolerance of breaches and adherence to policy should form part of the conditions of employment (Code of Conduct)

Financial reports and activities

- Establish a budget
- Provide monthly reports (timely) and explain variances
- Develop comparative financials
- Regularly review financial statements
- Daily deposits (person doing the banking should be different than the one that is collecting the monies)
- Only pay on original invoices – and cancel or mark it paid when it is processed for payment
- NEVER sign blank cheques and NEVER sign or authorize payments that are not fully completed

Segregation of duties

- Review system access rights
- Review processes and assess roles and responsibilities for the flow of the transaction:
  - Who initiates the transaction?
  - Who authorizes it?
  - Who records it (enters it into system)?
  - How is it processed? (manually or in computer system)
  - Who reports it?

Create an org chart showing the reporting lines/segregation of duties

Physical access

Control physical access to premises, cash registers, computer systems, sales and other secure systems. For example:

- Ensure doors, desks and filing cabinets are locked (personnel files, cheque stock, contracts)
- Implement systems that report on employee activity, such as who has viewed and altered data in your database
- Consider installing surveillance systems (alarms, cameras)

Reconciliations

- Perform timely bank reconciliations – consider your volume of transactions
- Review for fictitious employees in payroll – periodically compare payroll employees to employee records
- Reconcile to supplier statements (if provided) – review credits noted on statement to ensure accounted for on the books
- Complete payroll reconciliation – reconcile the balance sheet accounts and payroll records monthly and look for any discrepancies

Questions

Contact information

Dailene Kells

Partner, Enterprise Risk

dkells@deloitte.ca

(306) 370-2700

Appendix
COSO Framework

2013 COSO Framework

Components	Summarized Principles
Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies relevant objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Control Environment Principles and Points of Focus

Control Environment	Points of Focus
Principle #1 Demonstrates Commitment to Integrity and Ethics	• Sets the tone at the top • Establishes standards of conduct • Evaluates adherence to standards of conduct • Addresses deviations in a timely manner
Principle #2 Exercises Oversight Responsibility	• Establishes oversight responsibilities • Applies relevant expertise • Operates independently • Provides oversight for the system of internal control
Principle #3 Establishes Structure, Authority, Responsibility	• Considers all structures of the entity • Establishes reporting lines • Defines, assigns and limits authorities and responsibilities
Principle #4 Demonstrates Commitment to Competence	• Establishes policies and practices • Evaluates competence and addresses shortcomings • Attracts, develops, and retains individuals • Plans and prepares for succession
Principle #5 Enforces Accountability	• Through structures, authorities, and responsibilities • Establishes performance measures, incentives and rewards and evaluates for ongoing relevance • Considers excessive pressures • Evaluates performance

Risk Assessment Principles and Points of Focus

Risk Assessment	Points of Focus
Principle #6 Specify suitable objectives to enable identification and assessment of risk	• Reflects management's choices • Considers tolerances for risk • Includes operations and financial performance goals • Basis for committing of resources
External Financial Reporting Objectives	• Complies with applicable accounting standards • Considers materiality • Reflects entity activities
External Non-Financial Reporting Objectives	• Complies with externally established Standards and Frameworks • Considers the required level of precision • Reflects entity activities
Internal Reporting Objectives	• Reflects management's choices • Considers the required level of precision • Reflects entity activities
Compliance Objectives	• Reflects external laws and regulations • Considers tolerance for risk

Risk Assessment Principles and Points of Focus (cont'd)

Risk Assessment	Points of Focus
Principle #7 Identifies and Analyzes Risk	• Includes entity, subsidiary, division, operating, and functional levels • Analyzes internal and external factors • Involves appropriate levels of management • Estimates significance of risks identified • Determines how to respond to risks
Principle #8 Assesses Fraud Risk	• Considers various types of fraud • Assesses incentive and pressures • Assesses opportunities • Assesses attitudes and rationalizations
Principle #9 Identifies and Analyzes Significant Change	• Assesses changes in external environment • Assesses changes in business model • Assesses changes in leadership

Control Activities Principles and Points of Focus

Control Activities	Points of Focus
Principle #10 Selects and Develops Control Activities to Mitigate Risks	• Integrates with risk assessment • Considers entity-specific factors • Determines relevant business processes • Evaluates a mix of control activity types • Considers at what level activities are applied • Addresses segregation of duties
Principle #11 Selects and Develops General Controls over Technology	• Determines dependency between the use of technology in business processes and technology general controls • Establishes relevant technology infrastructure control activities • Establishes relevant security management process control activities • Establishes relevant technology acquisition, development and maintenance process control activities
Principle #12 Deploys through Policies and Procedures	• Establishes policies and procedures to support deployment of management's directives • Establishes responsibility and accountability for executing policies and procedures • Performs in a timely manner • Takes corrective action • Performs using competent personnel • Reassesses policies and procedures

Information & Communication Principles and Points of Focus

Information and Communication	Points of Focus
Principle #13 Uses Relevant Information	• Identifies information requirements • Captures internal and external sources of data • Processes relevant data into information • Maintains quality throughout processing • Considers costs and benefits
Principle #14 Communicates Internally	• Communicates internal control information • Communicates with the board of directors • Provides separate communication lines • Selects relevant method of communication
Principle #15 Communicates Externally	• Communicates to external parties • Enables inbound communications • Communicates with the board of directors • Provides separate communication lines • Selects relevant method of communication

Monitoring Activities Principles and Points of Focus

Monitoring Activities	Points of Focus
Principle #16 Conducts Ongoing and/or Separate Evaluations	• Considers a mix of ongoing and separate evaluations • Considers rate of change • Establishes baseline understanding • Uses knowledgeable personnel • Integrates with business processes • Adjusts scope and frequency • Objectively evaluates
Principle #17 Evaluates and Communicates Deficiencies	• Assesses results • Communicates deficiencies • Monitors corrective actions

Deloitte.