Good Governance

CAUBO 2016

Overview

1. Governance
2. Fraud
3. IT Security
4. Considerations for the Board
5. Questions

Governance Landscape

Increased focus on governance – Why?

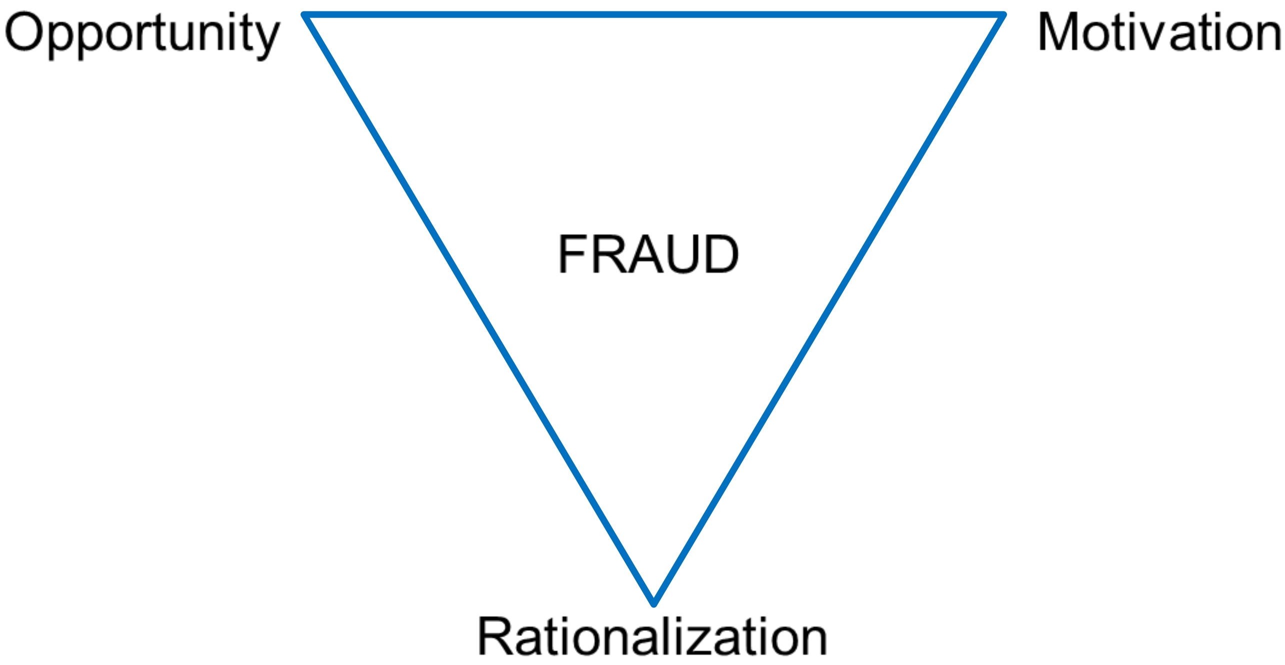
- Trust is at a historic low for Not for Profit organizations and Charities
- Post-secondary sector under great financial stress, now recognized as endemic and long-lasting
- Concerns and activism by faculty members and students
- Decentralization
- Faculty members in positions of financial oversight

Governance Landscape

What is “good governance”?

- Boards taking greater interest in the success of an institution
- Boards taking their role as governors more seriously
- Governance is now a professional competency, taught by business schools
- Requires hard and supported choices

The Fraud Triangle



Opportunity

Motivation

FRAUD

Rationalization

Characteristics and Red Flags

- Living beyond means
- Addictions
- Aggressive personality
- “Wheeler-Dealer”
- Lack of policies and procedures (formal or informal)

Headlines

1. Lavish spending by the Secretary of an institution who took excessive vacations and earned millions for outside work.
2. Allegation against an faculty member for misuse of university resources to benefit his passion in the opera.
3. Financial aid and student visa fraud allegations against 3 senior executives for generating $7.4M in illegal revenues.

Statistics and Current Trends

- Top three of the most common fraud:
  - Theft of Physical assets (22%)
  - Vendor, supplier or procurement fraud (17%)
  - Information theft (15%)
- Threat from Within
- Cyber Security

Unique challenges for Academic Institutions

1. Academia
    - Skillset and mindset
2. Culture of collegiality
    - Trust
3. Decentralized authority

Challenges for Fraud Investigations

1. Consideration of publicity and confidentiality
2. Appropriate policies and procedures
3. Privacy confidentiality concerns
4. Lack of supporting documents and evidentiary support
5. Labour relations issues

Good Governance Practice

1. Encourage strong ethical culture in organization

2. Ensure compliance with organization’s business practices

3. Mitigate potential for certain adverse events

   - Fraud and cyber incidents

   - Financial losses and reputational impact

Good Governance Practice

- Role of the Audit Committee
- “Whistleblower” hotline and safe disclosure
- Other fraud prevention processes and controls
- Fraud risk assessment

Fraud Risk Assessment

Why?

- Proactively manage the risk of fraud

How?

- Define a fraud universe
- Identify potential fraud schemes
- Assess the fraud risk (likelihood and impact)
- For the top fraud risks, identify existing controls and potential gaps

Fraud Risk Assessment

Outcomes:

- Prevention

  Through process enhancements, improved oversight

- Early Detection

  Through an improved, focused audit program

- Fraud awareness

Information is a Key Asset

- Value
- Vulnerability
- Information vs Systems

Headlines

- U.S. judge certifies class action over Target Corp data breach (Sep 2015)
- Heartbleed Remains a Risk 2 Years After It Was Reported (Apr 2014)
- Who hacked Ashley Madison and why? (July 2015)

IT Security Governance

“To Achieve effectiveness and sustainability in today’s complex, interconnected world, information security must be addressed at the HIGHEST LEVELS of the organization, not regarded as a technical specialty relegated to the IT department”

IT Governance Institute

Guidance for Boards of Directors and Executive Management

Governance vs Management

Governance	Management
Oversight	Implementation
Authorizes decision rights	Makes decisions
Enact policy	Enforces policy
Accountability	Responsibility
Strategic Planning	Project Planning
Resource allocation	Resource utilization

Governance Models

- International – ISO 27001/2
- United States – NIST (National Institute of Standards and Technology)
- Challenges of applying these models in the University setting

Governance Fundamentals

Duty of Care

- Protect critical assets
- Protect market share
- Govern employee conduct
- Protect reputation
- Ensure compliance requirements are met

Effective IT Security Governance

- Institution-wide
- Risk-based
- Defined roles and responsibilities
- Sufficient resources committed (aligned with strategies)
- Strong policy framework
- Staff training and awareness programs
- Reviews and audits

Internal Audit of IT Security – why?

- High level of risk
- Identification of areas for improvement
- Management engagement
- Improved governance and Board awareness

Five Principles that Boards should consider about IT Security

1. Enterprise-wide risk, not “just an IT issue”
2. Board members set expectations with management
3. Legal implications
4. Regular and adequate time on the Board agenda
5. Discussion of IT Security risks and how they are avoided, accepted, mitigated or transferred

Considerations for the Board

- Create a game plan with scenarios
- Educate and communicate to Board (audit/executives) early, often, thoughtfully
- Plan to manage expectations on mitigation and recovery
- Have a media or public relations plan for communication
- Don’t be defensive, arrange for extra support or expert backup

Questions ?