Leading Edge Practices in Fraud Risk Governance

Higher Education

University of California – Office of the President

Pamela Verick, Director
Investigations & Fraud Risk Management
December 4, 2014

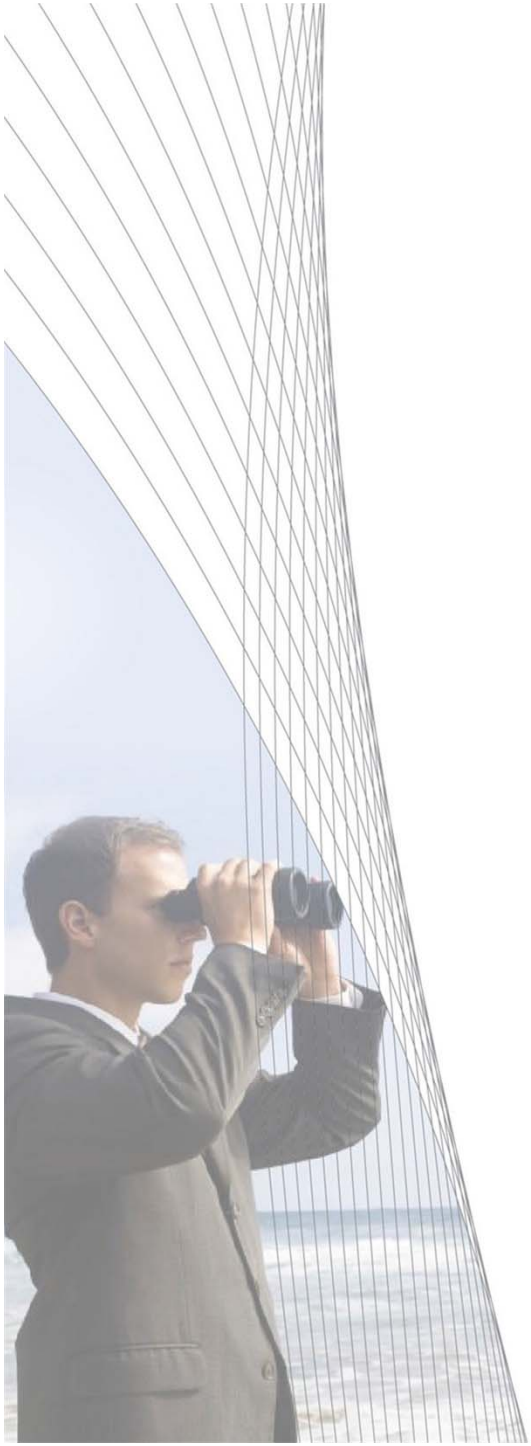
Powerful Insights.
Proven Delivery.®

protiviti®
Risk & Business Consulting.
Internal Audit.

Today's Learning Objectives

- What's in focus for Boards and Senior Management
- Discuss concept of organizational "fraud philosophy"
- Understand roles and responsibilities for fraud risk management
- Communicate key components of fraud control policy
- COSO 2013 – Principle 8

protiviti®



Powerful Insights.
Proven Delivery.®

What's in Focus?

protiviti®

What's Trending with Boards and Senior Management

1. Understanding how companies are defending against Cyber Crime
2. Considering impact of the Fraud Principle (COSO 2013)
3. Thinking about roles and responsibilities for fraud risk management
4. Reviewing framework for internal investigation activities
5. Requesting anti-corruption compliance audits

protiviti®

2014 Report to the Nations on Occupational Fraud and Abuse

Highlights - Education

80 cases (5.9% of cases reviewed in *Global Fraud Study*)

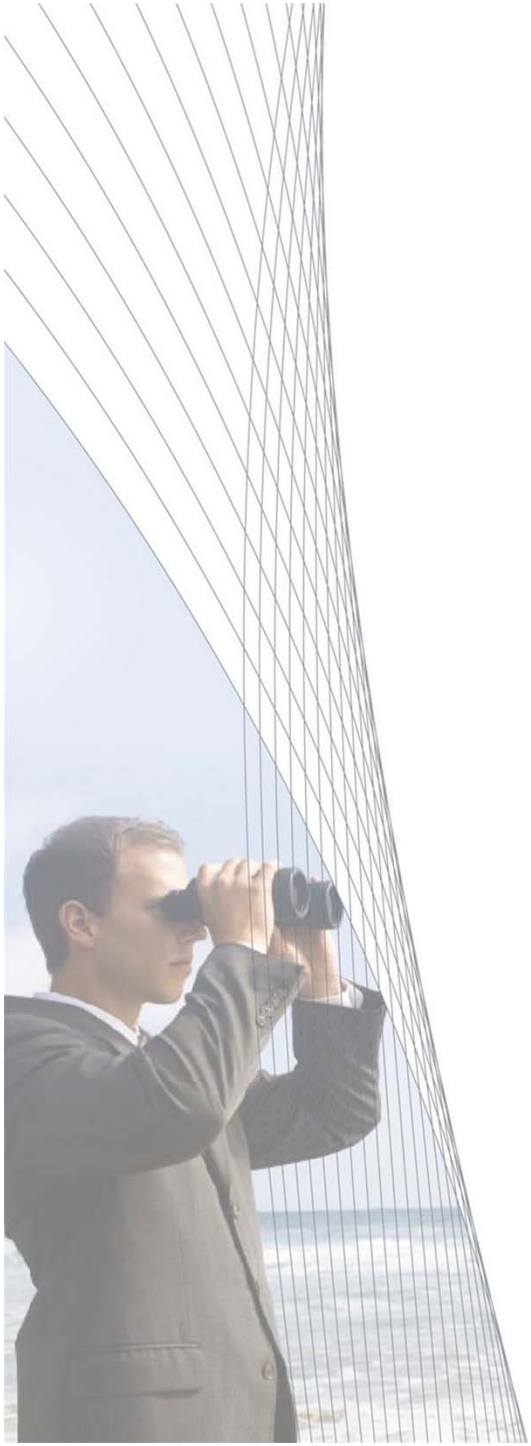
$58,000 (median loss)

Corruption (36.3%)

Billing Schemes (33.8%)

Expense Reimbursement Schemes (31.3%)

protiviti®



Powerful Insights.
Proven Delivery.®

Fraud Risk Governance

As part of an organization's governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding fraud risk.

- ***Managing the Business Risk of Fraud***
ACFE, IIA and AICPA, 2008

protiviti®

What is Fraud Risk Governance? (1/6)

Fraud Risk Governance

May be defined in a variety of ways….

- The system by which organizations control fraud risk.
- Process by which organizations are responsive to fraud risk.
- Manner in which management and those charged with oversight and accountability meet their fiduciary duties to address fraud risk.

protiviti®

What is Fraud Risk Governance? (2/6)

Managing the Business Risk of Fraud (AICPA, IIA and ACFE)

Role of Board of Directors

- Understand fraud risks
- Maintain oversight of fraud risk assessment
- Monitor reports on fraud risks, policies and control activities
- Oversee internal controls established by management
- Retain outside experts if needed
- Set appropriate tone at the top through CEO job description, hiring, evaluation, and succession-planning processes
- Ability to retain and pay outside experts where needed
- Provide external auditors with evidence regarding Board's active involvement and concern about fraud risk management

protiviti®

What is Fraud Risk Governance? (3/6)

Managing the Business Risk of Fraud (AICPA, IIA and ACFE)

Role of Audit Committee

- Independent board members, with one financial expert
- Active role in oversight of fraud risk assessment
- Use of Internal Audit or other designate to monitor fraud risk
- Discuss external auditors' planned approach to fraud detection
- As part of Audit Committee meetings, discuss (apart from management) how internal and external audit strategies address fraud risk
- Open and candid dialogue with external auditors regarding knowledge of fraud or suspected fraud
- Seek legal guidance in dealing with allegations involving fraud
- Alert to reputation risk stemming from fraud

protiviti®

What is Fraud Risk Governance? (4/6)

Managing the Business Risk of Fraud (AICPA, IIA and ACFE)

Role of Management

- Set tone within organizational culture
- Implement adequate internal controls
  - Documentation and evaluation of fraud risk management policies and procedures
- Regular reports to Board on actions taken to manage fraud risk
- In many organizations, one executive-level management member responsible for fraud risk management / reports to Board

protiviti®

What is Fraud Risk Governance? (5/6)

Managing the Business Risk of Fraud (AICPA, IIA and ACFE)

Role of Internal Audit

- Provide assurance to Board and management that controls are appropriate given:
  - Organization's fraud risk appetite
  - Identified fraud risk
- Review adequacy of risks identified by management (especially management override of control)
  - Comprehensiveness
  - Adequacy
- Consider organization's fraud risk assessment when developing Internal Audit plan

protiviti®

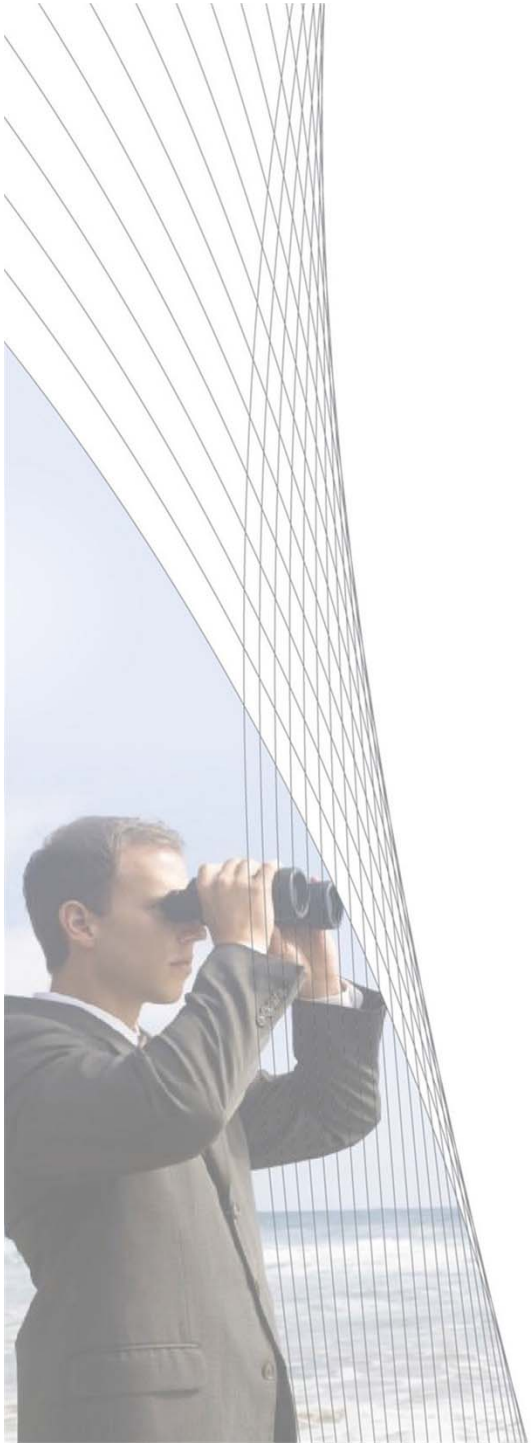
What is Fraud Risk Governance? (6/6)

Managing the Business Risk of Fraud (AICPA, IIA and ACFE)

Role of Staff

- Basic understanding of fraud
- Be aware of red flags
- Have an understanding of:
  - Roles
  - How job procedures are designed to manage fraud risk
  - Implications of non-compliance that may hamper fraud detection
- Read and understand policies and procedures
- Process participation (as necessary)
  - Strong control environment
  - Design and implementation of fraud control activities
  - Monitoring activities
- Report suspicious behavior or incidences of fraud
- Cooperate in investigations

protiviti®



Powerful Insights.
Proven Delivery.®

Fraud Philosophy

protiviti®

“Fraud Philosophy” (1/2)

***Attitudes** that inform an organization’s fraud philosophy:*

protiviti®

“Fraud Philosophy” (2/2)

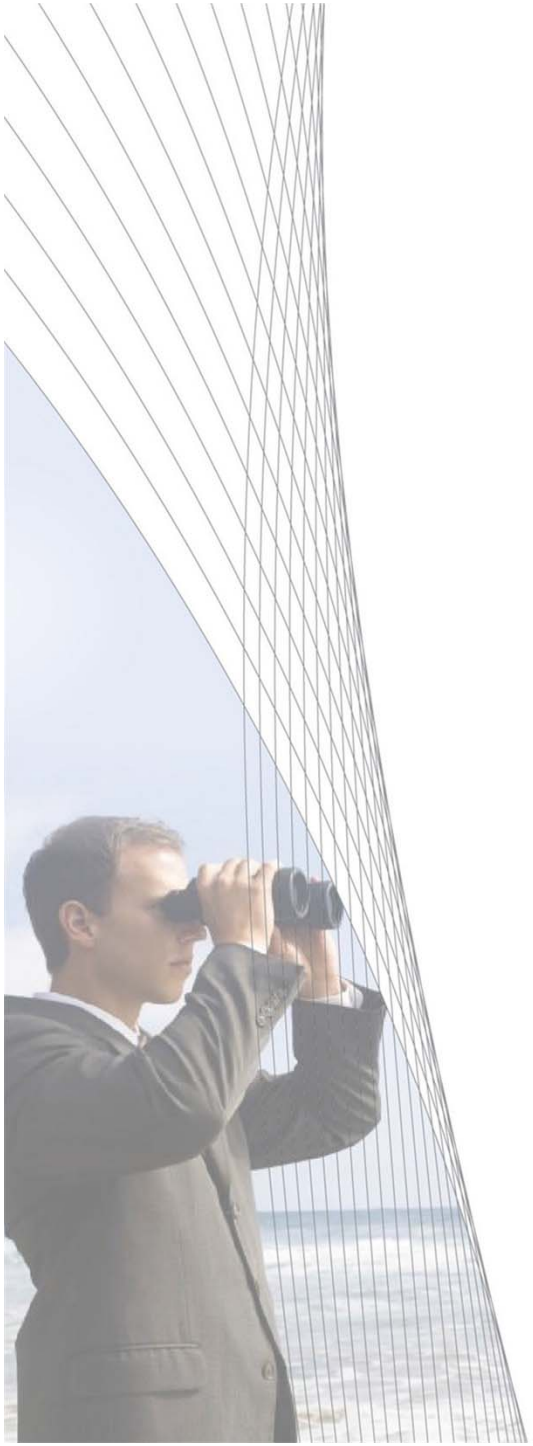
***Behaviors** that inform an organization’s fraud philosophy:*

- Ignoring red flags
- Failure to investigate concerns or complaints
- Lack of disciplinary action
- Recycling employees after a fraud risk event
- “Slow to no” remediation activity

Fraud Philosophy

“the most basic beliefs, concepts, and attitudes of an individual or group about fraud”

protiviti®



Powerful Insights.
Proven Delivery.®

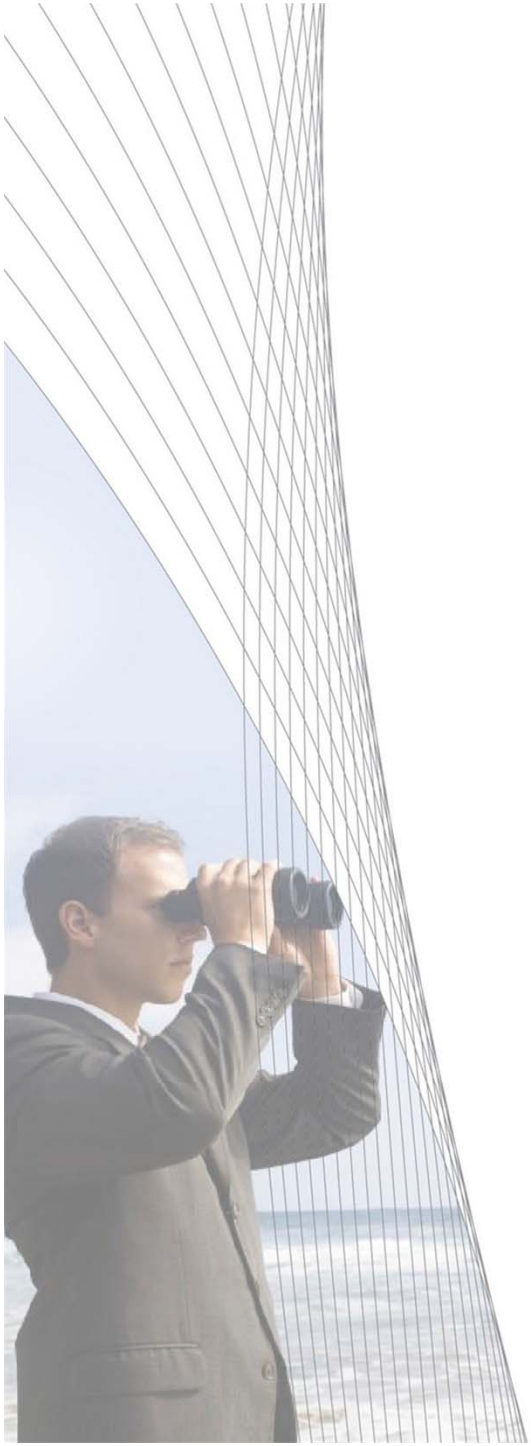
Fraud Control Policy

protiviti®

Fraud Control Policy

- Robust document that addresses an organization's approach to fraud risk management
- Components may include (but are not limited) to the following:
  - Executive summary/scope
  - Definition of fraud
  - Roles and responsibilities
  - Fraud control strategies
  - Fraud risk assessment
  - Reporting mechanisms and protocols
  - Conflicts of interest
  - Investigation protocols
  - Disciplinary action
  - Periodic and continuous monitoring
  - Quality assurance review

protiviti®



Powerful Insights.
Proven Delivery.®

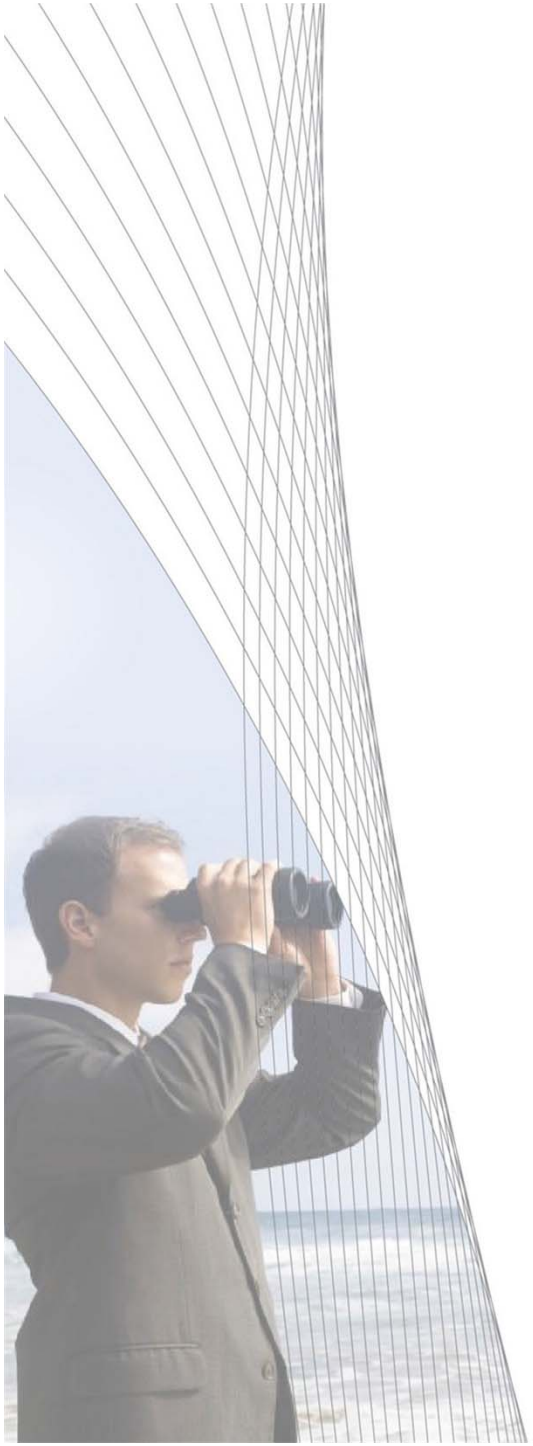
Investigation Policy

protiviti®

Investigation Policy

- Robust document that addresses an organization's approach to investigations
- Components may include (but are not limited to) the following:
  - Policy statement
  - Definitions
  - Receipt of concerns, complaints and reported violations
  - Retention of concerns, complaints and reported violations
  - Response to concerns, complaints and reported violations
  - Roles and responsibilities for investigation
  - Investigation protocols
  - Documentation of investigation
  - Corrective action
  - Investigation conclusion and feedback

protiviti®



Powerful Insights.
Proven Delivery.®

COSO 2013
Principle 8 (a/k/a “The Fraud Principle”)

protiviti®

What's Driving Today's Fraud Risk Assessment Activities?

COSO Internal Control – Integrated Framework – Principle 8 (May 2013)

The organization considers the potential for fraud in assessing risks to the achievement of objectives. This includes management's assessment of the "risks relating to the fraudulent reporting and safeguarding of the entity's assets," along with "possible acts of corruption" by entity personnel and outsourced service providers.

IIA Standard 2120.A2 (January 2009)

The internal audit activity must evaluate the potential for the occurrence for fraud and how the organization manages fraud risk.

Managing the Business Risk of Fraud: A Practical Guide (July 2008)

Non-binding guidance on topic of fraud risk management issued in collaboration between IIA, AICPA and ACFE. Includes consideration of fraud risk assessment.

IIA Standard 1210.A2 (revised January 2009)

Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

protiviti®

Fraud Principle 8

Key Driver in Today's Look at Fraud Risk Governance

- Many organizations have integrated their assessment of fraud risks and controls with their ICFR assessment
- Approach to addressing will depend on how effectively the organization has considered and documented fraud risk in the past
- For those that have documented controls to address common fraud scenarios, this could be incorporated into the mapping:
  - **Inventory elements of the anti-fraud program currently in place**
  - **Document an overall summary of significant fraud risks and how they are addressed through the anti-fraud program**
- Reconsider if the existing anti-fraud program is robust enough

2013 COSO Internal Control Integrated Framework

- **Considers various types of fraud**
- **Assesses incentives and pressures**
- **Assesses opportunities**
- **Assesses attitudes and rationalizations**

protiviti®

COSO 2013 - Fraud Principle 8

Types of Fraud

Fraudulent reporting – occurs when an organization's reports are intentionally prepared with omissions or misstatements.

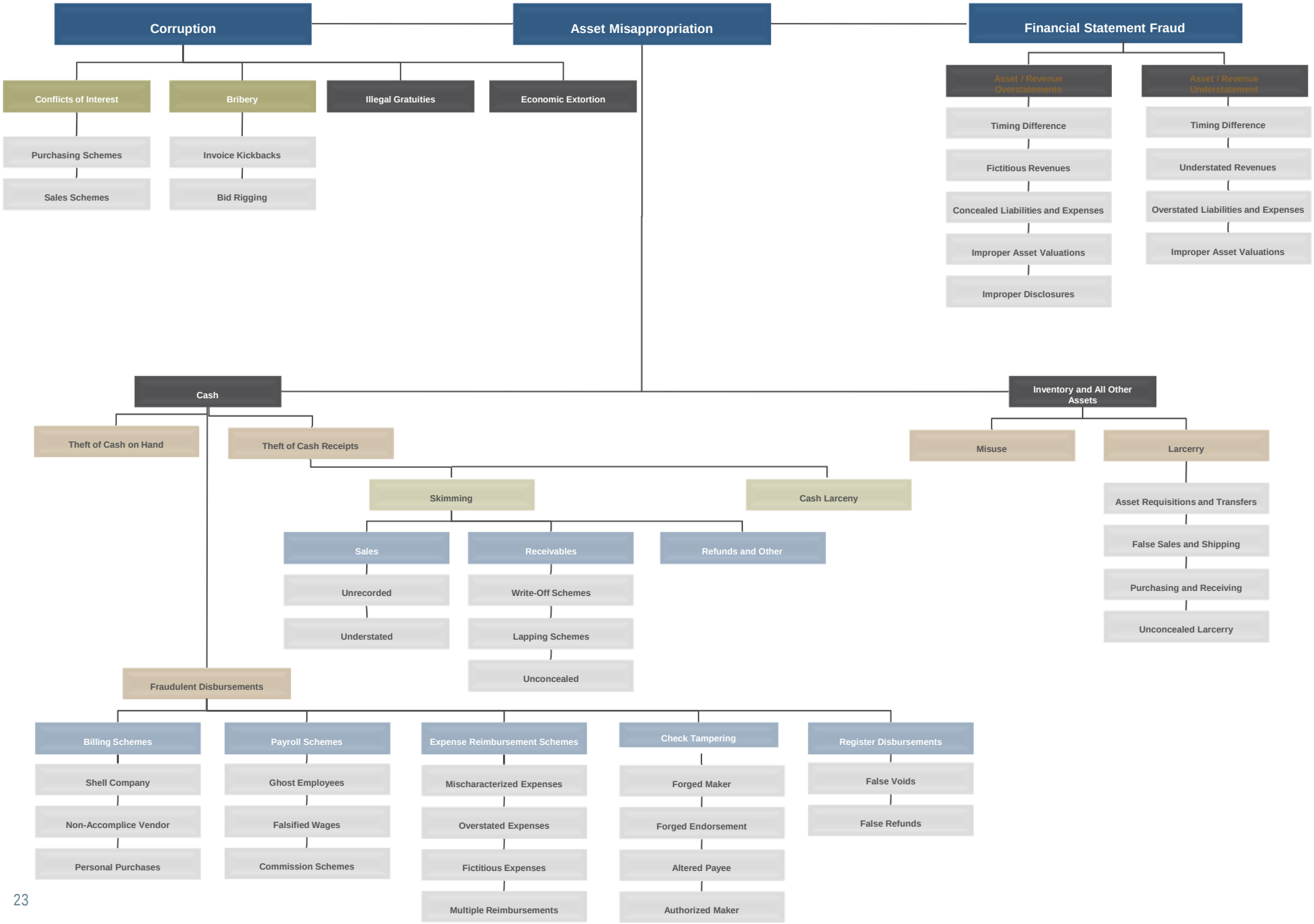
Safeguarding of assets – refers to protection from the unauthorized, inappropriate and intentional acquisition, use or disposal of organization's assets.

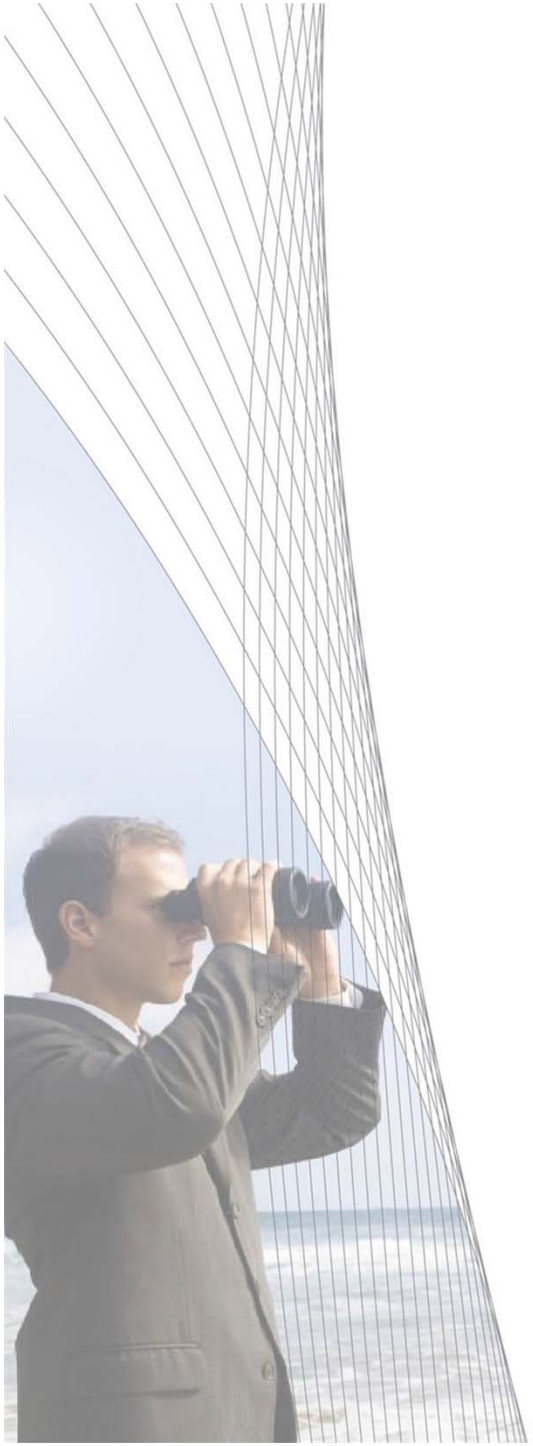
Corruption – involves improper use of an employee's influence in business transactions which violates duty to employer for purpose of obtaining benefit for themselves or someone else.

Management override – describes actions in which internal controls are intentionally overridden for an illegitimate purpose.

protiviti®

Occupational Fraud and Abuse Classification System
2014 Report to the Nations on Occupational Fraud and Abuse (ACFE)





Powerful Insights.
Proven Delivery.®

Q & A

protiviti®

Contact Information

Pamela Verick

protiviti®
Risk & Business Consulting.
Internal Audit.

1751 Pinnacle Drive
Suite 1600
McLean, VA 22102

Direct: 703.299.3539
Mobile: 703.338.2322
Fax: 571.382.7376
pam.verick@protiviti.com

Powerful Insights. Proven Delivery.™

protiviti®

Powerful Insights.
Proven Delivery.®