Vasquez & Company LLP
Effective Risk Assessment
Objectives

1. Understand the nature of a risk assessment
2. Understand the potential scope and components of a risk assessment
3. Learn how to make the risk assessment relevant to stakeholders
Introduction

Why should we care about Risk Assessment?
Maybe NEXT time you’ll hand the Risk Assessment in ON TIME!
Why Risk Assessment – or
What Could Possibly Go Wrong?

• Hacker finds and reveals unkind emails about important clients
• Sensitive business emails are sent on a personal account
• A Super Bug holds your financial system hostage
• A Super Bug infects patients
• The electricity grid is brought down – and stays down
Why Risk Assessment – or What Could Possibly Go Wrong?

• IT back-up procedures failed, but no one noticed
• IT Director “holds all passwords, etc” – and goes missing
• The newly-elected governing board wants lots of audits – but does not understand risk assessment.
Identifying risks and risk *management* techniques is a service Internal Audit can bring to the Organization and each department.

**TYPES OF RISK EXPOSURE**

- **Financial Risks**
  - Funding Source
  - Theft
  - Misappropriations

- **Compliance Risks**
  - Laws and Regulations
  - Grantor Requirements

- **Operational Risks**
  - Service Interruptions
  - Safety issues
  - Litigation
Objective #1

Understand the nature of a risk assessment
Risk Assessment Defined

A **systematic** process for identifying and evaluating **events** (*possible risks or opportunities*) that could affect the achievement of **objectives** (*positively or negatively*).

- Should be a structured process
- Requires knowledge of the organization’s objectives
- Should consider events both *external* (economy, regulations, elections, competition, hackers) or *internal* (people, processes, infrastructure, IT)
Risk Assessment Defined

Put another way:

Risk assessment is a mechanism for identifying variables to which the organization may be exposed or

What could possibly go wrong?
Risk Assessment in Dilbert’s World

WE’LL NEED A RISK ANALYSIS ON THIS PROJECT BEFORE I CAN APPROVE IT.

RISK 1: INDECISIVENESS
RISK 2: OVERANALYSIS
RISK 3: CLUELESSNESS
RISK 4: MICROMANAGEMENT...

I DON’T UNDERSTAND THESE RISKS.

THAT’S NUMBER THIRTY-SIX.
Risk Assessment Characteristics

- Identifies which risks represent *opportunities* and which represent potential *pitfalls*
- Considers the organization’s *objectives*
- Considers the organization’s *risk tolerance*
- Identifies potential events through a *collaborative process*
- Identifies *predictive indicators* to help anticipate possible risks before they occur
COSO – AGAIN!

Control Environment

Risk Assessment

Control Activities

Information & Communication

Monitoring Activities

Operations

Reporting

Compliance

Entity Level
Division
Operating Unit
Function
COSO Components: Risk Assessment

• Principle #6: Objectives
• Principle #7: Risk Identification
• Principal #8: Fraud Considerations
• Principal #9: Identifying Changes
COSO Components: Risk Assessment

• **Principle #6:** The organization specifies objectives with sufficient clarity to enable the identification and assessment of related risks. *(from the budget process?)*

• **Principle #7:** The entity identifies risks to achieving its objectives; determines how the risks should be managed *(collaboratively?)*
COSO Components: Risk Assessment

- **Principle #8:** The organization considers the potential for fraud in assessing risks to the achievement of objectives. *(computer fraud?)*

- **Principle #9:** The organization identifies and assesses changes that could significantly impact the system of internal control. *(new technology?)*
Types of Fraud Risks:

- Fraudulent financial reporting*
- Misappropriation of assets*
- Corruption

* Considered by external auditor.
Principal #8 - Examples of Fraud Risks

• Fraudulent financial statements which can lead to:
  – Concealing unauthorized expenditures
  – Concealing misappropriation of assets
  – Inaccurate reporting of revenues, costs, assets, debt, etc.

• Misappropriation of assets by:
  – Employees
  – Vendors
  – Former employees or other outsiders
Principal #8 - Examples of Fraud Risks

• Corruption may take the form of:
  – Bribery and gratuities
  – Aiding and abetting fraud by other parties (e.g., vendors).
  – Conflicts of interest
  – Improper use of grant funds
  – Embezzlement
Identify inherent fraud risk — Consider incentives, pressures, and opportunities to commit fraud; and IT fraud risks.

Assess likelihood and significance of inherent fraud risk — based on historical information, known fraud schemes, IT vulnerabilities and interviews with staff, including business process owners.

Respond to reasonably likely and significant fraud risks

  • Decide what the response should be;
  • Perform a cost-benefit analysis of fraud risks in relation to costs of controls or specific fraud detection procedures.
Indicators of Fraud Risk

- Conditions threaten entity’s financial stability
- Nature of the entity’s operations
- Monitoring of compliance is inadequate
- Organization structure is unstable or unnecessarily complex
- Communication by management is lacking
- Management’s willingness to accept high levels of risk in making significant decisions
Assessing Likelihood of Inherent Fraud Risks

Criteria to assess likelihood:

• Has the particular fraud occurred in the past?
• Is the fraud prevalent in the agency’s industry?
• Number of individual transactions
• Complexity of the risk
• Number of people involved in reviewing or approving the process.

Categories of likelihood: remote, reasonably possible, and probable.
Assessing Significance of Inherent Fraud Risks

Significance may be determined by:

- Financial statement significance
- Monetary significance
- Potential criminal, civil, and regulatory liability
- Reputational impact

Significance may be categorized as immaterial, more than significant and material.
How to Identify Inherent Fraud Risks

• **Brainstorm** to discuss:
  – incentives, pressures, and opportunities to commit fraud
  – risks of management override of controls
  – the population of fraud risks relevant to the agency
  – other risks, i.e., regulatory and legal misconduct risk,
  – the impact of IT on fraud risks

• **Share** the fraud risk identification information with the BOD or audit committee, and with senior management.
# FRAUD RISK ASSESSMENT FORM

<table>
<thead>
<tr>
<th>Identified Fraud risks and Schemes</th>
<th>Likelihood²</th>
<th>Significance³</th>
<th>People and/or Department⁴</th>
<th>Existing Anti-fraud Controls⁵</th>
<th>Controls Effectiveness Assessment⁶</th>
<th>Residual Risks⁷</th>
<th>Fraud Risk Response⁸</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINANCIAL REPORTING:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MISAPPROPRIATION OF ASSETS:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CORRUPTION:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[\text{Page 1 of 2} \]
Risk Overload

Well don't say I didn't warn you.
Risk of Management’s Override of Controls

- Personnel may know the controls and standard operating procedures that are in place to prevent fraud.
- Such knowledge can be used to commit and conceal fraud.
- Example - a manager who has the authority to set up new vendors and approve invoices may create and approve a fictitious vendor and then submit invoices for payment. 
  
  *Sound familiar?*

*An anti-fraud control is not effective if it can be overridden easily.*
Objective #1 - Review

**Objective** - Understand the nature of a risk assessment

**Summary** – Risk assessment is a tool for considering what could happen, what it would mean, and how to respond to this knowledge
Objective #2

Understand the potential scope and components of a risk assessment
Risk Assessment Potential

- Risk assessments (SOX-mandated) usually focus on internal control over financial reporting and operational risk management.

- Risk assessments could include risks that may impact business development, staff retention, profitability, operational efficiency or program effectiveness.
Operational Audit

Financial Audit

Compliance Audit

Cash handling, payroll, fixed assets, verification, expenditures, and revenue

Significant areas not often addressed:

- Revenue maximization and cost minimization
- Follow-up audits
- Compliance with Regulatory, legal and legislative mandates
- Service delivery
- IT management
The New COSO Framework

“The New COSO Framework reflects the increased relevance of technology”

Mainframes → Servers → The Cloud

Personal Computers → Kiosks → And Beyond??

Devices → Meter Reader Devices
**Good News** - Built-in Computer Controls such as:
- Segregation of accounts payable input and approval duties
- Segregation of vendor set-up and purchasing approval capabilities.
- Segregation of HR new hire authorizations from payroll processing

**Bad News** - However, agencies need to control unauthorized access.
IT and Fraud Risks

IT is a critical component to any risk assessment

• We rely on IT to conduct business, communicate, and process financial information.
• Poorly designed/controlled IT environments expose an agency to fraud
• Today’s computer systems, linked by national and global networks, face an ongoing threat of cyber fraud and more
• IT risks include:
  – threats to data integrity,
  – threats from hackers to system security,
  – theft of financial and sensitive information
  – Unauthorized access to sensitive data
  – Damages due to viruses.
Misappropriation of Assets

By Employees:

- Creation of, and payments to, fictitious vendors
- Charging personal expenses on procurement cards
- Payment of inflated or fictitious invoices
- Invoices for goods/services not received
- Theft of inventory

Which of these can be enabled through technology?
Misappropriation of Assets

By Employees in collusion with vendors, customers or third parties:
• Payment of inflated or fictitious invoices
• Invoices for goods not received or services not performed

By Vendors:
• Inflated or fictitious invoices
• Short shipments or substitution of lower quality goods
• Invoices for goods not received or services not performed.
IT and Misappropriation of Assets

Theft of assets
With access to assets (e.g., cash, inventory, and fixed assets) and to accounting systems that track and record activity related to those assets, IT can be used to conceal the theft of assets.

Examples - an individual establishes a fictitious vendor in the vendor master file to facilitate the payment of false invoices, or

Individual steals inventory and records the assets as disposed of, removing the asset from balance sheet.
Mitigating the Risk of Misappropriation of Assets

Risk Mitigation may require:

• Processing controls (separation of duties)
• Safeguarding controls (access restrictions)
• Detection controls (physical inventory)

Which of these are enabled (or defeated) with technology?
Unauthorized access to accounting applications

Personnel with inappropriate access to the general ledger, subsystems, or the financial reporting tool can post fraudulent entries.

Override of system controls

General computer controls include restricted system access, restricted application access, and program change controls. IT personnel may be able to access restricted data or adjust records fraudulently.
IT and Corruption

**Misuse of customer data**
Personnel within or outside the organization can obtain employee data and use such information to obtain credit or for other fraudulent purposes.

**Improper payments**
Individuals who can access, or convince others to access, systems to initiate payroll/disbursements may initiate improper payments
“We back up our data on sticky notes because sticky notes never crash.”
Objective #2 - Review

**Objective** - Understand the potential scope and components of a risk assessment.

**Summary** – The risk assessment should address IT-related risks, business risks, compliance risks and financial processing and reporting risks.
Objective #3
Learn how to make the risk assessment relevant to stakeholders
A new CEO asked his executive team to conduct a risk assessment to identify key obstacles the company faced. The team held a two-day workshop to identify these top-level issues. After the meeting, each executive was charged with analyzing in detail one or more of the issues. A month later, the team put together a report for the CEO to consider.

The report failed the CEO’s inexact but important test. “Not a single item on the list was something that kept me up at night”, he noted. “Not only that, but the executive team didn’t seem to have a plan to address the risks they identified.”
Critical Success Factors for Risk Assessment

1. Start with Enterprise-level *Objectives*
2. Use a common approach, processes and vocabulary
3. Look at risks across departments/functions and in relation to one another
4. Begin with top-down risk analysis; involve senior management
5. Involve lower-level personnel through technology
6. Look to external sources; events affecting peers
7. Have business owners take responsibility for risks
8. Create an action plan to manage risks – with milestones
9. Make risk assessment part of daily activities/planning
10. Link risk management to performance measures
Focus should be on:

• Key business risks
• Developing a risk profile
• Validating risk profile with mgmt./process owners
• Identifying significant risk drivers
• Evaluating impact and likelihood of key risks
• Capturing existing risk management activities
• Evaluating risk management activities
• Analyzing gaps and opportunities for improvement
• Reviewing existing monitoring procedures.
Benefits of effective risk management:

- Promotes better business performance
- Minimizes surprises through proactive identification of risks
- Increases stakeholder confidence
- Reduces likelihood of loss from negative events
- Helps identify and take advantage of opportunities
- Facilitates more effective decision-making when risk is known and mitigations factors are built into activities
- Increases efficiency by reducing time spent reacting to crises
- Improves governance by helping explain boundaries of acceptable conduct – both mandated and voluntary
The Risk Assessment Team

- Management identifies a risk assessment team
- Team should involve individuals throughout the organization with different knowledge, skills, and perspectives
  - Accounting/finance personnel familiar with internal controls
  - IT personnel familiar with IT systems and controls
  - Legal and compliance personnel
  - Nonfinancial business/operations personnel for insight into day-to-day operations
  - Internal audit personnel.
- **Management should participate** in the assessment, as they are ultimately accountable

Agree? BOD?
ROLE OF AN AUDIT COMMITTEE

- Review audit plans and budget
- Review requests for Internal Audit projects
- Review Department’s progress in implementing audit recommendations
- Review results of Internal Audit activities
PRIORITIZATION OF RESOURCES

Management

Discretion

Limited Audit Focus

Second Tier Audit Focus

First Tier Audit Focus

High Priority for audit focus

Probability of Occurrence

Low

High

Magnitude of Impact

Low

High

Limited Audit Focus

High

Low

Probability of Occurrence

High

Low

Magnitude of Impact
Residual Fraud Risks

• Certain fraud risks may be too expensive and time-consuming to address via controls
• If a fraud is discovered, zero tolerance for fraud will be applied
• Management and the BOD need to know that there ARE residual fraud risks
• The overall objective is to have the benefit of controls exceed their cost.
Implementing a Control Self-Assessment System

• Leverage the IA function by shifting some of the control monitoring responsibilities to the functional areas

• IA customers are responsible for monitoring controls in their environment

• Emphasis will be placed on training management and administrative personnel to recognize the need for controls

Control Self Assessment Continuum

Interactive Workshops
Control Model Workshops
Interview Techniques
Control Guides
Customized Questionnaires
ICQ Self Audit

Behavioral

Mechanical
One City’s Risk Assessment

1. Define audit universe (all departments and their activity groups – using budget)
2. Identify and rank major risks – using Management Questionnaires with 10 measurable risk factors
3. Each factor was assigned a risk score
4. Each factor was weighted
5. Maximum possible score of 900
6. Most audits selected scored less than 500
7. No IT audit consideration
8. No mention of the City’s objectives at any level
One City’s Risk Assessment Factors

1. Interface with general public
2. Mission critical nature of activity for dept. to achieve its goals
3. Support of internal operations is considered critical to other departments
4. Failure to achieve activity group’s mission leads to public displeasure or negative media coverage.
5. Level of cash or near cash activity
6. Activity groups use of performance measures
7. Regulation effect or impact on operations
8. Number of budgeted employees (FTE)
9. Level of budgeted annual revenues
10. Level of budgeted annual expenses
Objective #3

Objective: Learn how to make risk assessment relevant to stakeholders

Summary: Focus on what’s important; create a team; involve personnel throughout the organization, engage management/BOD
"We've considered every potential risk except the risks of avoiding all risks."
Contact Information

Peggy McBride

pmcbride@vasquezcpa.com

(213) 873-1706

(714) 231-6029